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

General Editors: Virgilio Ilari, Jeremy Black, Giovanni Brizzi.

Legal Editor (dir. responsabile Gregory Alegi **Ed. executive (comitato di redazione):** Viviana Castelli, Alessandro Carli, Emiliano Bultrini, Francesco Biasi, Francesco Pellegrini. **Special appointee for Intl cooperation:** Dr Luca Domizio.

Scientific Editorial Board : Foreign members: Prof. Jeremy Armstrong, Christopher Bassford, Floribert Baudet, Stathis Birtachas, Lee L. Brice, Loretana de Libero, Fernando Echeverria Rey, John France, Francisco García Fitz, Tadeusz Grabarczyk, Gregory Hanlon, Rotem Kowner, Armando Marques Guedes, Harold E. Raugh Jr, Yannis Stouraitis: **Italian members:** Giampiero Brunelli, Aldino Bondesan, Piero Cimbolli Spagnesi, Alessandra Dattero, Immacolata Eramo, Carlo Galli, Maria Intrieri, Roberta Ivaldi, Nicola Labanca, Luigi Loreto, Luca Loschiavo, Serena Morelli, Francesco Somaini, Gioacchino Strano, Giusto Traina, Federico Valacchi.

Senior Academic Advisory Board. Prof. Massimo de Leonardis, Magdalena de Pazzis Pi Corrales, John Hattendorf, Yann Le Bohec, (†) Dennis Showalter, Livio Antonielli, Marco Bettalli, Antonello Folco Biagini, Franco Cardini, Piero del Negro, Giuseppe De Vergottini, Gian Enrico Rusconi, Carla Sodini, Donato Tamblé,

Special Consultants: Lucio Caracciolo, Flavio Carbone, Basilio Di Martino, Antulio Joseph Echevarria II, Carlo Jean, Gianfranco Linzi, Edward N. Luttwak, Matteo Paesano, Ferdinando Sanfelice di Monteforte, Simonetta Conti, Elina Gugliuzzo, Vincenzo, Angela Teja, Stefano Pisu, Giuseppe Della Torre

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

©Authors hold the copyright of their own articles.

For the Journal: © Società Italiana di Storia Militare

(www.societaitalianastoriamilitare@org)

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)

NAM Studies & Documents
Special Dossier October 2025
Ukraine Military and Wartime Law

Edited by Ganna Sobko

Contents:

Informational and psychological security as factors of national security during martial law

by Olena Bortnikova, Bohdan Morklyanyk, Valentyn Pylypchuk, Kateryna Novytska, Marharyta Martynenko[1]

Abstract, In the article, based on the analysis of the current state of information and psychological security as factors of national security during martial law, the main problematic issues of the effective application of methods of ensuring information and psychological security within the limits of national security are identified and the ways to solve them are identified. Factors influencing the increase in the number of threats and risks of informational and cognitive destructive impacts on technological systems, the personnel composition of the Armed Forces of Ukraine, and the civilian population during a state of war were investigated. Additionally, aspects of ensuring societal information freedoms are disclosed, taking into account the protection of state information security in times of war. Priority directions for protecting the information space have been identified, and a review of typical threats to information security has been conducted. The main directions of information attacks against Ukraine have been outlined, and a classification of information-psychological threats has been provided. The negative consequences of information-psychological influence on the psyche have been examined, and effective measures for protection against it have been provided. The practical result of the study is a set of recommendations for increasing the effectiveness of methods of ensuring informational and psychological security within the framework of national security during martial law. The theoretical outcome is the identification of the fundamental patterns of interaction between information and psychological security within the framework of national security. The scientific novelty of the research lies in conducting an analysis of information and psychological security specifically as factors of national security during a state of war, and identifying the relationship between these types of security. This allowed for the formulation of recommendations to enhance the effectiveness of implementing methods for ensuring information and psychological security, thereby improving the overall state of national security. The scientific novelty of the research lies in conducting

1 Yevhenii Berezniak Military Academy, 04050, 81 Ilyenka St., Kyiv, Ukraine.

NAM, Anno 6 – Special Dossier
DOI: 10.36158/97912566922171
Ottobre 2025

an analysis of information and psychological security specifically as factors of national security during a state of war, and identifying the relationship between these types of security. This allowed for the formulation of recommendations to enhance the effectiveness of implementing methods for ensuring information and psychological security, thereby improving the overall state of national security. All this can be done only in the interaction of the state with private initiative: foundations, volunteers, media resources, press publishers, groups of psychologists.

Keywords: security factors, threats, information attacks, consequences of impacts, security measures, war.

Introduction

After the start of the aggression by the Russian Federation against Ukraine, a state of emergency was declared by the acting President of Ukraine, Oleksandr Turchynov, on March 17, 2014. This state of emergency lasted until September 26, 2016, and concluded with the demobilization of the sixth wave of mobilized individuals (Titarenko, 2024). In February 2022, the Russian Federation initiated a full-scale invasion, which served as a signal for declaring a state of war in Ukraine (Vasylchyshyn et al., 2022). The question of comprehensive national security provision has arisen before Ukrainian society as a crucial factor for its own survival during the war. Due to the constant information attacks by the Russian Federation on technological systems, the personnel composition of the Armed Forces of Ukraine, and the civilian population (Kalinichenko, 2020) the following destructive impacts have begun to manifest:

- partial destabilization of military command systems;
- breach of confidentiality of classified information;
- damage to equipment and communication lines;
- distrust among certain population groups;
- internal fragmentation of society;
- distrust towards key allies.

With the aim of ensuring the information security of Ukraine, the “Doctrine of Information Security of Ukraine” was approved by the Decree of the President of Ukraine on February 25, 2017 (Poroshenko, 2017). After the declaration of a state of war, on March 18, 2022, the decision of the National Security and Defense Council (NSDC) “On the Implementation of a Unified Information Pol-

icy in Conditions of Martial Law" was adopted. It emphasized the priority of implementing a unified information policy concerning national security matters. (2022). The recent bitter experience of Ukraine underscores that national independence exists only when national security is reliably ensured, based on the strategy of national security of Ukraine (National security and defense council of Ukraine, 2020; Smolyanyuk, 2018).

It should be noted that information and psychological security are as important factors of national security as military security. Therefore, in order to enhance national security, it is necessary to consider the main problematic issues of effectively implementing methods for ensuring information and psychological security during a state of war (Averyanova & Voropaeva, 2020; Panchenko, 2019). The need to consider issues related to the effective implementation of methods for ensuring information and psychological security during a state of war is also driven by a number of factors:

- heightened importance during wartime;
- imperfections in the state's information policy;
- continuous influence of communication tools on individual consciousness;
- widespread manipulation of people's consciousness and the use of information-psychological influence technologies on them;
- involvement of professional teams in information attacks;
- the ultimate consequence of destructive influences could be the undermining of the foundations of national security and even defeat in war.

As a result of the conducted research, the main problematic issues regarding the effective implementation of methods for ensuring information and psychological security within the framework of national security were identified. This allowed for the provision of recommendations aimed at enhancing the effectiveness of applying methods for ensuring information and psychological security within the framework of national security during a state of war. Additionally, the main patterns of interaction between information and psychological security were identified. The main drawback of the study can be attributed to a series of gaps resulting from insufficient information about the national security of Ukraine and the unavailability of confidential or secret data.

Further research on the defined topic should include examples of tools used

to ensure information and psychological security in several other countries. Measures to ensure national security in the United States, China, and EU member countries could be particularly interesting from a research perspective. This will allow for a comparison between the ideas proposed within the scope of the research regarding the provision of information and psychological security as factors of national security and the existing models in the specified countries. This comparison will enable the assessment of their effectiveness and the proposal of the best practices for practical implementation by Ukraine's special services.

Literature review

Leading countries around the world support their national security according to existing and forecasted risks and threats. They primarily ensure it through the development and implementation of a unified system of modern high-tech tools (Brantly et al., 2017). The category of "national security" was first voiced by President Theodore Roosevelt of the United States in 1904 in his message to Congress regarding the annexation of the Panama Canal Zone in accordance with the interests of national security (Abramov et al., 2016). Since then, the issue of national security has begun to interest researchers from around the world. These studies are especially relevant now due to international turbulence and new threats in the context of information and psychological security as factors of national security.

Among Ukrainian researchers, questions of national security have been studied by Vlasiuk O., Vonsovych O., Horbulin V., and Danyk Yu. The book by O. Vlasiuk (2016) explores the influence of domestic policy issues on Ukraine's national security and reflects the scholarly perspective on national security as a systemic phenomenon, problems of ensuring national security in the conditions of globalized world, evolution of threats to Ukraine's national security, issues of shaping Ukrainian national identity, human development, regional policy, information security, and reforming the state's military organization.

The article by O. Vonsovych (2017) contains research on the state of national security in Ukraine amidst modern geopolitical changes. It argues that the geopolitical rivalry for Ukraine between the Russian Federation and the United States of America introduces negative adjustments and renders our state dependent on external influences. The main affected spheres are specified:

- political;
- economic;
- social;
- informational.

In the joint research by Horbulin V. and Danyk Yu. (2020), the priorities of Ukraine's national security in the conditions of the pandemic are examined. As part of the research, the following directions for strengthening national security were identified as priorities:

- socio-economic;
- organizational;
- financial-economic;
- cyber-informational and high-tech.

Foreign researchers such as Krawciw, Ranjan, and Sayler have examined issues of national security. One of the chapters of Krawciw's book (2016) is dedicated to the development of national security after Ukraine gained independence. The main problems that hindered the effective implementation of national security policy were identified:

- chaotic processes;
- lack of experience;
- inability to clearly define own interests;
- absence of necessary legislation and institutions;
- internal struggles and conflicts.

In the article by Ranjan (2023), it is argued that in the process of implementing trade sanctions against Russia, countries may rely on their own national security interests and make exceptions to the rules of the World Trade Organization (WTO). In the report to the US Congress prepared by the research analyst Sayler (2020), the connection between artificial intelligence technologies and issues of national security is discussed. This report identifies China as a leading competitor in the development of artificial intelligence, according to the published plan of 2017, which aims to achieve global leadership in AI development by 2030. The essence of the report is to inform members of Congress about the threats to U.S. national security in the field of artificial intelligence.

It is also necessary to mention research on information and psychological security as factors of national security in the works of such domestic researchers

as Kachynskyi A., Prokopenko O., Fedoriienko V., Kulchytskyi O., and foreign scholars like Liu W., Shandler R., Gross M., Canetti D.

In the study by Kaczynski (2022), information is considered a critically important resource that impacts the state of national security in Ukraine, necessitating the development of theoretical foundations and practical methods for state information security policy. The conclusion of the research is the thesis that providing freedom of action to decision-making subsystems at all levels of the hierarchical structure will enhance the effectiveness of countering disinformation.

In the article by the collective of the Educational and Scientific Center for Strategic Communications in Ensuring National Security and Defense of the National Defense University, consisting of Prokopenko et al. (2023), the approach to identifying and analyzing information threats to Ukraine's national security within the strategic communications system is investigated. The methodological approach proposed in the article for monitoring the information space provided a comprehensive understanding of the information support for the work of the government, state institutions, and public figures through the communicative capabilities of the state.

Taiwanese scholar Liu (2024) examined the factors of psychological readiness, civil defense, and permanent warfare in the context of a potential military conflict in Taiwan. The purpose of the article is psychological preparation for the attack of China and resistance to the aggressor, the basis of the study was the war of the Russian Federation against Ukraine.

The research work of Shandler et al. (2023) includes an analysis of cyber attacks, psychological disorders, and military actions as components of national security. The conclusions of the study indicate that even non-physical destructive cyber attacks can lead to consequences comparable to armed aggression, thus justifying the use of armed force for self-defense.

Given the findings from the reviewed studies, it is worth noting that they do not address practical recommendations for enhancing the effectiveness of applying methods to ensure information and psychological security within the framework of national security during a state of war. The aim of the research is to analyze informational and psychological security specifically as factors of national security during a state of war, and to identify the correlation between these types of security. Furthermore, the goal is to provide recommendations for enhancing

the effectiveness of implementing methods to ensure informational and psychological security.

Methodology

The research utilized scientific literature related to the thematic focus, including monographs and scholarly-analytical publications by Ukrainian and international researchers on the studied issues, as well as the results of independent observations. To address the set objectives, a variety of general scientific methods were applied:

- monitoring method: Used for gathering, organizing, and analyzing information on psychological and informational security;
- comparison method: Was useful in reconnaissance during the investigation of the level of destructive influences on the population compared to those on the personnel of the Armed Forces of Ukraine;
- abstraction method: Used in the study to highlight the main concepts and categories;
- analysis and synthesis methods: Used in the process of identifying the stages and factors of development, as well as the most influential elements of the researched object;
- inductive method: Employed for predictive analysis of the expected effectiveness of implementing methods to ensure informational and psychological security;
- abstract-logical, dialectical, and scientific abstraction methods: Utilized in the study for forming theoretical generalizations, refining the conceptual framework, and formulating conclusions;
- specification method: Used to document the effectiveness and feasibility of proposed means to enhance the application efficiency of methods ensuring informational and psychological security;
- quantitative data processing method: Enabled the expression of various aspects of national security in numerical values.

For addressing specific tasks, the research utilized specialized methods including information collection, processing, analytical work, and justification.

The main objectives of the research are identified as follows:

- Analyzing the current state of information and psychological security as factors of national security during a state of war.
- Identifying the main problematic issues of effective application of methods for ensuring information and psychological security within the framework of national security.
- Determining the ways to address the problematic issues of effectively applying methods to ensure information and psychological security within the framework of national security.
- Researching the factors influencing the increase in the number of threats and risks of informational and cognitive destructive impacts on technological systems, the personnel of the Armed Forces of Ukraine, and the population during a state of war.
- Unveiling aspects of ensuring societal information freedoms while considering the protection of state information security in wartime conditions.
- Determining priority directions for safeguarding the information domain and conducting a review of typical threats to information security.
- Reviewing the negative consequences of informational-psychological influence on the psyche and proposing effective measures to protect against it.
- Identified the main patterns of interaction between informational and psychological security within the framework of national security.
- Providing recommendations to enhance the effectiveness of implementing methods to ensure informational and psychological security within the scope of national security during a state of war.

The research is characterized by its fundamental nature based on the following criteria:

- The findings can serve as a basis for new fundamental, applied, and exploratory research and developments.
- It yields a high internal scientific impact, leading to the emergence of a new direction in the development of science.
- The study is grounded in a broad theoretical framework and is profound in its analysis.

The relevance of the researched topic is underscored by the critical importance of psychological and informational security issues as factors in national security, particularly in light of Russia's war against Ukraine. Participation of

professional teams in informational attacks leads to negative consequences of destructive influence, thereby affecting the capabilities of the Armed Forces of Ukraine and Ukrainian society to resist aggression. The object of the chosen research is the process of assessing the state of informational and psychological security as factors of national security during a state of war, with the subject defined as the principles of informational and psychological security as factors of national security during a state of war.

Results

National security depends on the level of organization of state institutions and the level of awareness of the population. Only based on unity and interethnic harmony, with a national idea supported by the majority of the population, can the state become strong and developed. Therefore, the implementation of responsible domestic and foreign policies is the key to national security (Levchenko et al., 2019).

Let's identify the main factors of national security (Table 1).

Table 1. A generalized overview of the main factors of national security

№	The name of the factor	The essence of the factor
1	Information Security	Information security practices involve reducing information risks, typically entailing prevention or mitigation of the unauthorized or improper access to data, as well as illegal use, disclosure, breach, deletion, damage, alteration, inspection, recording, or destruction of information.
2	Economic Security	The ability of a state to sustain and develop its national economy, without which managing other dimensions of national security is impossible. Economic strength significantly determines the nation's defense capability, and therefore, reliable economic security directly affects the national security of the nation.
3	Psychological Security	Psychological security can be viewed as an integrative characteristic of the individual-subject, reflecting the degree of satisfaction of basic human needs (or group needs) for safety, psychological well-being, the creation of feelings of confidence, and stability. It encompasses a complex of cognitive, emotional-volitional, and characterological features of a person, their orientation, and worldview.

4	Energy Security	This is the connection between national security and the availability of natural resources for energy supply. International energy relations have contributed to the globalization of the world, leading to both energy security and, at the same time, energy vulnerability.
5	Military Security	It entails the ability of a nation-state to defend itself and/or deter military aggression. On the other hand, military security involves a nation-state's ability to ensure the implementation of its political decisions through the use of military force.
6	Ecological Security	It pertains to the integrity of ecosystems and the biosphere, particularly concerning their capacity to sustain a diversity of life forms, including human life. Ecosystem security has garnered increasing attention as human impact on the environment continues to escalate.

Source: compiled based on Alguliyev et.al., 2020; Fletcher, 2016, Shlyakhtunov, 2022; Overland, 2016; Haelig,2023; Liu et al., 2021

The current state of psychological and informational security in Ukraine is critical, and the trend is towards further deterioration, as Russia continues to exert informational influence aimed at shaping the consciousness of Ukrainian society. The main informational channels influencing the psychological state of the population are as follows:

- Official media outlets;
- Unofficial channels of information (Telegram, Viber, Instagram);
- Printed propaganda (leaflets, newspapers, books);
- Communication with citizens of the aggressor country.

Psychological influence is exerted through information attacks using fake accounts and bot farms, which condition individuals to unquestioningly accept any information and believe in its reality (Lyzanchuk, 2017).

The relationship between informational, psychological, and national security can be defined as a logical conjunction operation (union) of informational and psychological security, forming national security, expressed by the formula:

$$I \cap П = H \quad (1),$$

where I is informational security, П is psychological security, a H is national security.

This relationship between the factors of national security is depicted in Fig. 1.

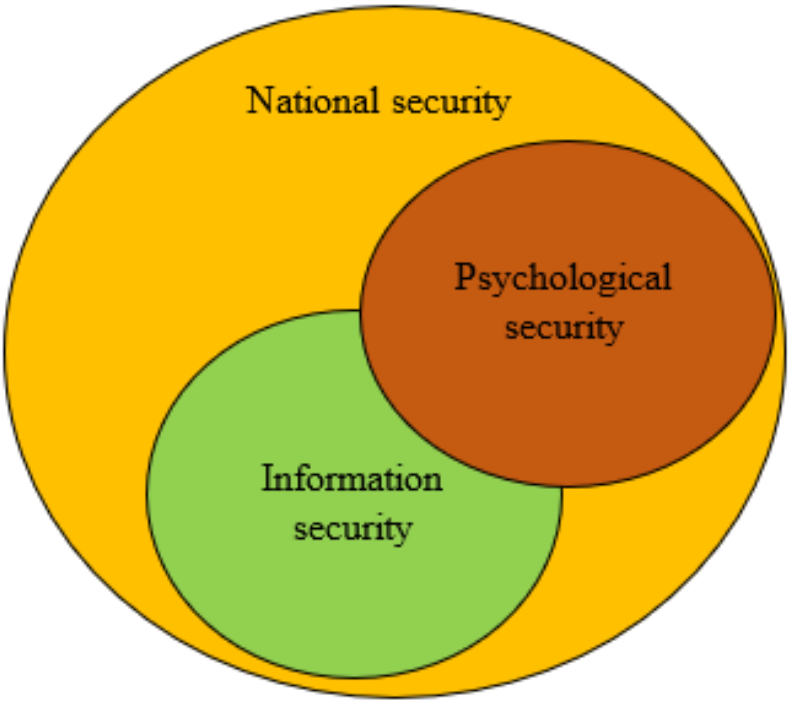


Figure 1**.** The interrelation of national security factors

Information security of the Armed Forces of Ukraine as the most important military state institution is the key to the security of the state. Protecting military information resources should indeed become the top priority task for security professionals. To mitigate threats, they need to be correctly identified and classified based on several factors:

- by origin;
- by the nature of their influence;
- by the level of danger.

Information security experts divide the types of threat sources into two groups: internal and external. Information security experts divide the types of threat sources into two groups: internal and external:

- creating tension or destabilizing the socio-political situation in the areas where military personnel are stationed: provoking personnel conflicts with the local population and inciting mass unrest;
- influencing the morale of the troops: falsification of military history facts, increasing social tension, and contact of personnel with representatives of hostile press;
- creating factions within the military: spreading radical political or religious ideas (Bodnar, 2014; Morklyanik et al., 2023).

To counter disruptions in the activities of the Armed Forces of Ukraine due to information-psychological operations, it is necessary to take a series of measures:

- conduct informational campaigns with the local population;
- teach servicemen the basics of countering information and psychological operations;
- commanders should control the content consumed by members of the military unit;
- when working with the press, verify information about journalists and publications.

Information operations are also hazardous not only for civilians or military personnel but also for the functioning of information systems. Examples of such threats and their consequences for national security can be seen in Table 2.

Table 2. Threats of information operations to information systems and their consequences

№	The name of the threat	The consequence of the information operation
1	Hacking into the military command system	It can provoke chaos during military operations, leading to the failure of the operation and resulting in casualties and equipment losses.
2	Hacking into the vehicle management system	Disabling fire and movement nodes would make the equipment an easy target for destruction.
3	Breach of data confidentiality	It can result in the recruitment of military personnel or pose a threat to their family members.
4	Theft of military secrets	It will provide the enemy with information about the activities of the armed forces, making it impossible to achieve the element of surprise during military operations.

5	Entering false data into weapons management systems	It poses a threat of destruction to own military personnel, civilian population, or infrastructure.

Source: developed by the author

To counter threats of information operations for information systems, the following means can be employed:

- further development of legislation to counter threats;
- involvement of cybersecurity professionals;
- utilization of exclusively closed networks with dedicated servers;
- collaboration among law enforcement agencies at the horizontal level;
- continuous administration of information systems.

After the start of full-scale aggression by the Russian Federation, the Verkhovna Rada adopted a bill on criminal liability for unauthorized photo and video recording of the movements of the Armed Forces and international military assistance during a state of war. On March 22, 2022, the Law of Ukraine came into force, significantly simplifying investigative procedures and access to the belongings and documents of suspects (Zelensky, 2022).

One of the most effective countermeasures against threats of information operations is the application of information operations against the enemy:

- misleading the enemy regarding measures and methods to counter threats in information security;
- regularly destroying communication centers and information systems;
- introducing harmful changes into the operation of enemy information systems;
- identifying and destroying enemy communication systems within the territory of Ukraine;
- stealing confidential information about the enemy's intentions;
- lowering the morale of enemy troops by using fakes and bot farms in hostile information networks.

For the implementation of tasks related to ensuring information security in Ukraine, various structural units of the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine are responsible (Fig. 2).

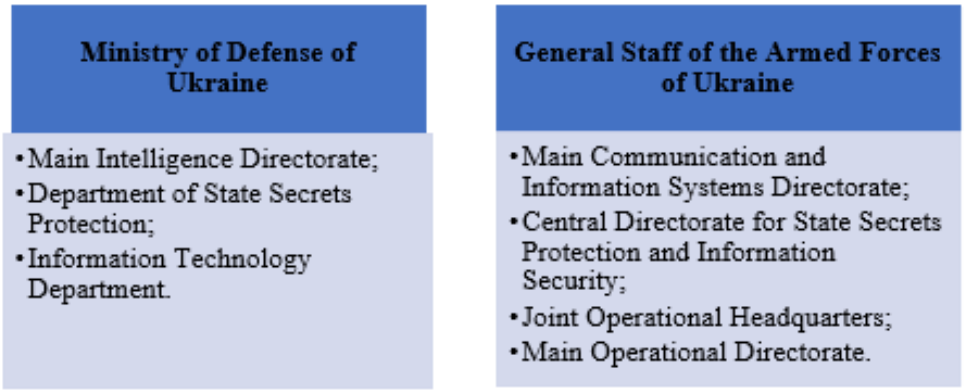


Figure 2. Structures responsible for information security in Ukraine
Source: compiled based on Danyk & Permiakov, 2018; Logvinenko, 2023.

Often these structures duplicate others and lack clearly defined goals, so it is proposed to create a single body that can ensure the implementation of the concept of information and psychological security of Ukraine as factors of national security. The main tasks of such a service are outlined in Table 3.

Table 3. The main tasks of the information-psychological security service of Ukraine and ways to address them

№	Name of the task	Way of solution
1	Participation in the formation and implementation of state policy on information and psychological security.	Participation in the formation and implementation of state policy on information and psychological security.
2	Formulation and implementation of the policy of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine regarding actions in the information space.	Cooperation and holding joint meetings and conferences with officials of the Ministry of Defense of Ukraine and commanders of the Armed Forces of Ukraine.
3	Participation in events related to the creation and development of information systems and resources in the Armed Forces of Ukraine.	Defining the information needs of the Armed Forces of Ukraine and engaging qualified specialists to work with the systems.

4	Participation in the development of standards for training specialists in information and psychological security.	Cooperation with representatives of the middle and higher education sectors to develop necessary educational programs.
5	Monitoring and analysis of the information field of Ukraine and the enemy, identification of vulnerabilities in information systems.	Use of statistical data and information security experts.
6	Participation in initiatives aimed at creating threats to the information and psychological security of the enemy.	Based on the vulnerabilities of the enemy, the most critical targets should be identified and subjected to informational and psychological attacks.

Source: developed by the author

In the proposed service structure, a number of specialized departments are to be created (Fig. 3.).

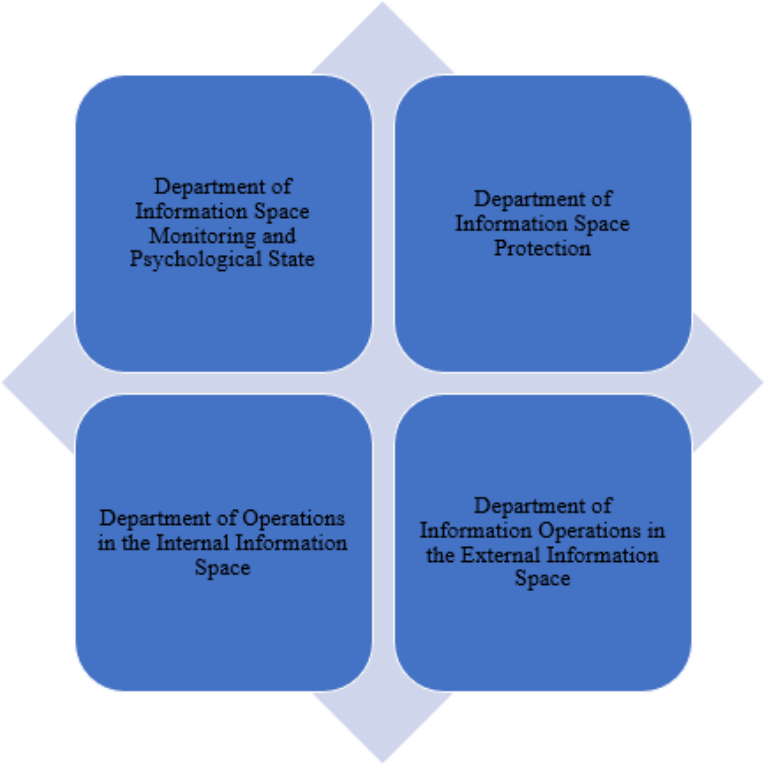


Figure 3. Departments of the proposed Information-Psychological Security Service
Source: developed by the author

Also important in the context of information security as a factor of national security is ensuring information rights and freedoms even in conditions of martial law. For this, the mechanism of the information security construction system should contain the following components:

- technical: creation and operation of all necessary technical components of the systems;
- political: state policies aimed at ensuring information security;
- legal: all regulated by laws or regulatory acts.

Obviously, during war, no state can guarantee full observance of human rights, which is a perfectly normal phenomenon in extraordinary circumstances. However, preserving the fundamental principles based on political and legal interaction mechanisms to ensure information security safeguards the foundations of democracy and the system of common principles of law from destruction (Koterlin, 2022).

Discussion

Although the topic of information and psychological security as factors of national security during wartime has gained some popularity among researchers, none of the reviewed sources have established a connection between these types of security. Also, no recommendations have been identified regarding enhancing the effectiveness of applying methods for ensuring information and psychological security that could be utilized in practice to strengthen the national security of Ukraine. The main reasons for such a situation are several factors:

- Lack of clear correlation between security factors and national security in some works (Danyk & Permiakov, 2018; Logvinenko, 2023), which impedes the establishment of hierarchical and horizontal connections between the identified categories within the scope of national security during a state of war.
- Limited theoretical foundation of research does not allow asserting its universal nature due to a large number of potential gaps (Smotrych & Brailko, 2023; Kosteniuk, 2023).
- Obsolescence of the materials used (Husar, 2022).

At the same time, some studies on information and psychological security as factors of national security during a state of war demonstrate certain unique

developments:

- effectiveness calculations have been conducted for implementing measures to counter and neutralize the negative impact of enemy information and psychological warfare (Prokopenko et al., 2023).
- a multi-tiered model of the structure of counter-propaganda organization has been developed (Kaczynski, 2022).

In one of the studies (Danyk & Permiakov, 2018), the creation of an information security management service is proposed, but the issue of psychological security in its activities and countermeasures to counter information operations threats was not addressed at all.

The recommendations for improving the effectiveness of applying methods to ensure information and psychological security, which could be used in practice to strengthen Ukraine's national security, based on this research are as follows:

- Establishing control over information channels influencing the psychological state of the population.
- Rapid and accurate identification and classification of threats.
- Striking first in information and psychological security against the enemy.
- Consolidating the structures responsible for information security in Ukraine into a single service responsible for both information and psychological security.
- Adhering to the legal regime within the framework of operations to ensure the fundamental information rights and freedoms of Ukrainians, even in times of war.
- Engage private initiatives in cooperation: foundations, volunteers, media resources, press publishers, and groups of psychologists (Bortnikova et al., 2024).

Conclusions

Indeed, during the research, an analysis of the current state of information and psychological security as factors of national security during a state of war was conducted. The main problematic issues of effective application of methods to ensure information and psychological security within the framework of national security were identified, and ways to address them were determined.

The reasons for the increase in the number of threats and risks of informa-

tional and cognitive destructive influences on technological systems, personnel of the Armed Forces of Ukraine, and the population during a state of war have been identified.

The main directions of protecting the information field have been considered, and a review of typical threats to information security has been conducted. The main directions of information attacks against Ukraine have been identified, and a classification of information-psychological threats has been provided. Negative consequences of information-psychological influence on the psyche have also been considered, and effective measures to protect against it have been provided.

A series of recommendations have been provided to enhance the effectiveness of implementing methods to ensure information and psychological security, which could be utilized in practice to strengthen the national security of Ukraine. For the first time, the connection between information, psychological, and national security has been demonstrated through logical operations, and a visual scheme illustrating their interaction has been constructed. Further research on the identified topic should include examples of the tools used to ensure information and psychological security in several other countries (such as the USA, China, and EU member states).

References

Abramov, V.I., Sytnyk, G.P., & Smolyaniuk, V.F. (2016). Global and national security. Retrieved from https://moodle.znu.edu.ua/pluginfile.php/1120366/mod_resource/content/0/%D0%93%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%20%D1%82%D0%B0%20%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B0%20%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA.pdf

Alguliyev, R., Imamverdiyev, Y., Mahmudov, R., & Aliguliyev, R. (2020). Information security as a national security component. *Information Security Journal: A Global Perspective. 30*, 1-18.

Averyanova, N., & Voropaeva, T. (2020). Information security of Ukraine: socio-philosophical aspects. *A young scientist, 10*(86), 297-303.

Bodnar, I.R. (2014). Information security as the basis of national security. *Mechanism of Economic Regulation, 1,* 68-75.

Bortnikova, O., Kashperska, D., Leonov, O., Rubel, K., & Chumak, O. (2024). Informa-

tion security of the state: Motives, necessity, and sufficiency criteria. *Lex Humana, 16*(1).

Brantly, A., Cal, N., & Winkelstein, D. (2017). Defending the borderland Ukrainian Military Experiences with IO, Cyber, and EW. Retrieved from https://apps.dtic.mil/sti/citations/AD1046052

Danyk, Y.G., & Permiakov, O. (2018). Modern information technologies in ensuring national security and defense: realities and development trends. *Modern Information Technologies in the Field of Security and Defense, 31*(1), 159-176.

Decision of the National Security and Defense Council of Ukraine regarding the implementation of a unified information policy under martial law. (2022) Retrieved from https://zakon.rada.gov.ua/laws/show/n0004525-22#Text

Fletcher, M. (2016). An introduction to information risk. The National Archives. Retrieved from https://blog.nationalarchives.gov.uk/introduction-information-risk/

Gorbulin, V.P., & Danyk, Y.G. (2020). National security of Ukraine: focus of priorities in the conditions of the pandemic. *Bulletin of the National Academy of Sciences of Ukraine, 5,* 3-18. Retrieved from http://dspace.nbuv.gov.ua/handle/123456789/170038

Haelig, C.G. (2023). Political-military integration the relationship between national security strategy and changes in military doctrine in the United States Army and marine corps. Retrieved from https://asiapolicy.utexas.edu/team/carlton-haelig/

Husar, O. A. (2022). Human information security under martial law. https://er.nau.edu.ua/bitstream/NAU/61299/5/%d0%86%d0%bd%d1%84%d0%be%d1%80%d0%bc%d0%b0%d1%86%d1%96%d0%b9%d0%bd%d0%b0%20%d0%b1%d0%b5%d0%b7%d0%bf%d0%b5%d0%ba%d0%b0%20_67-70.pdf

Kaczynski, A. (2022). A system model of the organization that ensures informational and informational and psychological security. *Information and Law, 4*(43), 102-108.

Kalinichenko, B.M. (2020). The phenomenon of information warfare in the Ukrainian mass media. *Politicus, 2*, 88–93.

Kosteniuk, N. (2023). Psychological features of managerial decision-making in the field of national security. *Theoretical and Applied Issues of State Formation, 30*, 20-27.

Koterlin, I.B. (2022). Information security in the conditions of martial law in the aspect of ensuring informational rights and freedoms. *Actual Problems of Domestic Jurisprudence, 1,* 150-155.

Krawciw, N.S. (2016). Ukrainian perspectives on national security and Ukrainian military doctrine. In the international politics of Eurasia: v. 5: State building and military power in Russia and the New States of Eurasia. Retrieved from https://www.taylorfrancis.com/books/edit/10.4324/9781315483771/international-politics-eurasia-5-state-building-military-power-russia-new-states-eurasia-bruce-parrott

Levchenko, O.G., Zemlyanska, O.V., Prakhovnik, N.A., & Zatsarny, V.V. (2019). Life safety and civil protection. Retrieved from https://opcb.kpi.ua/wp-content/uploads/2014/09/%D0%9A%D0%BE%D0%BD%D1%81%D0%B-

F%D0%B5%D0%BA%D1%82-%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9-%D0%91%D0%96%D0%94-%D0%A6%D0%97-%D0%A4%D0%9C%D0%9C-%D1%80%D0%B5%D0%B42020-.pdf

Liu, T., Wang, H.Z., Wang, H.Z., & Xu, H. (2021). The spatiotemporal evolution of ecological security in China based on the ecological footprint model with localization of parameters. *Ecological Indicators, 126,* 107636. Retrieved from https://www.sciencedirect.com/science/article/pii/S1470160X21003010

Liu, W. (2024). The mundane politics of war in Taiwan: Psychological preparedness, civil defense, and permanent war. *Security Dialogue, 55*(1), 103-122.

Logvinenko, E.S. (2023). Legal principles of providing cyber security under the conditions of the state of martial. Retrieved from https://univd.edu.ua/science-issue/issue/5525

Lyzanchuk, V.V. (2017). Information security of Ukraine: theory and practice. Retrieved from https://journ.lnu.edu.ua/wp-content/uploads/2020/11/Lyzanchuk-Informatsiyna-bezpeka-Ukrainy-2017.pdf

Morklyanik, B., Korchenko, O., Kubiv, S., Kazmirchuk, S., & Teliushchenko, V. (2023). The method of phasification of intervals for solving cybersecurity assessment tasks at critical infrastructure facilities. *Ukrainian Scientific Journal of Information Security, 29*(3).

National security and defense council of Ukraine. (2020). Decision of the National Security and Defense Council of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/n0005525-20#Text

Overland, I. (2016). Energy: The missing link in globalization. *Energy Research & Social Science, 14*, 122-130.

Panchenko, O. (2019). Information component of national security. *Bulletin of the National Academy of the State Border Service of Ukraine. Series: public administration, 3*.

Poroshenko, P.O. (2017). Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine dated December 29, 2016 "On the Information Security Doctrine of Ukraine". Retrieved from https://zakon.rada.gov.ua/laws/show/47/2017#Text

Prokopenko, O., Fedorienko, V., & Kulchytskyi, O. (2023). An approach to the identification and analysis of information threats to the national security of Ukraine in the system of strategic communications. *A Collection Of Scientific Works of the Center for Military and Strategic Studies of Ivan Chernyakhovsky National University, 2*(78), 35-43. Retrieved from http://znp-cvsd.nuou.org.ua/issue/view/17206

Ranjan, P. (2023). Russia-Ukraine war and WTO's national security exception. *Foreign Trade Review, 58*(2), 246-258.

Sayler, K.M. (2020). Artificial intelligence and national security. *Congressional Research Service, 2,* 45178.

Shandler, R., Gross, M.L., & Canetti, D. (2023). Cyberattacks, psychological distress,

and military escalation: An internal meta-analysis. *Journal of Global Security Studies, 8*(1), ogac042.

Shlyakhtunov, M.A. (2022). Human Psychological Security In Terms Of National Security. *Specialusis Ugdymas, 1*(43), 2252-2259.

Smolyanyuk, V.F. (2018). System principles of national security of Ukraine. *Bulletin of the National University "Law Academy of Ukraine named after Yaroslav the Wise", 2*(37), 107–123.

Smotrych, D., & Brailko, L. (2023). Information security in the conditions of martial law. *Scientific Bulletin of the Uzhhorod National University. Series: Law, 2*(77).

Titarenko, N. (2024). Is there a special period in Ukraine? Retrieved from https://zakon.rada.gov.ua/rada/show/n0031697-16#Text

Vasylchyshyn, O., Tytor, V., & Kekish, I. (2022). National security of the state: features of provision in the martial law regime. *Economic Analysis, 32*(4), 289-297.

Vlasyuk, A.S. (2016). National security of Ukraine: evolution of domestic policy problems. *NISD National Institute of Strategic Studies.* Retrieved from https://niss.gov.ua/sites/default/files/2017-01/Vlasuk-fin-99d56.pdf

Vonsovych, O.S. (2017). National security of Ukraine in the conditions of modern geopolitical changes. *Scientific Bulletin of the Diplomatic Academy of Ukraine, 24*(2), 18-24.

Zelensky, V. (2022). The Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Strengthening Criminal Liability for the Production and Distribution of Prohibited Information Products". Retrieved from https://zakon.rada.gov.ua/laws/show/2110-20#Text

Legal Foundations of the Application of Combat Immunity in Ukraine, the United Kingdom, and the U.S. of America: A Comparative Legal Analysis

by Yuriy Harust[1], Mykhailo Chalyi[2], Yaroslav Demchyna[3], Ihor Hanenko[4], Vasyl Shut[5]

Abstract. The article analyzes the administrative and legal aspects of the application of the combat immunity institution to exempt military personnel from legal liability for offenses committed in Ukraine, the United Kingdom, and the United States of America. Based on the study of court cases heard by the courts of these countries, legal norms contained in national legislation are identified, which determine the grounds and conditions for applying combat immunity. The history of the implementation of this legal institution, its normative consolidation, and practical application in armed conflict conditions are examined. The main issues and legal conflicts related to the application of combat immunity in the national legislation of the analyzed countries are identified. Suggestions are made on improving the administrative and legal mechanism for applying the combat immunity institution in Ukraine, taking into account international experience.

Keywords: combat immunity, armed conflict, war crimes, military law, exemption of military personnel from legal liability, law of armed conflict, armed forces, Russo-Ukrainian war.

1 Department of Military Law and Law Enforcement, National University of Defense of Ukraine, 03049, 28 Povitryanyi Sil avenue, Kyiv, Ukraine.

2 The Department of Military Law, Military Law Institute, Yaroslav Mudryi National Law University, 61024, 77, Hryhorii Skovorody Street, Kharkiv, Ukraine.

3 Military Law Institute, Yaroslav Mudryi National Law University, 61024, 77, Hryhorii Skovorody Street, Kharkiv, Ukraine.

4 Department of Criminal Procedure and Criminalistics, Odessa State University of Internal Affairs, 65000, 1, Uspenska Street, Odesa, Ukraine.

5 Department of Military Leadership, Military Academy, 65009, 10, Fontanska Road, Odesa, Ukraine.

NAM, Anno 6 – Special Dossier
DOI: 10.36158/97912566922172
Ottobre 2025

Introduction

The Verkhovna Rada of Ukraine has legally defined that the temporary occupation of certain territories of Ukraine by the Russian Federation began on February 19, 2014. Consequently, our country has been in a state of war for 11 years. Throughout this period, especially after February 24, 2022, the Armed Forces of Ukraine and other security and defense sector entities have been actively engaged in combat, while commanders have made management decisions aimed at fulfilling combat tasks, which in some cases could have conflicted with the current legislation of Ukraine.

One of the key issues in conducting military operations to defend Ukraine's sovereignty against the aggressor has been the prosecution of military commanders for decisions they made under combat conditions. This issue has led to a reduction in initiative and effectiveness in decisions made by military commanders while carrying out combat orders, highlighting the need to introduce the institution of combat immunity into national legislation. This article is dedicated to a comparative analysis of the legal norms regulating the application of combat immunity in Ukraine, the United Kingdom, and the United States.

Methodology

The following methods were used in the course of the research:

- Comparative legal method – for comparing domestic legislation on the legal regulation of combat immunity in Ukraine with legal norms in the United Kingdom and the United States.
- Expert evaluations – analysis and incorporation of the opinions of scholars, lawyers, and experts on the norms regarding the application of combat immunity to assess the problematic issues of its application.
- System analysis – examining the studied norms as part of judicial practice when making decisions regarding the application of combat immunity to military personnel and the exemption of commanders from liability.
- Empirical method – for collecting facts regarding the application of combat immunity, their initial generalization, subsequent description of research data, systematization, and classification.
- Formal-legal method – when studying legislative acts regulating the application of combat immunity.

Results

The Verkhovna Rada of Ukraine has legislatively defined that the temporary occupation of certain territories of Ukraine by the Russian Federation began on February 19, 2014, (Verkhovna Rada of Ukraine, 2014) and, accordingly, our country has been in a state of war for 11 years. As is well known, throughout this period, especially after February 24, 2022, the Armed Forces of Ukraine and other entities of the security and defense sector have been actively engaged in combat operations in Eastern Ukraine. Commanders at various levels made management decisions aimed at fulfilling combat tasks, which at times could have contradicted the current legislation of Ukraine. As a result, a number of commanders were held accountable for various offenses, including criminal liability. The reason for this was the absence, in Ukraine's national legislation at the time, of the legal concept of «combat immunity» and the legal mechanism for exemption from responsibility for violations of legal norms protected by law, for individuals who intentionally violated them in the course of fulfilling a combat order.

A vivid example of criminal liability for issuing an order under combat conditions is the court proceedings in the criminal case against Deputy Commander of the Anti-Terrorist Operation (ATO), General Viktor Nazarov, who was accused of committing a crime under Part 3 of Article 425 of the Criminal Code of Ukraine (Negligent Attitude Toward Military Service). General Nazarov gave the order for the aircraft with a parachute assault unit to take off to the city of Luhansk to carry out a combat mission aimed at de-occupying the city. On June 14, 2014, during the approach for landing at Luhansk Airport, the Ukrainian Il-76 aircraft was shot down by Russian military forces. As a result of General Viktor Nazarov's decision, 9 crew members and 40 military personnel from the combined parachute assault company were killed.

The judicial investigation lasted until mid-2021. According to the decision of the first-instance court, the defendant, Viktor Nazarov, was found guilty of committing the crime and sentenced to 7 years of imprisonment. In other words, the head of the military command body was convicted for a decision aimed at the effective execution of a combat mission, made based on the planning of military operations in combat conditions and under tight time constraints. Although all participants in the court session were convinced that General Nazarov had made a lawful and correct decision, directed at fulfilling the combat task, at that time,

there were no legal norms in Ukraine's criminal legislation that could have exempted him from criminal liability.

After 6 years of pre-trial investigations and court proceedings in various instances, on May 21, 2021, the Cassation Criminal Court within the Supreme Court, following the review of the case concerning Viktor Mykolayovych Nazarov, canceled the previously made judicial decisions and closed the criminal proceedings due to the absence of a criminal offense in Nazarov's actions. (Verkhovna Rada of Ukraine, 2021) The Supreme Court overturned the seven-year prison sentence for General Viktor Nazarov in this case and closed the case due to the absence of any criminal wrongdoing. In this way, in 2021, the Supreme Court, by applying criminal law institutions, specifically emphasized that according to Article 42 of the Criminal Code of Ukraine, an act (action or inaction) that caused harm to legally protected interests is not considered a criminal offense if it was committed under conditions of justified risk to achieve a significant socially useful goal. At the same time, the risk is considered justified if the goal could not have been achieved in that situation without the action (inaction) associated with the risk, and the person who allowed the risk reasonably believed that the measures they took were sufficient to prevent harm to legally protected interests.

In our opinion, the Supreme Court, in its decision, effectively arrived at the legal concept of applying combat immunity. However, it was only with the onset of Russia's full-scale invasion of Ukraine that the Ukrainian Parliament made the necessary amendments to the Law of Ukraine «On Defense of Ukraine,» by supplementing it with the definition of «combat immunity.» The basis for introducing this new legal mechanism for exemption from legal liability was the fact that, in February 2022, nearly all of Ukraine's population took up arms to defend its independence. The civilian population began to engage in active armed resistance against the Russian occupation forces, during which numerous violations of established legal norms occurred.

Considering the above, we can assert that, in the context of warfare, the introduction of combat immunity was the correct, logical, and effective decision, which allows us to predict the absence of such unfounded cases in the future, as the criteria for reasonable caution and justified risk during wartime are much broader. However, we cannot ignore the other negative consequences caused by the existence of such criminal cases in society. For example, the prolonged inves-

tigation and prosecution of combat commanders for decisions made under combat necessity lead to a decrease in initiative and the effectiveness of decisions made by other officers due to the threat of criminal liability, unfulfilled aspirations of the relatives of the deceased in their pursuit of what they believe to be justice, and much more. At the same time, combat immunity does not mean unconditional exemption from responsibility; it only pertains to adherence to certain criteria, the development of which remains the responsibility of the judicial system.

According to Article 1 of the Law of Ukraine «On the Defense of Ukraine,» combat immunity is the exemption of military command, military personnel, special police forces of the National Police of Ukraine, volunteers of the Territorial Defense Forces of the Armed Forces of Ukraine, law enforcement officers participating in the defense of Ukraine, individuals defined by the Law of Ukraine «On Ensuring the Participation of Civilians in the Defense of Ukraine,» from liability, including criminal liability, for the loss of personnel, military equipment, or other military property, the consequences of the use of armed and other force during the repulsion of armed aggression against Ukraine or the liquidation (neutralization) of an armed conflict, or the performance of other defense tasks using any kind of weaponry. This immunity applies to situations where the occurrence of these consequences, considering reasonable caution, could not have been predicted when planning and carrying out such actions (tasks), or which are covered by justified risk, except in cases of violation of the laws and customs of war or the use of armed force defined by international agreements, the binding nature of which has been approved by the Verkhovna Rada of Ukraine. (Verkhovna Rada of Ukraine, 1991)

The necessity of introducing legal norms that define the permissible limits of violations of Ukrainian legislation, and most importantly, the conditions and categories of persons who may be exempt from legal liability for offenses committed, was prompted by the rapid development of events during the defense of Ukraine's sovereignty in the context of the Russo-Ukrainian war. In this regard, we note several circumstances that encouraged the Ukrainian authorities to introduce the institution of combat immunity into the Ukrainian legal system. Among them, the key ones are:

1) Numerous instances of harm caused to interests protected by domestic legislation during the use of armed or other force;

2) Fears among military personnel and others regarding possible criminal and other legal liability for certain damages;
3) The difficulty of planning combat operations under conditions of limited information and tight deadlines for decision-making, as well as the frequent necessity for military personnel to show initiative and make urgent decisions to carry out combat tasks in a combat environment;
4) Actions of military personnel during combat operations often bordered on committing a range of military crimes (Baulin, 2023).

Considering this, it can be argued that the Ukrainian authorities, in the context of active hostilities by the Russian Armed Forces at the beginning of the full-scale invasion, sought to resolve the criminal-legal issues arising during the armed resistance of the Ukrainian people in the shortest possible time. Thus, with the Law of Ukraine «On Amendments to the Criminal Code of Ukraine and Other Laws of Ukraine Regarding the Determination of Circumstances That Exclude Criminal Illegality of an Act and Ensure Combat Immunity in Conditions of Martial Law» dated March 15, 2022, No. 2124-IX, Section VIII of the Criminal Code of Ukraine was supplemented by Article 43-1 «Execution of the Duty to Defend the Homeland, Independence, and Territorial Integrity of Ukraine». (Verkhovna Rada of Ukraine, 2022a)

Part 1 of this article stipulates: An act (action or inaction) committed in conditions of martial law or during an armed conflict aimed at repelling and deterring the armed aggression of the Russian Federation or the aggression of another country is not considered a criminal offense, if it causes harm to the life or health of a person carrying out such aggression or causes harm to the protected interests, in the absence of signs of torture or the use of methods of warfare prohibited by international law, or other violations of the laws and customs of war as specified in international treaties to which the Verkhovna Rada of Ukraine has given its consent for binding force. (Verkhovna Rada of Ukraine, 2001)

That is, in Ukraine, in the spring of 2022, a new type of exemption from criminal liability was introduced. At the same time, the circumstance (combat immunity) that excludes criminal liability is not provided by the provisions of the Criminal Code of Ukraine, but by Article 1 of the Law of Ukraine «On the Defense of Ukraine,» which is a certain legal innovation and goes beyond the scope of criminal legislation.

Also, a mandatory condition for the application of Article 43-1 of the Criminal Code of Ukraine, as defined by the provisions of the Criminal Code of Ukraine, is the presence of a state of martial law or a period of armed conflict. At the same time, this legislative act does not formulate these conditions but refers to paragraph 3 of Article 9 of the Law of Ukraine «On the Legal Regime of Martial Law» dated May 12, 2015, No. 389-VIII, which stipulates that in conditions of martial law, a person authorized to perform the functions of the state or local government is not held liable, including criminal liability, for decisions, actions, or inactions whose negative consequences could not be predicted or are covered by justified risk, provided that such actions (inactions) were necessary to repel armed aggression against Ukraine or to eliminate (neutralize) an armed conflict. (Verkhovna Rada of Ukraine, 2015)

Considering the provisions of the aforementioned legislative acts, we can outline the circle of subjects to whom the norms of Article 43-1 of the Criminal Code of Ukraine apply, i.e., those who are not subject to criminal liability due to the application of the legal norms of combat immunity. Thus, these subjects include:

- Officials of military command bodies;
- Military personnel;
- Police officers of the special purpose police of the National Police of Ukraine;
- Volunteers of the Territorial Defense Forces of the Armed Forces of Ukraine;
- Law enforcement officers who, according to their powers, participate in the defense of Ukraine;
- Civilian individuals (citizens of Ukraine, foreigners, and stateless persons lawfully present on the territory of Ukraine) as defined by the Law of Ukraine «On Ensuring the Participation of Civilian Individuals in the Defense of Ukraine» (Verkhovna Rada of Ukraine, 2022b);
- Individuals authorized to perform state or local government functions.

At the same time, part 3 of Article 43-1 of the Criminal Code of Ukraine defines a list of offenses for which the individuals mentioned above are not subject to criminal liability, namely:

- The use of weapons (armament), combat ammunition, or explosive substances against individuals who are conducting armed aggression against Ukraine;
- The damage or destruction of property in connection with this. (Verkhovna Rada of Ukraine, 2001)

The key legal fact here is that individuals who commit these offenses are not exempt from criminal liability, but rather, they are not subject to criminal liability. In other words, we can assert that the commission of the above-mentioned unlawful actions, if carried out in the conditions of martial law or during an armed conflict and aimed at repelling and deterring armed aggression by the Russian Federation or another country's aggression, is not considered a criminal offense, as stipulated by Article 11 of the Criminal Code of Ukraine. Therefore, under no circumstances should an investigator, detective, or prosecutor initiate pre-trial investigations into such facts based on Article 214 of the Criminal Procedure Code of Ukraine. (Verkhovna Rada of Ukraine, 2012) However, despite active combat and the limited number of investigators at the State Bureau of Investigations, the application of the legal mechanism of combat immunity provided by Article 43-1 of the Criminal Code of Ukraine occurs through the release from criminal liability of military personnel via a court decision, following a pre-trial investigation.

For a comprehensive and objective investigation of this issue, we decided to explore the application of combat immunity in other democratic countries. The concept of combat immunity, in one form or another, exists in the legal systems of various countries and indicates that military leadership is not held accountable for actions taken in a combat environment or during military operations. However, the basis for its application is a thorough analysis and determination of the circumstances under which a particular decision was made. (Behunets, 2023) At the same time, we can assert that our analysis of judicial decisions in partner countries regarding the application of combat immunity shows the ambiguity of the legal norms regulating the introduction of the combat immunity institute in these countries.

The analysis of case law in the United Kingdom points to the diversity of judicial interpretation of legal norms concerning the application of combat immunity. Evidence of this can be seen in the cases: *Smith v. Ministry of Defence*, *Ellis v. Ministry of Defence*, and *Allbutt v. Ministry of Defence*, which were opened as a result of lawsuits concerning the deaths and serious injuries of British servicemen during military operations in Iraq. In these legal proceedings, the plaintiffs' claims were related to negligence by commanders, while the defendant, the Ministry of Defence, argued that all claims should be dismissed based on the application of combat immunity norms. The Ministry of Defence referred to the doctrine of combat immunity, which has a sufficiently broad jurisdiction to

cover all actions or omissions by commanders that allegedly led to the death and injury of subordinates during combat operations, and whose foundation rests on the principle that state interests should prevail over individual interests. Consequently, the application of this doctrine should result in the complete exclusion of any responsibility for negligence by commanders in the course of military operations from judicial jurisdiction.

In this case, the judge made a nuanced decision. While he believed that the doctrine of combat immunity should be interpreted narrowly, he partially dismissed the plaintiffs' claims on the grounds that they did not fall under the jurisdiction of the United Kingdom when the soldiers died. However, he upheld the claim regarding the Ministry of Defence's obligation to compensate for the material damages claimed by the plaintiffs. (United Kingdom Supreme Court, 2013)

A completely different decision was made by the court in the case of Richard Mulcahy v. the Ministry of Defence of the United Kingdom. Applying the doctrine of combat immunity, the Court of Appeal ruled that during combat missions and operations, the Armed Forces are not obligated to exercise excessive caution regarding potential losses and injuries among servicemen, and it fully dismissed the claim. (England and Wales Court of Appeal, 1996)

An interesting legal innovation in the UK legislation is the mechanism that grants the Secretary of State for Defence the power to establish combat immunity for servicemen of the Armed Forces through their decision when national security is threatened and during military operations outside the United Kingdom. This applies in cases where the responsibility of military personnel for the death, injury, or harm caused to another person during combat missions and guard duties is to be waived. (Law "On Judicial Cases (Armed Forces)", 1987)

At the legislative level, it is stipulated that the State is not liable for the death or injury of military personnel caused by the peculiarities of the terrain, natural conditions, as well as the condition of aircraft, ships, or military equipment used under special conditions (Law «On Crown Court Jurisdiction», 1947). When applying the aforementioned provisions, only the court can determine the conditions under which immunity does not apply to military personnel. The principle of combat immunity is that military personnel who are directly involved in combat operations (fights) cannot be held liable under general law for negligence, actions, or inactions. This approach is confirmed by the majority of judicial deci-

sions and national legislation of the United Kingdom.

Thus, we can conclude that according to the criminal law doctrine of the United Kingdom, military personnel of the British Army are entitled to combat immunity, which protects this category of individuals from liability for offenses that may lead to negative legal consequences during combat operations. This principle stipulates that holding military personnel accountable for decisions or mistakes made during combat is incorrect, unjust, and unreasonable. At the same time, we can note that the legal mechanism for applying the combat immunity institution in the legislation of the United Kingdom is not flawless. As mentioned above, in certain court cases, the courts claim that the Ministry of Defence of the United Kingdom failed to provide military personnel with the appropriate military equipment that could have prevented their injuries and deaths, and they do not apply the principle of combat immunity. In other cases, it is stated that the damage caused to military personnel occurred due to the conduct of combat operations, and the guilty parties are released from liability, citing the doctrine of combat immunity.

To support our conclusions, Martin Molloy, a special advisor to the Ministry of Defence of the United Kingdom, in his speech at a scientific-practical conference in Ukraine on the application of legal norms of combat immunity, stated that the United Kingdom has not yet been able to regulate the application of combat immunity for military personnel serving within the country, including due to the ongoing internal conflict in Northern Ireland. The legal framework of the United Kingdom provides for a separate system of legal responsibility for military personnel. Legal responsibility for military personnel is part of the general legal responsibility system in the United Kingdom. In the case of a crime committed by a military member, the corresponding investigation is conducted by military justice authorities. (Defense Strategy Center, 2021)

The concept of combat immunity is applied somewhat differently in the United States. Until 1946, any lawsuits against the federal government without its consent were prohibited by the doctrine of sovereign immunity in the U.S. However, this legal position was changed by the Federal Tort Claims Act (FTCA), which can be considered similar to the «Crown Proceedings Act of 1947» in the United Kingdom. The FTCA abolished sovereign immunity in relation to the federal government in most cases. However, according to 28 U.S.C.A. §2680(j),

the sovereign immunity of the federal government is not waived in connection with «any claims arising out of the combat activities of the armed forces or naval forces or the Coast Guard during wartime.». (Federal Law "On Tort Claims")

Another exception, which pertains to «injuries sustained during service,» was introduced through case law and is known in the U.S. as the Feres Doctrine (Feres v United States, 340 U.S. 135 (S.Ct. 1950)) (Speiser et al., 2010). The justification for the Feres Doctrine is quite critical and substantial, particularly regarding military disciplinary structures. According to the Feres Doctrine, the plaintiff cannot demand a civilian court to reconsider military decisions made by commanders if the injured party is a service member (U.S. Supreme Court, 1977), and the plaintiff's claim for damages cannot be upheld. The Feres Doctrine stipulates that a lawsuit cannot be allowed to potentially undermine the foundation of military discipline.

Another case, Chappell v Wallace, involved U.S. Navy service members filing a lawsuit for damages against senior officers, claiming that they were discriminated against due to their race during the assignment of duties and imposition of penalties, violating their constitutional rights. The court dismissed the claim on the grounds that the contested actions were military decisions that were not subject to review, and the defendants were entitled to immunity. Citing the Feres Doctrine, the court ruled that service members could not file claims for damages against senior commanders for alleged wrongdoings. According to U.S. law, the necessity for military commanders to make clear and decisive decisions about their subordinates, as well as the need for the unchallenged actions of the subordinates, cannot be undermined by judicial review within the legal protection that imposes personal responsibility on officers for those they command. Given this, we can state that within the U.S. judicial system, two subsystems coexist: one for civilians and another for service members. (U.S. Supreme Court, 1983)

The «Randulich Rule» also operates in the U.S., which is based on judicial practice in the country. The case concerns the responsibility of commanders for mistakes made during wartime. The tribunal concluded that the decision made by Randulich could be incorrect, but not criminal. As stated in the ruling, «the circumstances under which the commander made the decision justify the necessity of the conclusion made.» The Randulich case serves as the foundation for the general standard regarding commanders' responsibility for decisions made

during combat operations. (Furman, 2022)

The legislative foundation for the provisions of combat immunity is Article 2680 (J) of the U.S. Code, which defines the immunity of the U.S. Government from any claims related to the combat actions of the Army, Navy, and Coast Guard during wartime (U.S. Code, 2023). The main principles of implementing the combat immunity mechanism and addressing the issue of holding commanders and military personnel accountable in the U.S. are contained in the special instruction «Law of Armed Conflict Deskbook» (2024) and in the «Operational Law» handbook (Military Legal Resources, 2022), as well as in judicial decisions. The legal norms outlined in these documents require a thorough analysis and study of all the circumstances under which a commander acted when making the corresponding decision and the regulatory legal documents they followed.

Considering the judicial practice and national legislation of the United States, we can assert that the actions of commanders in the U.S. Army and the decisions they made under combat conditions for applying combat immunity norms are evaluated exclusively based on the information available at the time of making those decisions. At the same time, the U.S. Senate has determined that any decisions made by commanders, military personnel, or other individuals responsible for planning and carrying out military operations (combat actions) must be reviewed exclusively by the court based on information that was reasonably available to the accused at the time of planning, authorizing, and executing military operations. The court should not consider information that became known and accessible after the operation took place.

Therefore, the institution of combat immunity in the United Kingdom and the United States is much more developed than in Ukraine. There is a solid explanation for this, which lies in the time frame of its introduction and, accordingly, in its legal support. However, after examining the legal mechanisms for the implementation of combat immunity in the aforementioned countries, we can note the lack of a unified approach in their national legislation for applying the norms and principles of combat immunity to commanders and military personnel who have committed offenses during combat operations. At the same time, in our opinion, the principle of its application is quite important, when the interests of the state should prevail over the interests of the individual. This principle is crucial for commanders and military personnel when making managerial decisions in com-

bat zones, i.e., under combat conditions. It is important for them to know that their command decisions, aimed at effectively carrying out the assigned combat task, will not lead to legal consequences.

When studying the legal mechanism for the application of combat immunity norms in Ukraine, which has been at war for over 10 years, we note that it is still underdeveloped. At the same time, the use of experience from its application in partner countries also has certain specifics due to the lack of a unified legal approach. In our opinion, the development of the combat immunity institution in Ukraine and its adaptation to the realities of the Russo-Ukrainian war will provide a strong impetus for the introduction of new legal innovations into the established mechanisms of combat immunity application in partner countries.

Based on the results of our research, we propose developing the necessary regulatory and legal framework for the application of the norms of Article 43-1 of the Criminal Code of Ukraine, both with and without the opening of criminal proceedings. This article clearly defines that actions (acts or omissions) that harm the life or health of a person committing aggression, or cause harm to protected interests, committed under martial law or during an armed conflict and aimed at repelling and deterring armed aggression by the Russian Federation or any other country, are not considered criminal offenses (Verkhovna Rada of Ukraine, 2001). Therefore, criminal procedural legislation of Ukraine does not apply to such actions.

Analysis

Analyzing the legal foundations for the application of combat immunity, it can be noted that its introduction in Ukraine was driven by the practical need to protect military commanders and service members from legal prosecution for actions taken during the execution of combat orders. The case of General Nazarov demonstrates the legal uncertainty that existed in Ukrainian legislation until 2022, when there was essentially no legal mechanism in the criminal law of Ukraine for exemption from criminal liability for offenses committed in combat conditions while defending the national sovereignty of Ukraine.

However, despite the introduction of the institution of combat immunity in domestic legislation, one unresolved legal issue remains: for individuals who committed offenses in the conditions of combat operations, the norms of criminal

procedural law are applied to exempt them from criminal liability, even though the act in question, according to criminal law, is not considered a criminal offense. This legal conflict requires further in-depth academic research.

The comparison with the legal systems of the United Kingdom and the United States reveals similar legal mechanisms regulating military responsibility in combat conditions. In the United Kingdom, the principles of command responsibility and military immunity are enshrined in both national and international law. In the United States, there is the Feres Doctrine, which limits the ability of military personnel to file claims against the state for harm incurred during the performance of their duties. Therefore, the introduction of combat immunity in Ukraine represents a logical and evolutionary step in its legal system, aligning with international standards.

Discussion

The introduction of combat immunity in Ukraine marks a significant step in the evolution of military law. This decision helps to enhance trust among military commanders and provides legal guarantees for carrying out combat missions without the risk of unjustified criminal prosecution. However, there are certain challenges related to the potential misuse of such immunity. An important task is the development of control mechanisms to prevent impunity for crimes that violate international humanitarian law.

One limitation of this study is the insufficient empirical base regarding the application of combat immunity in Ukraine, as this legal mechanism is still in its early stages. Future research may focus on analyzing judicial practices following its introduction and examining specific cases where combat immunity was applied or, conversely, was not recognized by the judicial authorities.

Thus, combat immunity is a crucial element of legal protection for military personnel, but its effectiveness will depend on the application of the law and a proper balance between safeguarding service members and adhering to international humanitarian law.

References:

Baulin, Yu.V. (2023). Combat Immunity as a Circumstance Excluding Criminal Liability. Criminal-Legal and Procedural Responses to the Challenges of Martial Law in Ukraine: Materials of the Round Table Held within the Framework of Science Days at the Faculty of Law of the National University of «Kyiv-Mohyla Academy.». 17–24.

Behunets, A.O. (2023). Immunities in Criminal Law of Ukraine.. Retrieved from: https://karazin.ua/storage/static-content/source/documents/aspirantura/zakhysty/behunts/diss_Behunts_AO.pdf

Defense Strategy Center. (2021). Combat Immunity as One of the Guarantees of Protection of Military Personnel's Rights. Retrieved from: https://defence.org.ua/

England and Wales Court of Appeal (Civil Division) Decisions (1996).

Federal Law «On Tort Claims» (FTCA) 28 U.S.C.A. §2680(j). Retrieved from: https://www.law.cornell.edu/uscode/text/28/2680

Furman, V. (2022). Combat Immunity. Overview of Legislative Changes. Retrieved from: https://jurliga.ligazakon.net/news/210201_boyoviy-muntet-oglyad-zmn-do-zakonodavstva

Law «On Crown Court Jurisdiction.» (1947). Retrieved from: www.legislation.gov.uk/ukpga/Geo6/10-11/44/ni/enacted

Law «On Judicial Cases (Armed Forces)» (1987). Retrieved from: www.legislation.gov.uk/ukpga/1987/25/pdfs/ukpga_19870025_en.pdf

Law of Armed Conflict Deskbook. (2024). Retrieved from: https://www.jagcnet.army.mil.pdf

Military Legal Resources (2022). Operational law. Retrieved from: https://www.loc.gov/collections/military-legal-resources/?q

Richard Mulcahy v Ministry of Defence. Retrieved from: www.bailii.org/ew/cases/EWCA/Civ/1996/1323.html

Speiser, S.M., Krause, C.F., and Gans A.W. (2010). The American Law of Torts. Retrieved from: https://lawcat.berkeley.edu/record/1153273

U.S. Code (2023). Title 28 - Judiciary and judicial procedure. Retrieved from: https://www.law.cornell.edu/uscode/text/28

U.S. Supreme Court (1977). Stencel Aero Engineering Corp. v. United States, 431 U.S. 666. Retrieved from: https://supreme.justia.com/cases/federal/us/431/666/

U.S. Supreme Court (1983). Chappell v. Wallace, 462 U.S. 296. Retrieved from: https://supreme.justia.com/cases/federal/us/462/296/

United Kingdom Supreme Court. (2013). Smith & Ors v The Ministry of Defence. Retrieved from: http://www.bailii.org/uk/cases/UKSC/2013/41.html

Verkhovna Rada of Ukraine (2022b) Law of Ukraine «On Ensuring the Participation of Civilians in the Defense of Ukraine.». Retrieved from: https://zakon.rada.gov.ua/laws/show/2114-20#Text

Verkhovna Rada of Ukraine (1991) Law of Ukraine «On Defense of Ukraine». Retrieved from: https://zakon.rada.gov.ua/laws/show/1932-12#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 (2014). Law of Ukraine «On Ensuring the Rights and Freedoms of Citizens and the Legal Regime in the Temporarily Occupied Territory of Ukraine». Retrieved from: https://zakon.rada.gov.ua/laws/show/1207-18#Text

Verkhovna Rada of Ukraine (2015). Law of Ukraine «On the Legal Regime of Martial Law.» Retrieved from: https://zakon.rada.gov.ua/laws/show/389-19#Text

Verkhovna Rada of Ukraine (2021). The decision in the case of V. Nazarov. Retrieved from: https://supreme.court.gov.ua/supreme/pres-centr/news/1123699/

Verkhovna Rada of Ukraine (2022a) Law of Ukraine «On Amendments to the Criminal Code of Ukraine and Other Laws of Ukraine Regarding the Definition of Circumstances Excluding Criminal Wrongfulness of an Act and Ensuring Combat Immunity Under Martial Law.». Retrieved from: https://zakon.rada.gov.ua/laws/show/2124-20#Text

Verkhovna Rada of Ukraine. (2012). Criminal Procedure Code of Ukraine. Retrieved from: https://zakon.rada.gov.ua/laws/show/4651-17#Text

Challenges in classifying violent military offenses

by Ganna Sobko[1], Victoria Shchyrska[2], Kateryna T. Izotenko[3], Andrii Svintsytskyi[4], Yuriy Ponomarenko[5]

Abstract, The article is devoted to the military doctrine of Ukraine, the main task of which is to ensure military security in the Armed Forces and other military organizations by performing special (security) services, namely: combat duty, combat service, border service, punitive service, watch service, public order and public security, internal service, and patrolling in the garrison. The article examines four corpus delicti of criminal offenses, which include: violation of the rules of combat duty (Article 420 of the Criminal Code of Ukraine); violation of the rules of border service (Article 419 of the Criminal Code of Ukraine); violation of the statutory rules of guard service or patrolling (Article 418 of the Criminal Code of Ukraine); violation of the statutory rules of internal service (Article 421 of the Criminal Code of Ukraine). This paper compares the military's awareness of responsibility for violating an order with the expediency of taking into account the legal experience of international criminal tribunals. It also expresses the issue of dualistic legislative regulation of the duty of a serviceman to execute an order received in his address. Furthermore, it analyses the possibilities of resolving the conflict in terms of absolute necessity. Subsequent to this, the authors analyze in detail the corpus delicti of criminal offenses and their legislative constructions, as well as their important features in qualifying a criminal act.

Keywords: military statutory order of service, military duty, military order, criminal offenses.

1 Department of Criminal Law, Criminology and Penalty Law, Odesa State University of Internal Affairs, 65000, 1 Uspenska Str., Odesa, Ukraine.

2 Department of Criminal Law and Criminology, Faculty of Training Specialists for Pre-Trial Investigation Bodies, Odesa State University of Internal Affairs 65000, 1 Uspenska Str., Odesa, Ukraine.

3 «KROK» University of Economics and Law, 03113, 30-32 Tabirna Str, Kyiv, Ukraine.

4 Department of the Criminal Procedure and Criminalistics, Educational and Scientific Humanitarian Institute, National Academy of the Security Service of Ukraine, 03066, 22 Mykhail Maksymovych Str, Kyiv, Ukraine.

5 Department of Criminal Law, Yaroslav Mudryi National Law University, 61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine.

NAM, Anno 6 – Special Dossier
DOI: 10.36158/97912566922173
Ottobre 2025

1. Introduction

Ukraine's military doctrine states that ensuring military security is the most important activity of the state. The main tasks of ensuring military security are to prevent, localize and neutralize military threats to Ukraine. These tasks are solved mainly through the organization of special (security) services in the Armed Forces and other military organizations. These services include: combat duty, combat service, border service, punitive service, watch service, public order and public security, internal service, and garrison patrol (Navrotskyi, 1997).

These types of special military service have a number of common characteristics. Firstly, they are usually related to the performance of combat missions (active duty) and involve the use of physical force, weapons, special means and military equipment, if necessary. Secondly, special services are organized in such a way that they are carried out periodically, within a certain period of time, by changing (duty) units or individual outfits of servicemen, which are separated from military units, subunits. Thirdly, servicemen are in a special legal position during their service - they are out of subordination to their superiors and become subordinate to the officials of the respective outfit, acquire additional rights and obligations related to the nature of the respective service (Judiciary of Ukraine, 2024).

The procedure for performing special services is a component of the procedure for military service (military law and order), and is strictly regulated by military regulations, guidelines, instructions and other normative legal acts. Violations of this procedure pose a serious public danger and can lead to grave consequences. They create conditions for violating the inviolability of the land border, air and sea space, causing damage to the enemy, stealing military property, etc. The most dangerous violations of the order of special services are recognized as crimes.

Crimes against the order of special services include: violation of the rules of combat duty (Article 420 of the Criminal Code of Ukraine); violation of the rules of border service (Article 419 of the Criminal Code of Ukraine); violation of the statutory rules of guard service or patrolling (Article 418 of the Criminal Code of Ukraine); violation of the statutory rules of internal service (Article 421 of the Criminal Code of Ukraine).

The elements of criminal offenses against the order of special services have

a pronounced special character. These are the offenses that are traditionally considered in criminal law theory as offenses with a special subject of a criminal offense. However, the essence of criminal offenses with a special subject is such that they have not only the subject, but also other elements (object, objective and subjective sides) of a special nature.

The main feature of these special elements of criminal offenses, which, in fact, makes the elements special, is the special nature of the relations that act as the main direct object of criminal offenses in Articles 418, 419, 420 of the Criminal Code. These relationships develop and are preserved in relation to the necessity of carrying out certain socially required tasks inside the state's military structure in order to guarantee the state's military security through internal service and guard duty. Special relations are a certain order of behavior and activities regulated by special legal norms that ensure the performance of the relevant functions.

The peculiarity of the analyzed criminal offenses is the presence in their corpus delicti of both "special" objects and "general" objects that act as additional objects. The difficulty in establishing them in these norms is that the relevant social values (life, health, freedom, etc.) are not directly indicated in them. Additional objects in criminal offenses against the procedure for performing special types of military service, which indicate the possibility of violent nature of some of these offenses, are mainly revealed in a detailed analysis of the procedure for performing a particular special service.

The relevant regulations contain rules aimed at ensuring the physical and mental safety of a person. In other words, these criminal offenses against military service, as well as all violent criminal offenses in general, are multi-objective, with physical and mental well-being of a person acting as an additional object. The purpose of this article is to analyze the legislative regulation and to identify gaps and the current state of non-performance or improper performance of duty by servicemen in the course of performing their duties.

2.Methodology

This study examines the subjective elements, specifically the internal attitudes of individuals involved in violent military offenses. The study's primary focus is on the indicators of violence that influence the form of guilt and the range of personnel who may commit these offenses, including guard chiefs, sentries,

scouts, assistant guard chiefs, technical operators, vehicle drivers, and checkpoint guards. Furthermore, the study examines the role of sentries and escorts within military brigades and their responsibilities in the protection of military facilities. Comparative statistical data reveal the prevalence of these offenses across different periods in Ukraine: peacetime prior to 2014, anti-terrorist and Joint Forces operations from 2015 to 2021, and the period following Russia's full-scale invasion from 2022 to 2023. The data demonstrate a correlation between an increase in such offenses and the military situation. Additionally, the research incorporates case examples to illustrate the judicial handling of these cases and suggests legislative amendments aimed at mitigating these criminal offenses among military personnel.

To accomplish this task, the following research methods were used:

- Formal-dogmatic - used in the analysis of Articles 418 of the Criminal Code, 419 of the Criminal Code, 420 of the Criminal Code and Article 421 of the Criminal Code of Ukraine to build the disposition of the article and identify the shortcomings in the legislative construction, on the basis of which proposals for improving the legislation were made;

- The method of hermeneutics was used to interpret and understand the content of the text of legislation;
- A quantitative analysis was conducted to examine criminal cases initiated under Articles 418, 419, 420, and 421 of the Criminal Code of Ukraine. This approach yielded data on the prevalence of these offenses throughout Ukraine, as well as insights into the profiles of the individuals involved. The analysis encompassed the review of sentences issued for these offenses as well as data from the Prosecutor General's Office regarding prosecutions under these articles. This quantitative assessment enabled a structured examination of patterns and trends related to these criminal offenses.
- The sociological method is utilized to examine social phenomena and processes that contribute to the non-performance or improper performance of military duties. This approach provides insights into the underlying social factors that influence these behaviors.
- The comparative legal method is employed extensively for the purpose of analyzing the composition of criminal offenses and identifying conflicts and gaps within military and criminal law. This method entails the comparison of per-

tinent legal frameworks across diverse branches of law, with a particular emphasis on delineating the responsibilities of parents and guardians - or those acting in a parental capacity - in the event of their absence or unavailability. This approach illuminates potential avenues for legislative adjustments that could enhance clarity and consistency in legal responsibilities.

3.Results

In order to gain a deeper understanding of these articles, the authors propose a new approach to the analysis of their statistical data, which is outlined in the following sections:

1. Before the beginning of Russia's military aggression against Ukraine in 2014;
2. During the ATO and JFO (Anti-Terrorist Operation and Joint Forces Operation), which lasted 8 years from 2015 to 2021;
3. The last indicators, which relate specifically to the time of Russia's full-scale invasion of Ukraine (martial law).

Statistics for 2014 are unavailable, preventing examination and comparison with this category (Judiciary of Ukraine, 2024). However, martial law and the percentage of criminal offenses committed is increasing.

Given the volume and complexity of the data provided, the court statistics for Articles 418, 419, and 426-1 for 2021 and 2022 are presented (Table 1.), (Judiciary of Ukraine, 2022).

Table 1. Summary of court statistics for Articles 418, 419, and 426-1 of the Criminal Code of Ukraine (2021–2022)

Cases	Descriptions of Violations					
	Guard Service (Art. 418)		Border Service (Art. 419)		Excess of Power by Military ()Art. 426-1)	
	2021	2022	2021	2022	2021	2022
Pending	1	1	1	3	47	41
New	0	0	0	2	13	13
Considered	1	2	0	3	15	3

Sentences passed	0	0	0	2	13	3
Guilty verdicts	0	0	4	0	6	0
Closed	0	0	0	0	1	1
Unresolved	2	3	3	3	35	39

Table 1. allows for clear visualization of data across the two years for each article, highlighting both the availability of statistics and providing easy comparability between years. A review of the data in the chart reveals that there are no recorded cases for Articles 420 and 421, indicating that there are no cases currently pending in court. In contrast, Articles 418 and 419 indicate a relatively low number of recorded offenses, which suggests a low incidence of violent criminal offenses. In peacetime, the number of criminal offenses was reported to be zero. However, the statistics for Article 426-1 of the Criminal Code are noteworthy in that they reflect an increasing trend in military service-related criminal offenses since the onset of the ATO and the JFO. A comparison of the indicators from the period of martial law with those from earlier measured times reveals an upward trend in offenses. In contrast, the rates observed during the ATO and JFO periods demonstrate minimal variation.

This pattern is consistent across all analyzed indicators, with the exception of the number of verdicts issued, which decreased by half during martial law. This decline may be attributed to the fact that many offenders are currently engaged in combat or because of the increasing caseload in the courts. However, these factors do not impact the challenges related to the accurate qualification of these offenses, which will be examined next. This trend underscores the relevance of the topic being studied.

3.1. Specificity and subjectivity of war crimes.

In the context of discussions pertaining to military accountability and the legal implications of orders issued within a military hierarchy, it is imperative to consider a range of perspectives drawn from international legal doctrine. It is worth noting the presence of a particularly rational viewpoint articulated in foreign legal scholarship. This perspective posits that conferring absolute rehabilitative status upon military orders would represent a significant misstep by legislators. Such

an approach would imply that the Supreme Commander-in-Chief, as the highest authority within the military hierarchy, would bear responsibility for all crimes committed under their command, thereby undermining the principle of individual accountability (Figure 1.), (Cassese et al., 2013). This notion gives rise to critical questions concerning the balance between obedience to orders and the legal and moral obligations of military personnel.

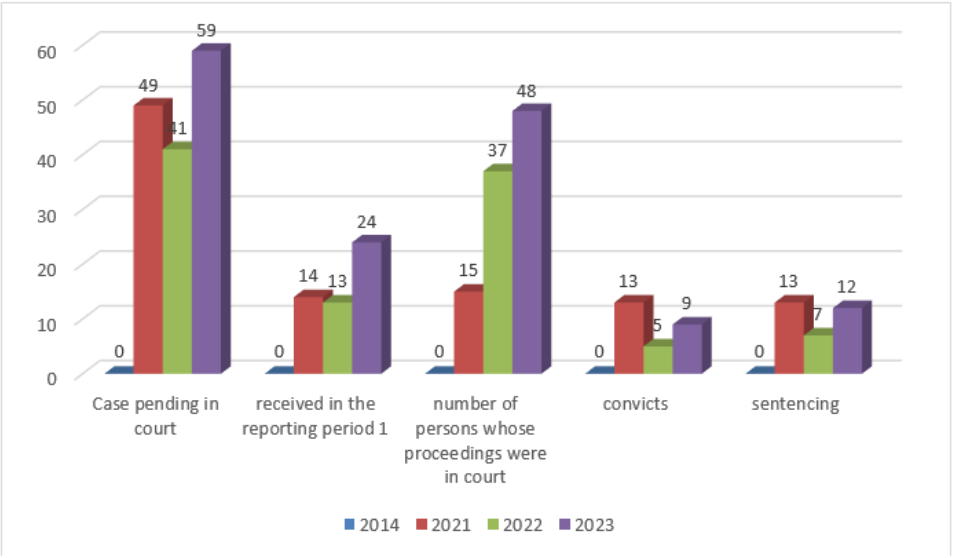


Figure 1. Dynamics of committing military service criminal offenses

Based on Figure 1., it is important to notice that the case count includes separate incidents or offenses related to the same individual or group. Given the fact that in Ukraine it is hardly appropriate to talk about the existence of an established law enforcement practice on the issue under consideration and the uncertainty regarding the subjective component, in the context of the serviceman's awareness of the illegality of the order addressed to him, it is advisable to take into account the legal experience of international criminal tribunals. The most problematic issue in practice is whether the perpetrator was aware of this circumstance, which is of key importance (Sobko et al., 2023a; Hutnyk, 2016).

The procedure for military service can be categorized as either general or special. According to the Judiciary of Ukraine (2023), the general procedure, which encompasses general military relations, is applicable to all servicemen. In contrast, the special procedure involves specific military relations that are established

in particular areas of military service activity and pertain to the fulfillment of certain tasks. This special procedure is not applicable to all servicemen but rather to specific categories of personnel. It is crucial to differentiate between the general and special procedures for military service when establishing the framework for criminal offenses against military service. Some criminal offenses contravene the general procedure, while others contravene the special procedure. The former include, in particular, criminal offenses against the order of subordination and military statutory relations (Articles 404 - 406 of the Criminal Code of Ukraine), (Verkhovna Rada of Ukraine, 1992).

In order to provide a clear definition of the a priori criminality of acts committed by a serviceman while following an order, it is necessary to define these acts in the following way:

- killing captured members of opposition armed forces and/or civilians in the occupied territory;
- torture of captured members of armed groups and/or civilians (the entire range of accompanying circumstances is taken into account, the context of inflicting pain, the tools used, the physical condition of the victim, etc.);
- ill-treatment of prisoners of war by members of armed groups and/or members of the civilian population (meaning the provision of insufficient food, inadequate medical care and conditions for meeting basic human physiological needs);
- intentionally causing serious bodily injury or harm to health;
- taking hostages from among members of armed groups and/or representatives of the civilian population;
- sexual acts of a violent nature;
- the use of “indiscriminate” weapons, military equipment and other means in an armed conflict to harm the enemy, if the use of such means may result in “unnecessary” suffering or damage;
- intentional attacks on civilians (the prohibition of these actions is interpreted as an indisputable absolute, the diminution of which cannot be explained by any military needs);
- attacking or shelling unprotected settlements that are not military targets (Panov, 2006)

According to these decisions, it is about the occurrence of such harmful consequences that cause a strong destructive effect on the human body, its appearance or emotional background. In this case, the said harm must prevent a person from normal, full-fledged life activities for a long time. In general, the consequences of such crimes include damage to both the main and additional objects of the crime. For example, the grave consequences of violating the rules of public order and public security service may simultaneously include harm to the victim's health, disorganization of this service, and failure to perform a combat mission. A special act in Articles 418, 419. 420, 421 of the Criminal Code of Ukraine is an act related to the violation of duties stipulated by the relations on performing special types of military service (which form a special object of a criminal offense). The special consequences of these criminal offenses are the damage caused to the values protected by the criminal law in the form of violation of special relations (the procedure for performing special types of military service) that ensure the safety of these values (Karpenko, 2019)

The particular and subjective aspects of special offenses pertain to the infringements of the regulations that govern the performance of specific types of military service. Signs of the subjective element - guilt, motive, purpose, emotions - reflect the subject's mental attitude to the act and its consequences. The form of the subjective element is the same for all criminal offenses - these are mental processes; however, the content of the subjective element of each criminal offense is specific, its features reflect the specifics of the object, act, consequences and other circumstances.

The content of the subjective side in the special corpus delicti of criminal offenses in Articles 418-421 of the Criminal Code is determined by the special object, special nature of the action and consequences. The perpetrator mentally reflects these special circumstances and therefore his/her guilt (in some cases, motive and purpose) are also special. In the literature, the subjective side of these criminal offenses is disclosed in different ways. In particular, some authors point out that the very violation of the rules in Part 1 of Art. 418, Part 1 of Art. 419, Part 1 of Art. 420 and Part 1 of Art. 421 of the Criminal Code of Ukraine is intentional, and the attitude to the consequences is characterized by negligence.

Other authors believe that some criminal offenses are committed intentionally, others - recklessly, but the attitude to the consequences of the committed viola-

tions may be reckless or indirect intent. Pursuant to Article 24(2) of the Criminal Code, if the legislator does not specify the form of guilt in the articles, then the crime can be committed both intentionally and negligently. With this in mind, in the articles of Section 19 of the Criminal Code of Ukraine, where the form of guilt is not specified, and the terminology used allows for both intent and negligence, both forms of guilt are possible.

Otherwise, if there are any doubts about the essence of the order given and its legality, they should be interpreted in favor of the subordinate, which naturally follows from the general responsibility of the superior for this, as well as from the fact that the subordinate does not have all the information necessary to decide on the legality of the order. At the legislative level, there is no possibility of preliminary collection and analysis of such data, and the serviceman must immediately and unconditionally execute the order addressed to him (Sobko et al., 2023b). Thus, a dualistic situation arises: on the one hand, the obligation of a serviceman to execute an order received in his address is absolute, at the same time, a serviceman, being, first of all, a citizen of the state, must strictly comply with the provisions of criminal law, refraining from taking a criminal path, both by order and in its absence (Chervyakova, 2019; Shkuta, 2020).

In the absence of any alternative models of behavior, except for the execution of an illegal order, the actions of a serviceman should be such that the harm that occurred was less significant when compared to that which would have been caused by his other behavior. The rationality of this proposal is questionable. Such a dilemma should not exist at all, and a subordinate should not, under any circumstances, follow an illegal order. Any authority is based on its legal basis and legal limits of operation. If an authorized entity exceeds the limits of its competence and gives a clearly illegal order, the subordinate is not obliged to follow it. If he does otherwise, the mechanism of legal liability comes into play (Korystin, 2022).

In violations of the rules of guard duty and internal service, damage to the physical and mental well-being of a person is always caused, i.e., these additional objects are optional. For example, most violations of the rules of service (sleeping during military service, leaving a sentry's post, stealing protected military property, etc.) are not related to violent acts. Hence, violations of the rules of service are fully treated as violent offenses, unlike criminal offenses against the

order of statutory relations between servicemen, in which violence is the main, essential feature (Morozyuk & Sobko, 2022).

The distinctive characteristics of the procedures for performing specific types of military service have a profound impact on the actions of personnel within these formations. In special units, violations are primarily the result of breaches of established relationships and duties. Therefore, the acts perpetrated in these contexts tend to exhibit similarities, frequently manifesting as violations of specific responsibilities and conduct rules. For example, criminal offenses delineated in Articles 418, 419, and 420 of the Criminal Code - including sleeping while on duty, leaving one's post, and using violence - are illustrative of a failure to adhere to the protocols of a particular service (Dmytrenko, 2020).

In the corpus delicti of criminal offenses against the procedure for performing special types of military service, the subject is usually named. For example, in Article 418 of the Criminal Code, the subject of a criminal offense is a person who is a member of a guard (watch), such servicemen include: the chief of the guard, sentries, scouts, assistant chief of the guard (if any), assistant chief of the guard for technical means or change of operators (if necessary), vehicle driver, and checkpoint guards. The guard at the brig also includes sentries and escorts. For the direct protection and defense of facilities, the following sentries are posted as part of the guard.

In criminal offenses against the procedure for performing special types of military service, violence is the result of a violation of the established rules for performing a particular special service and is manifested, as a rule, in the unlawful use of physical force, weapons, special means (equipment). The use of violence in these crimes has features characteristic of other criminal offenses against military service, as well as some general criminal violent crimes. In this regard, in theory and in practice, questions often arise as to the distinction between these acts. A study of court practice in this category of cases shows that the issues of distinguishing criminal offenses against the procedure for performing special types of military service committed with the use of violence from violations of the statutory rules of relations between military personnel in the absence of subordination and abuse of authority, as well as from certain violent crimes against the person are very relevant.

3.2. Qualification of war crimes and violation of the rules of statutory relations between military personnel.

When qualifying military violent crimes, situations often arise when the offense has signs of violation of the rules of special types of military service (Articles 418-421 of the Criminal Code of Ukraine) and violation of the statutory rules of relations between military personnel in the absence of a relationship of subordination (Article 406 of the Criminal Code of Ukraine). For example, a company day officer uses violence against a serviceman who does not fulfill the requirements of the persons on duty (for example, to go for physical exercises, etc.). There are several ways to qualify such cases.

Violations of the rules of special types of military service may occur along with other criminal offenses. In a number of cases, the assessment of one criminal act containing signs of different crimes (ideal aggregate, i.e., part 2 of Article 33 of the Criminal Code of Ukraine) caused difficulties. The most difficult to qualify are acts that can be committed by both private and public officials who use their official powers, although the dispositions of the relevant articles of the CC do not mention this. The literature suggests that when such criminal offenses are committed by officials, the ideal combination of such offenses with the relevant criminal offenses against the interests of the service should be stated, provided that the offense, of course, has all the elements of the relevant official criminal offense, since the act harms two independent main objects.

As a general rule to be followed, the following should be borne in mind:

The commission of any unlawful act (embezzlement, violation of statutory rules of relations between servicemen, etc.) can simultaneously form the elements of a criminal offense of this category only if the perpetrator violated the rules of a special type of military service, the task of which was to prevent the harmful consequences. The ideal set of criminal offenses is evidenced by the encroachment on various direct objects and the infliction of real damage to each of them".

It is necessary to clearly establish a system (set) of rules for the performance of special types of military service. In this regard, these rules should have a special purpose, i.e., correspond to the goals set for a particular special service. As noted, the criminal law independence of blanket rules is achieved by including in them the entire scope of rules contained in a specific sectoral source, but only those that reflect the special purpose of the rule, which is determined in relation to

the object of protection. Violation of rules that have a special purpose, i.e., that do not ensure the fulfillment of the tasks of certain types of special services (units), should be qualified if there are appropriate grounds from other articles.

In this regard, it is important to clarify whether the general rules of relations between servicemen are included in the system of rules governing the procedure for performing special types of military service. An analysis of the relevant legal sources from this perspective shows that the general rules of relations between servicemen established by the Statute of the Internal Service of Ukraine are not included in the system of special rules for performing a particular special service. This means that special rules of service, for example, patrolling and internal service, guard service, do not regulate the procedure of relations between servicemen, which is referred to in Article 406 of the Criminal Code. Violation of the general order of relations between servicemen, which does not directly ensure the solution of the tasks of special types of military service, cannot be considered as a violation of the order of performance of a particular special service protected by Articles 418-421 of the Criminal Code.

The foregoing allows to state that in cases where a serviceman who is a member of a particular service commits a violation of the general rules of statutory relations between servicemen (in particular, uses violence), his actions, if there are appropriate grounds, should be qualified under Article 406 of the Criminal Code. This position is also shared by some judicial officers. In accordance with Article 406 of the Criminal Code of Ukraine, the defendant was found culpable of having thrown the individual to the floor while on a daily patrol in his company for presenting claims against him in the service in an unreasonable manner. As a result of hitting the floor, the individual sustained a closed head injury with a fracture of the bones of the vault and the base of the skull, which constituted serious bodily harm. In light of the fact that the defendant's actions fully encompassed the elements of the crime as defined in Part 3 of Article 406 of the Criminal Code, the court excluded Article 421 of the Criminal Code from the defendant's charges.

The proposal to qualify such situations as a set of crimes under Articles 418-421 and 406 of the Criminal Code does not seem to be quite successful for other reasons. In particular, its implementation leads to a de facto double treatment of the same circumstances. Thus, one of the grounds for qualifying the use of violence under Articles 418, 420 and 421 of the Criminal Code is the infliction

of certain physical consequences (physical pain, bodily harm, etc.). In fact, these same actions (use of violence) and consequences (physical harm) are also attributed to the said serviceman when assessing their behavior under Article 406 of the Criminal Code. This state of affairs clearly contradicts Part 3 of Article 2 of the Criminal Code (no one may be held criminally liable for the same act more than once).

The use of violence in some cases can be a type of violation of special rules of certain types of military service. These are situations where one of the tasks of a special service is to protect military personnel (guard (watch) service), ensure personal safety, protect human and civil rights and freedoms (combat duty), and ensure compliance with internal regulations (daily duty). Violation of such rules is usually expressed in the unjustified use of physical force or weapons, sometimes other special means. The physical consequences resulting from the use of violence are covered by the relevant articles of Section 19 of the Criminal Code of Ukraine, since the prevention of these consequences (along with others) is established by a particular special service.

Thus, the following special rules of qualification can be formulated:

a) violation of the general rules of statutory relations between servicemen in the course of performing special types of military service, which involves the use of violence, should be qualified, if there are appropriate grounds, only under Article 406 of the Criminal Code of Ukraine;

b) violation of special rules of military service intended for the protection of servicemen (guard (watch), ensuring compliance with internal regulations (daily duty), expressed in the unjustified use of physical force, weapons and other special means, should be qualified under Articles 418, 419 and 421 of the Criminal Code of Ukraine. In theory and in practice, the question of qualifying the unlawful use of weapons by a person who is a member of a guard is difficult to answer when such actions result in harm to the life and health of third parties. For example, a sentry, having detected an offender on the territory of the post, uses weapons against him in violation of the relevant provisions of the Statute of the Armed Forces of Ukraine (in particular, does not stop him with a shout “Stop, get back” or “Stop, go to the right (left)”, does not warn the offender with a shout “Stop, I will shoot” or does not make a warning shot upwards). As a result of such actions, the offender may suffer death or harm to

health of varying severity, including intentionally. In this regard, the question arises as to whether the offense committed by the guard should be qualified as a criminal offense under Article 418 of the Criminal Code and the relevant articles of Section II of the Criminal Code, or whether everything is covered only by the provisions of the chapter on crimes against life and health (Bogutsky, 2006).

In Article 418 of the Criminal Code, the main direct object of the criminal offense is the order of guard duty. This object is a certain system, the structure of which consists of persons who are members of the guard and objects for which or in connection with which this type of security service is established. Damage to this object of a criminal offense is manifested primarily in the damage to the objects protected by the guard. Accordingly, the grave consequences referred to in Art. 418 of the Criminal Code must necessarily be associated with "guarded objects", the security of which is the purpose of guard service. The Statute of the Garrison and Guard Services of the Armed Forces of Ukraine does not include such goods as the life and health of third parties (including offenders) as "objects protected by the guard".

This implies that harm to the life and health of an unauthorized person as a result of a violation of the procedure for the use of weapons is not covered by the concept of "grave consequences" in Article 418 of the Criminal Code and should be qualified as a relevant criminal offense against life and health (of a person). The exception will be cases when a sentry (outgoing) causes harm to the life and health of persons in the guardhouse or in a disciplinary military unit, since ensuring the safety of these persons is one of the purposes of organizing the guard service (as discussed in subsection 2.3.).

This is in accordance with the established position of court practice. The court found Sergeant guilty of the aforementioned offenses, in addition to other criminal acts, in violation of Article 418 of the Criminal Code of Ukraine. This resulted from the Sergeant's failure to adhere to the established rules and regulations governing the performance of guard duties, which ultimately led to significant and adverse consequences. As stated in the verdict, the accused was on guard duty in May 2007 as part of the garrison guard. During this period, he perpetrated multiple assaults against two other servicemen, including an attack on a sergeant. Subsequently, while under the influence of alcohol, the accused perpetrated the

fatal shooting of Private one of the servicemen with an assault rifle. The investigative authorities and the court, in addition to the aforementioned charges under the Criminal Code of Ukraine, classified the accused's illicit actions under Article 418 as a contravention of the statutory rules of guard service that resulted in severe consequences. In its cassation ruling, the panel underscored that the essential element of this criminal offense is not merely any violation of the statutory rules of guard service, which the accused indisputably committed, but specifically those violations that resulted in damage to the protected objects. The case did not establish that the accused's unlawful actions caused any damage to the protected objects of the guard, which included the accused himself.

In consideration of the aforementioned factors, the panel reached the conclusion that the elements of the criminal offense as defined in Article 418 were absent in the accused's actions. As a result, the verdict in this regard was annulled, and the criminal case was terminated (Supreme Court of Ukraine, 2023). A comparable resolution was reached in a separate case. The warrant officer, who was on duty as a park guard and was issued a pistol. After obtaining authorization from the commanding officer, the guard proceeded to his residence in the evening and made a stop at an officers' café along the route back, where he began to consume alcohol with his colleagues. Subsequently, in flagrant violation of public order, the guard initiated physical contact with citizens, grasping their clothing, and then discharged several rounds from the firearm at the floor. One of the bullets struck a bystander in the leg, causing a minor injury.

The pre-trial investigation authorities classified the actions of the guard under Part 3 of Article 296 and Article 421 of the Criminal Code of Ukraine as hooliganism and a violation of the statutory rules of internal service. In reaching the conclusion that the actions in question did not constitute a criminal offense under Article 421 of the Criminal Code, the court correctly stated that, according to the law, liability under this article is only applicable if there are consequences that the daily patrol on internal service is responsible for preventing. As there was no damage to the internal order in the park and no disruption to the duties of the relevant unit, there were no grounds for holding the guard additionally accountable under Article 421 of the Criminal Code of Ukraine (Kyiv District Administrative Court, 2020). In the general doctrine of official criminal offenses, it is generally recognized that, along with general criminal offenses in office in Chapter 17 of the Criminal Code of Ukraine, other chapters contain special corpus delicti. The

latter are committed by certain officials or in a certain area of activity specified in the law.

The literature suggests the following types of special official criminal offenses:

1) criminal offenses committed only by officials specially identified in the dispositions of articles (e.g., Article 206 of the Criminal Code of Ukraine, etc.)
2) criminal offenses committed with the "use of official position", as indicated in the dispositions (Article 151, Article 182 of the Criminal Code of Ukraine, etc.)
3) criminal offenses that name as perpetrator a specific entity whose rights and duties are of an official nature - a member of an election commission; a person who was responsible for compliance with safety and labor protection rules, etc. (Articles 158-3, 172, 137, 218, 219-1, etc.)
4) criminal offenses in which the subject is not named, but the nature of the action itself, which can only be committed by an official (Art. 168, Art. 372, Art. 371, etc.)
5) criminal offenses that can be committed by both officials using their official position and private individuals.

In all these cases, there are problems of competition of norms and qualification of service criminal offenses in the aggregate (ideal aggregate) with other criminal offenses.

The criminal law literature unanimously states that competition of norms occurs in cases where one criminal offense (as opposed to an aggregate) is committed, which falls under (contains features of) two or more norms, but only one of them is subject to application precisely because one criminal offense has been committed. At the same time, the question always arises as to which of these norms should be applied to qualify the offense. The rule developed by the general theory of law, namely - *lex speciali degorat legi generali* - a special law cancels the effect of a general law - was not enshrined in the Criminal Code of 2001, but the draft of the new law of Ukraine on criminal liability already provides for its legislative enshrinement.

Specialized literature distinguishes two types of special rules based on the object of criminal legal protection: a) special rules which have the same main object of protection as general rules (single-object rules); b) special rules whose

object of protection differs from the object of the relevant general rules (two-object rules). Of course, it would be quite reasonable to distinguish another type of special rules on this basis - special rules with a "mixed" (complex) object of criminal legal protection. Such rules should include Articles 418-421 of the Criminal Code. These articles protect the procedure for performing a particular type of special military service, which ensures the security of protected objects. An integral part of this procedure is the managerial activity of the relevant military officials who are part of a particular outfit. In these military criminal offenses, the interests of managerial activity cannot be considered as additional objects, since without management, military service in general, including its special varieties, is unthinkable. This aspect of the allocated type of special norms is not taken into account both in the works devoted to the problems of qualification of service criminal offenses and in judicial practice (Navrotskyi, 1997).

In cases where general and special norms are in competition, it is proposed that the following approach be taken: when the actions of an official exhibit characteristics of a general crime against the interests of the service and its special type, or when such a general criminal offense is clearly indicated by the meaning of the norm, the general norm should be applied. In such cases, the service in question, or its specific type, constitutes a special type of criminal offense that explicitly allows for its commission by an official in conjunction with other subjects. Alternatively, the possibility of such commission is clearly implied by the meaning of the norm itself (Us, 2018). In cases where the articles specifically provide for liability for crimes committed with the use of official position, it is proposed to qualify only under these articles without combining them with articles providing for liability for official crimes.

The special features of Articles 418-421 of the Criminal Code of Ukraine in comparison with the general norm (Article 364 of the Criminal Code) and the special norm (Article 426-1 of the Criminal Code) are, firstly, a special circle of military commanders (persons who are members of certain outfits), and secondly, a certain sphere of managerial activity - the performance of special types of military service. The specificity of these types of military service lies in the fact that military officers, while performing them, have a dual official status:

a) general - rights and obligations that they always have in connection with their official functions;

b) special - rights and obligations that they are endowed with only during the period of special service.

The issue of the correlation between general and special rules of military service and the relevant qualification rules was discussed above. It is clear that the proposed solutions are fully applicable to the cases under consideration: the abuse of general official powers by military commanders falls under Article 426-1 of the Criminal Code of Ukraine, and the abuse of special official powers - under Articles 418-421 of the Criminal Code of Ukraine. The above allows to formulate the following qualification rule.

Actions: if the actions of a military official resulted in a violation of the rules of special service related to the abuse of special official powers rather than general ones, the act should be qualified under the article providing for liability for violation of the procedure for performing this service. In judicial practice, difficulties arise in qualifying the unlawful use of weapons by a superior during the performance of special types of military service. The literature and court practice suggest that such actions should always be qualified as a military service criminal offense, i.e., under Article 426-1 of the Criminal Code of Ukraine.

The correct solution to this issue should be based on the following provisions: a) the use of weapons is a part of the power (organizational and administrative) functions of a military official; b) the grounds and procedure for the use of weapons in the conditions of military service are regulated by the general rules of the Disciplinary Statute of the Armed Forces of Ukraine. The above rules for qualifying the actions of military officials in the competition between general and special rules are fully applicable to this situation. Thus, if a military officer, while performing special types of military service, violates the general procedure for the use of weapons, his/her actions, if there are relevant signs, should be qualified under Art. 426-1 of the Criminal Code.

4.Discussion

Based on the above, the following special rule of qualification can be formulated: violation of the rules of special types of military service, which was expressed in the unlawful use of weapons by a military official, should be qualified as abuse of power (Article 426-1 of the Criminal Code of Ukraine) only if the use of weapons

was violated. In cases where special rules for the use of weapons while on duty are violated, the act should be qualified under Articles 418, 414 and 420 of the Criminal Code.

The use of violence in case of violation of the rules of special types of military service can cause various physical consequences: pain, damage to health, death, restriction of liberty. The problem of establishing the scope of physical consequences in the concept of "grave consequences" (Articles 418-421 of the Criminal Code) has already been considered in this paper.

Within the framework of this issue, it is advisable to dwell on the main conclusions made earlier:

1) in part 1 of Art. 418 of the Criminal Code of Ukraine, the damage to the objects protected by the guard, covering such grave consequences, should be limited to several persons
2) the scope of physical harm in Article 421 of the Criminal Code covers only intentional infliction of grave harm,

As it can be seen, the consequences of the use of violence in criminal offenses against the order of special types of military service are not always fully covered by the relevant corpus delicti. In the literature and court practice, it is proposed to qualify such cases under a set of criminal offenses. For example, the Review of Court Practice in Cases of Criminal Offenses Against Military Service and Some Official Criminal Offenses Committed by Military Personnel (2001) emphasizes that under certain conditions, criminal offenses under Articles 418, 419, 420 and 421 of the Criminal Code of Ukraine may also form criminal offenses against life and health. This method of qualifying complex violent criminal offenses is very common and is due to a number of circumstances.

Firstly, in articles that do not use the term "violence" and its derivatives ("violence dangerous to life and health", "violence not dangerous to life and health", etc.), but the crime itself allows for the use of violence as an alternative, the sanctions reflect the social danger of not all forms of violence, but only some of its varieties. In general, the discussion focuses on inflicting physical pain, light bodily injuries, and sometimes of moderate severity, restraint of liberty, for example, Articles 120, 180, 137, 164, 258 of the Criminal Code, etc. At the same time, the literature notes that in some of these cases, the scope of violence is limited to putting the victim in a helpless state, as well as a slight restriction of his or her

freedom (Articles 120 and 180 of the Criminal Code). Secondly, even in those cases where the corpus delicti of criminal offenses contain the element of "violence" (or its derivatives), the determination of the amount of physical harm is significantly influenced by the comparative severity of the sanction for a criminal offense committed with the use of physical violence and the sanctions in Articles 121, 122, 127, 146 of the Criminal Code, including for qualified corpus delicti of these criminal offenses.

Analysis from this perspective of the current legislation shows that in most cases the attribute of "violence" covers infliction of moderate bodily harm without additional qualification under Article 122 of the Criminal Code, in particular, Articles 262, 308, 314, 303, 364, etc. Infliction of grievous bodily harm in such criminal offenses, as a rule, requires additional qualification under Article 121 of the Criminal Code, especially if the offense has the qualifying circumstances provided for in this Article. Thirdly, the attribute of "violence" never covers the intentional infliction of death. Here, qualification under Article 115 of the Criminal Code of Ukraine is always mandatory. This traditional rule of qualification of complex violent criminal offenses is due to two circumstances: first, the exceptionally high public danger of murder compared to other criminal offenses, and second, the exceptionally severe punishment of the latter (long terms of imprisonment) is not found for other violent criminal offenses.

5. Conclusions

In consideration of the aforementioned points, the following qualification rules are proposed: In cases of medium gravity crime (Article 122 of the Criminal Code of Ukraine) and grievous bodily harm (Article 121 of the Criminal Code of Ukraine), the violation of the statutory rules of guard duty committed with the use of violence does not necessitate additional qualification. Similarly, in cases of causing moderate bodily harm (Article 122 of the Criminal Code of Ukraine) and serious harm to health (Article 121 of the Criminal Code of Ukraine), the violation of the rules of service for the protection of public order and ensuring public safety committed with the use of violence does not require additional qualification. A violation of the statutory rules of internal service and patrolling committed with the use of violence does not necessitate additional qualification in

cases of medium gravity crime (Article 122 of the Criminal Code of Ukraine) and grievous bodily harm (Article 121 of the Criminal Code of Ukraine). Conversely, the intentional infliction of death as a result of a violation of the rules of special types of military service requires additional qualification under Article 115 of the Criminal Code of Ukraine.

The use of violence by persons during the performance of special types of military service should be qualified under Articles 418, 419, 420 and 421 of the Criminal Code only when the general rules of relations between military personnel are violated, and not the special rules established in the norms regulating the procedure for performing a particular military service. The abuse of authority by military commanders who are members of the squads, which resulted in the use of violence, including weapons, is assessed as a criminal offense against the order of performing special types of military service only in case of violation of special duties provided for the organization of performing a particular special military service. Establishment of the scope of physical harm in criminal offenses against the order of performance of special types of military service, which does not require additional qualification in conjunction with criminal offenses against life and health, is largely due, among other circumstances, to the comparative severity of sanctions for military criminal offenses and relevant criminal offenses against life and health of Ukraine.

References

Bogutsky, P.P. (2006). The right of military service in the context of the realization of military duty by citizens.In *Actual Problems of Theory and History of Human Rights, Law and State: Materials of the 4th All-Ukrainian Scientific Conference of Lawyers-Beginners* (pp. 104-111). Odesa: Yurydychna Literatura.

Cassese, A., Gaeta, P., Baig, L., Fan, M., Gosnell, C., & Whiting, A. (2013). *Cassese's International Criminal Law*. Oxford: Oxford University Press.

Chervyakova, O. (2019). *Work program of the discipline "Military Law"* Kyiv: The National Defense University of Ukraine.

Dmytrenko, N.A. (2020). Crime in the Armed Forces of Ukraine. *InterConf*, *15*, 166-169.

Hutnyk, V.V. (2016). *Procedural rights of participants of international armed conflicts in international criminal courts*. Lviv: Ivan Franko National University of Lviv.

Judiciary of Ukraine. (2022). No. 1-k Report of the courts of first instance on consideration of criminal proceedings. Retrieved from https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2022

Judiciary of Ukraine. (2023). No. 1-k Report of the courts of first instance on consid-

eration of criminal proceedings Retrieved from https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2023

Judiciary of Ukraine. (2024). Form 1: Report of the courts of first instance on the consideration of cases in criminal proceedings. Retrieved from https://court.gov.ua/inshe/sudova_statystyka/lkflghkjlh

Karpenko, M. I. (2019). War crimes: issues of theory, legislation and practice. *Enterprise, Economy And Law, 8*, 244-248. https://doi.org/10.32849/2663-5313/2019.8.45

Korystin, O., Svyrydiuk, N., Sobko, G., Mitina, O., & Aleksander, M. (2022). Risk assessment of cyberattacks in conditions of hybrid war based on analysis of cybersecurity basic capacity in the civil security sector in Ukraine. *CEUR Workshop Proceedings*, *3530*, 91-101

Kyiv District Administrative Court. (2020). Decision in the name of Ukraine No. 320/140/19 of January 24, 2020. Retrieved from https://zakononline.com.ua/court-decisions/show/87165182

Morozyuk, N.S. & Sobko, G.M. (2022). Military violent criminal offenses in Ukraine, the problem of their classification and codification. *Scientific Journal South Ukrainian Law Review*, *4*, 84-86

Navrotskyi, V.O. (1997). *War crimes. Special part of international criminal law*. Lviv: Ivan Franko National University of Lviv.

Panov, M.I. (2006). *Crimes against the established order of military service (Military crimes)*. Kharkiv: Pravo.

Shkuta, O. O. (2020). Crimes in the Military Sphere: Reasons and Conditions. *European Reforms Bulletin*, *2*, 74-77

Sobko, G. (2020). *Mental Violence: Criminological and Criminal Law Principles of Counteraction: A Monograph.* Kherson: Helvetica Publishing House.

Sobko, G., Chenshova, N., Viunyk, M., Duiunova, T., & Palii, E. (2023a). Characteristics of Punishment for Property Embezzlement and Appropriation by Military Personnel through Abuse of Office. *Legality*: *Jurnal Ilmiah Hukum*, *31*(1), 157-180

Sobko, G., Volodymyrivna, M.H., Hryhorchuk, M., Mykolaiovych, D.I., & Lvova, I. (2023b). Problems and conflicts related to measures to ensure the right to a fair trial in accordance with the european convention on human rights. *Janus.Net*, *14*(2), 302-321

Supreme Court of Ukraine. (2023). Review of the case law of the Criminal Court of Cassation within the Supreme Court (current practice) Retrieved from https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/ogliady/Oglyad_KKS_04_2023.pdf

Us, O. V. (2018). *Theory and practice of criminal legal qualification*. Kharkiv: Pravo. Verkhovna Rada of Ukraine. (1992). Law of Ukraine No. 15 "On social and legal protection of military personnel and their families". Retrieved from https://zakon.rada.gov.ua/laws/show/2011-12#Text

Problematic aspects of determining the administrative and legal status of conscription support entities in Ukraine

by Anatoliy Yatsyshyn[1]

Abstract. The purpose of this study is to identify the issues related to establishing the legal status of military administration entities which ensure conscription during martial law. Using the methods of legal analysis and specification, the author examines the legal aspects of establishing the administrative and legal status of the subjects of conscription. According to the results of the study, it was established, that one of the main military administration bodies responsible for ensuring conscription is the territorial recruitment and social support centres. Despite the fact that the legal framework for regulating mobilisation issues has been in place since the 1990s, the current analysis shows that the definition of the legal status of conscription support entities is not perfect. The challenges of war and high mobilisation needs clearly demonstrate that most of the powers of the authorities are enshrined in legislation in a rather vague manner, which leads to ambiguous interpretation of the norms and inefficient management of the mobilisation process. Given that it is the TCR and SS that carry out most of the mobilisation activities, together with local self-government bodies and executive authorities at the local level, the primary task is to determine the administrative and legal status of the TCR and the SS at the legislative level, not only by bylaws.

Keywords: military duty, special period, armed aggression, military administration, mobilisation measures.

Introduction

The issue of ensuring mobilization has become particularly important since the beginning of the aggressor's full-scale invasion, revealing new problems in the legal regulation of mobilization and mobilization readiness. State bodies play a decisive role in ensuring conscription into military

1 Department of Law Enforcement and Anti-Corruption Activities, Interregional Academy of Personnel Management, 03039, 2 Frometivska Str., Kyiv, Ukraine.

NAM, Anno 6 – Special Dossier
DOI: 10.36158/97912566922174
Ottobre 2025

service, as they are responsible by law for shaping state policy in the field of mobilization preparation and mobilization, as well as for implementing various mobilization measures, including military registration. An equally important factor for effective management in this area is the clear distribution of powers between state authorities and the precise definition of their administrative and legal status, which includes the main areas of activity, responsibilities, and tasks that must be enshrined in law.

Moreover, the unprecedented scale of the ongoing armed aggression has revealed systemic shortcomings in the current legal framework, highlighting the need for detailed legislation that clearly delineates the roles and responsibilities of all entities involved in mobilization. Addressing these gaps is crucial not only for improving operational efficiency but also for ensuring the protection of citizens' rights and the proper functioning of state authorities under extraordinary circumstances.

This study examines the definition of the specific administrative and legal status of military command structures directly involved in mobilization activities. An essential element of the study is the analysis of the activities of bodies involved in conscription and their legal regulation during a special period. In the context of martial law, society faces new challenges and risks, and legal regulation regarding the administrative and legal status of authorities responsible for conscription into military service must be improved and adapted to real-time needs. Clarifying the legal status of these authorities also facilitates better coordination with local government bodies, enhances accountability, and ensures that mobilization activities are conducted in accordance with both national legislation and international standards. Such legal clarity is particularly important in a wartime context, where rapid decision-making and precise execution of mobilization measures can significantly affect national defense outcomes

The aim of the research is to reveal the key problematic issues in the legal regulation of the administrative status of state authorities tasked with conscription into military service. The core objectives of the study include examining the legal framework that establishes the status of bodies involved in mobilisation support, assessing the significance of motivating individuals liable for military service, and identifying existing gaps in the legal regulation of the status of these bodies.

Foreign and domestic researchers have examined issues related to the legal

status of persons subject to conscription. For example, Kosonen and Malkki (2022) studied various models of conscription in Europe and Asia, emphasized the importance of motivating persons subject to military service, and conducted a comparative analysis of different approaches to ensuring mobilization. Their findings show that, in light of the current global security situation, many states are reintroducing compulsory military service. In these works, the authors seek to identify the optimal approach to mobilization that would allow for the effective implementation of mobilization measures while protecting the fundamental rights of citizens.

The authors Baran (2023) and Marleku & Llalloshi (2024) considered the impact of the mobilization system on military service on public administration as a whole. The papers study the essence of military duty and consider the issue of subjects of conscription in the context of their tasks and responsibilities. The authors raise the question of how important it is to guarantee fundamental human rights in the process of implementing mobilization measures and explore opportunities for improving the effectiveness of mobilization measures, taking into account different experiences.

Scientists Axatov & Akhmatkulov (2021) and Altenburger (2025) in their works considered the peculiarities of military conscription, advantages and disadvantages of mandatory military service, as well as the peculiarities of organising and conducting pre-conscription military training. The authors believe that, given the current security situation, the issue of compulsory conscription is becoming increasingly relevant.

Materials and Methods

The study was based on an examination of regulatory and legal acts that define the administrative and legal status of the subjects of conscription at the legislative level. In addition, a number of bylaws were developed. Both general and specific methods of scientific inquiry were used in the course of the study. In particular, the historical and legal method was used to study the stages of formation of territorial recruitment and social support centres and their evolutionary development. Using a formal legal method, the main regulatory and legal acts defining the legal status of conscription authorities were studied, and subordinate legal acts regulating the powers of military authorities were examined. With the help of le-

gal analysis, the author defines the legal status of conscription service providers, identifies the peculiarities of the administrative and legal status of such providers during martial law, and also identifies the problematic aspects in determining the legal status of conscription service providers which affect the system of mobilisation measures in general. Using the generalization method, the main ways to improve the legislation that establishes the legal status of military management bodies were identified.

The study was conducted in several stages. First, the concept of administrative status and its components were examined. At the first stage, the concept of administrative status and its components were studied. The regulatory framework, which forms the basis for the activities of conscription authorities, was reviewed. The next step in the research was to study the main stages in the formation of military management bodies such as the TCR and SS, and to determine their place and significance in the mobilization system. After studying the development and establishment of the legal status of conscription authorities, the issues of establishing such status for military management bodies were identified and the main directions for resolving these issues were outlined.

To ensure reliability of results, the research also incorporated a comparative approach, contrasting Ukrainian regulations with international practice in conscription and mobilization. This made it possible to identify not only the strengths of the national system but also areas requiring alignment with broader European and global standards. In addition, the study relied on systemic and structural analysis to reveal interconnections between state bodies, their powers, and the mechanisms of cooperation during mobilization. Attention was also paid to practical aspects of law enforcement, namely how regulatory provisions are implemented at the regional and local levels. The combination of these methodological approaches enabled a comprehensive exploration of the administrative and legal status of conscription bodies, ensuring both theoretical depth and practical applicability of the findings.

Results

The regulatory basis governing the activities of conscription authorities has been examined. The subsequent stage of the research focused on the formation of military administration bodies, such as the TCR and SS, and clarified their role and significance within the mobilisation system. The analysis of the development and consolidation of the legal status of conscription authorities revealed difficulties in defining such a status for military administration bodies, as well as possible directions for addressing these challenges. Administrative and legal status is generally understood as the totality of rights and obligations assigned to a subject of administrative legal relations. In administrative law theory, legal status is divided into general and special categories, depending on its scope. The general administrative and legal status encompasses the rights and obligations common to all subjects of administrative legal relations, whereas a special status is conferred on particular entities for the fulfilment of specific tasks and functions.

The Law of Ukraine "On Mobilization Preparation and Mobilization" designates the Verkhovna Rada of Ukraine, the President of Ukraine, the Cabinet of Ministers of Ukraine, and local self-government bodies as the entities responsible for conscription. Additional participants in mobilisation include the National Security and Defense Council of Ukraine, the Ministry of Defense, the Armed Forces of Ukraine, and other military authorities whose activities are regulated by law. Among the key institutions directly entrusted with implementing mobilisation plans, maintaining military registration, and ensuring mobilisation measures are the territorial recruitment and social support centres (Verkhovna Rada of Ukraine, 1992; 1993; 1996; 2015).

This institution has special administrative and legal status in mobilization because it does specialized stuff related to military service. However, there are certain problems in determining the exact status of organizations vested with such special powers, including territorial centers for recruitment and social support (Verkhovna Rada of Ukraine, 2017; 2018; 2023). To provide clarity in defining the status of military command bodies and to identify existing challenges, it is necessary to trace the stages of development of these entities in Ukraine, as illustrated in Table 1.

Table 1. Stages in the development of legal regulation of conscription service providers in Ukraine

Period	Legislative activity	Result.
16 July 1990	Adoption of the Declaration of State Sovereignty of Ukraine and the Act of Independence of Ukraine	Changes in the social system and political life. This gave impetus to the further development of legislation for the creation of its own armed forces.
11 October 1991	The Concept of Defence and Construction of the Armed Forces of Ukraine was adopted	The ways and principles of military reform were defined. The fundamental principle was the principle of reasonable sufficiency in terms of the number of weapons and human resources.
November-December 1991	The legal framework for the functioning of the AFU was adopted, in particular, the Law on Defence of Ukraine, the Law on the Armed Forces of Ukraine and others.	The following legislative acts defined the principles of the armed forces
30 March 2021	The Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Improving Certain Issues of Military Duty and Military Registration".	Improving the organisational and legal framework for manning the Armed Forces of Ukraine, bringing the activities of military command and control bodies and the military accounting system in line with NATO standards
23 February 2022	Resolution of the Cabinet of Ministers of Ukraine No. 154 "On Approval of the Regulations on Territorial Centers for Recruitment and Social Support"	This provision defines the legal status, functions, and procedures of the TCR and SS

30 December 2022	Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Procedure for Organizing and Maintaining Military Records of Conscripts, Persons Subject to Military Service, and Reservists"	A mechanism for maintaining military records of individuals liable for military service, in line with the new legislative requirements, was established by the procedure.
16 January 2024	Law of Ukraine "On Amendments to Certain Laws of Ukraine Regarding the Improvement of the Procedure for Processing and Using Data in State Registers for Military Registration and Acquiring the Status of War Veteran During Martial Law"	Improvement of military registration procedures and mobilization measures to improve the efficiency of military unit replenishment
11 April 2024	Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine Regarding Certain Issues of Military Service, Mobilization, and Military Registration"	The most significant changes were adopted: the conscription age was lowered, the procedure for granting deferrals was changed, and the categories of persons eligible for deferrals were changed
10 May 2024	Procedure for maintaining the Unified State Register of Conscripts, Military Service Obligors, and Reservists "Oberig"	Defines the procedure for maintaining the Unified Register of Persons Subject to Military Service, establishes the procedure for collecting, storing, and using data on persons subject to military service
16 May 2024	Resolution of the Cabinet of Ministers of Ukraine No. 560 "On Approval of the Procedure for Conscription of Citizens for Military Service during Mobilization, for a Special Period"	The procedure and rules for mobilization during martial law are regulated in detail

Through the transformation of district and city commissariats into TCR and SS, local military authorities shifted from administrative and coercive bodies into entities performing recruitment and social service functions. The main task of the MCC and JVs is to carry out recruitment activities for military service. The

TCR and SS are regulated by the Constitution and laws of Ukraine, acts of the President of Ukraine, the Cabinet of Ministers of Ukraine, orders of the Ministry of Defense, orders and directives of the Minister of Defense, orders and directives of the Commander-in-Chief of the Armed Forces of Ukraine, as well as other legal acts. The main tasks of the TCR and SS also include registering citizens with draft boards, maintaining military records of citizens, conscripting citizens for military service in peacetime and wartime, selecting persons subject to military service for contract military service, citizens for service in the military reserve, preparing and conducting the mobilization of human and transport resources during special periods, providing legal and social support to military personnel and veterans, engaging in military-patriotic education of citizens, and implementing measures to prepare and conduct territorial defense and other defense activities in accordance with the law (Verkhovna Rada of Ukraine, 2024a; 2024b).

When determining the legal status of entities responsible for conscription, it should be noted that the legal status of any public administration entity is a rather multifaceted and broad category (Shafritz et al., 2022; Kruchynina, 2024). Legal status includes a certain legal position of a public authority, which is established by a legislative act or an administrative act based on the public interest and the need to perform public functions. Administrative and legal status may be general and special. The general administrative and legal status is inherent in all subjects of power. A special legal status implies the granting of certain special powers to solve tasks or to perform a certain type of authority.

The special administrative and legal status is established by certain legislative norms and is a consequence of the state will, through which a certain entity is vested with certain functions. The structure of legal status includes the subject or purpose of the activities of the authority, as well as the rights and powers of the state authority. (Rosenbloom et al., 2022). Considering the subjects that ensure conscription, it should be noted that the purpose of all military authorities is to carry out effective mobilisation to ensure the defence capability of the state. All subjects of power authorised to carry out mobilisation activities are defined in the Law of Ukraine "On Mobilisation Preparation and Mobilisation." Both general and special subjects are endowed by the Law with their functions and must perform their tasks.

TCR and SS are the bodies with the greatest competence in the field of mobilisation, as they are authorised to provide full support to persons liable for military service instead of military commissariats. In accordance with current legislation, TCR and SS perform the following tasks. Participation in the day-to-day management of pre-conscription training is ensured. Decisions of local government authorities and draft boards on conscription of citizens for military service are prepared and implemented. Teams of new recruits are formed and conscripts sent to military units from assembly points in territorial centers. Military records are kept for persons liable for military service who are in the reserve, as well as for citizens who have participated in combat operations and those who have become disabled during military service.

Cooperation with local executive authorities and local self-government bodies is maintained on issues related to military registration of conscripts, including reservists, as well as conscripts and the reservation of conscripts for the period of mobilization and wartime. Plans for mobilising human and transport resources during a special period are developed, and the system of warning, collection, and delivery of these mobilisation resources is improved in the relevant territory. Records of enterprises involved in the performance of mobilisation tasks, as well as of human and transport resources intended to meet the needs of the state's defence, are maintained. Control is exercised over the implementation by enterprises of measures for maintaining military records of persons liable for military service and measures for reserving such persons for the period of martial law. Participation is ensured in controlling the implementation of mobilisation measures within their powers. Social and legal protection is provided for military personnel, persons liable for military service and persons in the reserve, war veterans, and their families (Verkhovna Rada of Ukraine, 2022).

The TCR and SS are responsible for conscripting citizens into the Armed Forces of Ukraine, ensuring mobilisation in line with the constitutional duty to defend the state (Timofeev & Natochii, 2024). Their administrative and legal status remains controversial. As relatively new military structures, they had limited experience exercising their powers before martial law, and their legitimacy depends on mobilisation success and public trust. Analysis of current legislation reveals gaps in regulating the TCR and SS. Their legal status is defined only by the 23 February 2022 Regulation "On Territorial Recruitment and Social Support Centres," a subordinate act that sets basic organisational rules. While regulations

guide internal operations and employee conduct, they do not establish a comprehensive legal framework for interaction with other state and local authorities. This legislative gap limits the clarity of TCR and SS powers relative to their full operational responsibilities.

Determining the place of the TCR and SS among other state administration bodies is complicated by the fact that, according to Article 19 of the Constitution of Ukraine, all state authorities must act only on the grounds and within the limits defined by the Constitution and laws of Ukraine. Article 6 of the Constitution also states that all state authorities must exercise their powers in accordance with the laws of Ukraine. Based on these provisions of the Basic Law, it appears that the activities of state authorities are provided with clear legislative regulation, which obviously also applies to territorial recruitment and social support centres (Magdalina, 2024).

Another problematic issue in determining the administrative and legal status of territorial recruitment and social support centres is the lack of an unambiguous approach to the classification of TCR and SS as military command and control bodies. Based on the tasks assigned to the TCR and SS, the question arises whether such bodies can be directly attributed to military administration bodies. The concept of "military management body" is defined in Article 1 of the Law of Ukraine "On Defence of Ukraine" of 6 December 1991. However, the relevant concept appeared in the law in the wording of this legal act of 5 October 2000. At that time, the military command included the Ministry of Defense of Ukraine, other executive bodies responsible for the management of military units, the General Staff of the Armed Forces of Ukraine, as well as other departments, formations, headquarters, and military commissariats responsible for the implementation of legislation in the field of military duty, military service, mobilization preparation, and mobilization. In the above definition, military commissariats, and subsequently territorial recruitment and social support centres, are not mentioned in the main list of military administration bodies, but rather as a supplement to this list - through the language construction "as well as". This wording may be used as a consequence of the imitation of post-Soviet legislation, since in the post-Soviet period, the armed forces were recruited through military enlistment offices as a special structure. Today, the TCR and SS are vested with much broader powers that go far beyond the solely organisational component of military management (Magdalina, 2024).

The administrative and legal status of territorial recruitment and social support centers shows that TRCs and SSs are military management bodies under the executive branch, created, funded, and dissolved by the Ministry of Defense of Ukraine. They must operate in line with legislation on mobilization, military training, and social protection of servicemembers and their families. To formalize their status, the Law of Ukraine "On Mobilization Preparation and Mobilization" should be amended. Article 14 could include a new part detailing the main functions and powers of TRCs and SSs. Additionally, a dedicated law should be introduced to comprehensively regulate their activities, reflecting the full scope of their responsibilities. Strengthening the legal framework would not only clarify the responsibilities of TRCs and SSs but also enhance transparency and accountability in the mobilization process. Clearer legislative guidance could reduce operational ambiguities and improve coordination between military authorities and local administrations.

Discussion

This paper examines the regulatory framework that establishes the legal status of entities responsible for conscription. The author examines the legislative provisions that regulate the main tasks and responsibilities of military authorities in the field of mobilisation. Unlike the work of Baran (2024), which explores issues related to the analysis of the historical evolution of conscription and the relationship between the security of society as a whole and the observance of individual rights, this study reveals the historical development of conscription service providers, their features and modes of operation. The main attention was paid to the administrative and legal status of territorial recruitment and social support centres as one of the main military management bodies that can carry out mobilisation measures on the ground.

Melnyk (2022) examines the administrative and legal status of military administrations in Ukraine during martial law, analyzing their functions and the relationship between military and civilian authorities. In contrast to Melnyk, this study focuses on the legal status and functional powers of military administration bodies involved in conscription. This study not only analyzes their legal basis but also highlights current issues in determining the status of bodies involved in conscription. Confirming Voitovich's (2020) observation, the administrative and

legal status of security and defense bodies remains insufficiently researched, with many outdated norms needing to be brought into line with modern practice and international standards. This study is unique in that it focuses on mobilization bodies with special powers in this area.

Boyko (2024), like this study, also examines the genesis of legal regulation of administrative and legal regulation of mobilisation. However, this work is more narrow, aimed at identifying the problems in the consolidation of the legal status of the subjects that should ensure the conscription. The work of Semenets-Orlova, et al., (2022) and others raise the issue of development of the public administration system with a human-centred approach. The authors note the importance of replacing the brutal administrative pressure in the management system with the creation of a management culture. Agreeing with the authors' opinion, this work also examines the administrative and legal status of individual subjects of administrative law and seeks ways to improve the system of administrative management in the field of mobilisation.

Yermachenko et al. (2023) examined public administration in infrastructure development, emphasizing a "smart" management approach that considers societal needs and challenges. This study similarly analyses the structure of public administration in mobilisation processes, highlighting that the administrative and legal status of authorities their powers and position within the mobilisation system – is key to effective management. Yarusevych (2023) provides a detailed analysis of the administrative and legal status of defence industry entities, identifying elements of their regulatory framework. Unlike these studies, the present work focuses specifically on mobilisation bodies operating under martial law. Thus, while previous research provides valuable insights into administrative and defence structures, there remains a clear need for focused studies that examine the operational and legal intricacies of conscription authorities, particularly those that function during extraordinary circumstances such as martial law.

It should be emphasised that most studies do not address the issue of the administrative and legal status of conscription authorities at all. The studies consider either the security and defence sector or individual subjects of power. In most cases, the authors consider the subjects of conscription in their historical development, but there are no studies on their current legal status and no studies that could suggest ways to improve the legal norms that establish the administrative

and legal status of military authorities that are directly responsible for mobilisation activities. This research gap is essential to provide a coherent and modern legal framework for mobilization authorities, ensuring an appropriate balance between the interests of the state and society in times of national emergency.

Conclusions

One of the main factors of effective management in the field of mobilisation is a clear delineation of powers of the subjects of power, a specific establishment of their administrative and legal status, which includes the main areas of activity, duties and tasks that should be defined at the legislative level. The problem of determining the administrative and legal status concerns, first of all, the determination of the administrative and legal status of entities with special powers, such as territorial recruitment and social support centres. The legal status includes a certain legal position of a public authority, which is established by a legislative act or administrative act based on the public interest and the need to perform public functions. TCR and SS are the subjects of administrative legal support for the mobilisation of the UAF, which are responsible for ensuring the fulfilment of the call-up of citizens of Ukraine for military service to fulfil their constitutional duty to defend the state. The study found that the TCR and SS are military command and executive bodies.

The study found that the main problem of determining the administrative and legal status of conscription support entities, in particular, the TCR and SS, is the following legal aspects: the activities of territorial recruitment and social support centres, which have the broadest powers in the field of mobilisation, are regulated exclusively by the Regulation. In addition, TCR and SS are not included in the list of entities responsible for mobilisation training and mobilisation in accordance with the Law of Ukraine "On Mobilisation Training and Mobilisation". Other problematic aspects include the fact that the current legislation does not clearly delineate the powers of the entities involved in mobilisation activities.

In view of this, some areas for improving the legal regulation of conscription support entities were identified, in particular, the adoption of a separate law on territorial recruitment and social support centres, the definition of the powers of TCR and SS in the Law of Ukraine "On mobilisation preparation and mobilisation", as well as a more specific delineation of the tasks of conscription support

entities during martial law. In order to consolidate the administrative and legal status of the TCR and SS at the legislative level, amendments should be made to the Law of Ukraine "On Mobilization Preparation and Mobilization." Specifically, Article 14 of this Law should be supplemented with Part 3, which should specify the main functions and powers of the TCR and SS. In addition, given the full scope of tasks assigned to the territorial centers for recruitment and social support, the legislative framework should be expanded with a special law on the TCR and SS, which will regulate their activities in detail.

The prospect for further research lies in providing a detailed definition of the powers, tasks, and scope of the TCR and SS, with the aim of drafting legislation on territorial recruitment and social support centres. The limitations of this study stem from its primary focus on determining the legal status of the TCR and SS, as this represents the most urgent issue, while the administrative and legal status of other conscription-related entities was not examined in full.

References

Altenburger, S. (2025). Reconsidering military and civilian conscription. *The Journal of Politics*, *87*(2), 464-478. https://doi.org/10.1086/730738

Axatov, S. A., & Akhmatkulov, U. M. (2021). Basics of pre-conscription military training subject. *ACADÉMICA: An International Multidisciplinary Research Journal*, *11*(8), 441-447. Retrieved from https://saarj.com/wp-content/uploads/paper/ACADEMICIA/2021/ABSTRACT/ACADEMICIA-AUGUST-2021/8.74%2C%20Samariddin%20Alikulovich%20Axatov.pdf

Baran, A. (2023). Legislation on conscription: Comparative analysis. *Visegrad Journal on Human Rights*, *(1)*, 29-35. Retrieved from https://journal-vjhr.sk/wp-content/uploads/2024/06/3.pdf

Baran, A. (2024). Conscription, coercion and international human rights law. *Visegrad Journal on Human Rights*, *(3)*, 20-28. https://doi.org/10.61345/1339-7915.2024.3.3

Boyko, B. V. (2024). Public administration in the field of mobilisation training and mobilisation: The genesis of doctrinal research and regulatory and legal regulation in Ukraine in 2014-2024. *Scientific Bulletin of Uzhhorod National University, 2*(85), 248-257.

Kosonen, J., & Mälkki, J. (2022). The Finnish model of conscription. In *Successful public policy in the Nordic countries: Cases, lessons, challenges*. Oxford: Oxford University Press.

Kruchynina, O. M. (2024). Organisation of personnel support for territorial recruitment and social support centres. https://dspace.znu.edu.ua/jspui/bitstream/12345/

25811/1/%d0%9a%d1%80%d1%83%d1%87%d0%b8%d0%bd%d0%b8%d0%b-d%d0%b0%20_%20%d0%bc%d0%b0%d0%b3%d1%96%d1%81%d1%82.pdf

Magdalina, I. V. (2024). *The essence of the educational function of the state: philosophical and legal dimension*. Dnipro: Dnipro State University of Internal Affairs.

Marleku, A., & Llalloshi, E. (2024). The impact of the war in Ukraine on conscription policies in Western Balkan countries. In *Conference Book of Proceedings of the UBT International Conference* (p. 20). Retrieved from https://knowledgecenter.ubt-uni.net/cgi/viewcontent.cgi?article=4787&context=conference

Melnyk, S. M. (2022). Administrative and legal status of military administrations in Ukraine under the legal regime of martial law. *Dnipro Scientific Journal of Public Administration, Psychology, Law*, *(6)*, 100-104. https://doi.org/10.61345/1339-7915.2024.2.16

Rosenbloom, D. H., Kravchuk, R. S., & Clerkin, R. M. (2022). *Public administration: Understanding management, politics, and law in the public sector*. New York: Routledge.

Semenets-Orlova, I., Shevchuk, R., Plish, B., Moshnin, A., Chmyr, Y., & Poliuliakh, R. (2022). Human-centred approach in new development tendencies of value-oriented public administration: Potential of education. *Economic Affairs*, *67*(5), 899-906. https://doi.org/10.46852/0424-2513.5.2022.25

Shafritz, J. M., Russell, E. W., Borick, C. P., & Hyde, A. C. (2022). *Introducing public administration*. New York: Routledge.

Timofeev, V. P., & Natochii, A. D. (2024). Conflict between the territorial centre of recruitment and social support and the civilian population. *Analytical and Comparative Law*, *(6)*, 177-182. https://doi.org/10.24144/2788-6018.2024.06.26

Verkhovna Rada of Ukraine. (1992). The Law of Ukraine "On Military Duty and Military Service". https://zakon.rada.gov.ua/laws/show/2232-12#Text

Verkhovna Rada of Ukraine. (1993). The Law of Ukraine "On Mobilisation Training and Mobilisation". https://zakon.rada.gov.ua/laws/show/3543-12/conv#Text

Verkhovna Rada of Ukraine. (1996). Constitution of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

Verkhovna Rada of Ukraine. (2015). Law of Ukraine "On the Legal Regime of Martial Law". https://zakon.rada.gov.ua/laws/show/389-19#Text

Verkhovna Rada of Ukraine. (2017). Law of Ukraine "On the Unified State Register of Conscripts, Military Conscripts and Reservists". https://zakon.rada.gov.ua/laws/show/1951-19#Text

Verkhovna Rada of Ukraine. (2018). The Law of Ukraine "On National Security of Ukraine". https://zakon.rada.gov.ua/laws/show/2469-19#Text

Verkhovna Rada of Ukraine. (2022). The law of Ukraine No. 154 "On approval of the regulations on territorial recruitment and social support centres". https://zakon.rada.gov.ua/laws/show/154-2022-%D0%BF#Text

Verkhovna Rada of Ukraine. (2023). The Law of Ukraine "On Amendments to the Law of Ukraine On Military Service and Military Duty". https://zakon.rada.gov.ua/laws/show/3127-20#Text

Verkhovna Rada of Ukraine. (2024a). The Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine Regarding Certain Issues of Military Service, Mobilisation and Military Registration". Retrieved from https://zakon.rada.gov.ua/laws/show/3633-20#Text

Verkhovna Rada of Ukraine. (2024b). The law of Ukraine No. 560 "On approval of the procedure for conscription of citizens for military service during mobilisation, for a special period". Retrieved from https://zakon.rada.gov.ua/laws/show/560-2024-%D0%BF

Voytovych, I. I. (2020). Methodological principles of researching corruption crime in the sphere of military security. *Legal Science, 3*(105), 12-18. https://doi.org/10.32844/2222-5374-2020-105-3.02

Yarusevych, A. S. (2023). *Administrative and legal status of subjects of management of state-owned objects in the defence-industrial complex*. Sumy: Sumy State University.

Yermachenko, V., Bondarenko, D., Akimova, L., Karpa, M., Akimov, O., & Kalashnyk, N. (2023). Theory and practice of public management of smart infrastructure in the conditions of the digital society's development: Socio-economic aspects. *Economic Affairs*, *68*(1), 617-633. https://doi.org/10.46852/0424-2513.1.2023.29

Intellectualization of financial investigations
in the system of anti-corruption compliance of procurement in accordance with NATO standards in ensuring the stability of national security

by Karina Nazarova[1], Volodymyr Hordopolov[2], Tetiana Lositska[3]

Abstract. During warfare and martial law, Ukraine's defense procurement system requires urgent reform to ensure national security and effective international cooperation. Therefore, the study aims to propose practical steps for implementing NATO-aligned anti-corruption and investigative mechanisms in Ukraine's defense procurement, thus ensuring stability and security under martial law. The research applies methods such as analysis, synthesis, induction, deduction, dialectics, analogy, abstraction, and generalization to assess how intellectualized investigations and digitalization can mitigate corruption risks. As a result, it is established that the existing system fails to address high corruption risks and global market shifts, resulting in operational delays, inefficiencies, and diminished trust from international partners. Core issues include the duplication of powers, poor inter-agency coordination, and a lack of effective oversight, with corruption remaining the most critical threat. This study highlights the potential of intellectualized financial investigations and digital anti-corruption tools, aligned with NATO compliance standards, to strengthen control mechanisms and minimize human error. The NATO approach demonstrates that procedural flexibility and transparency are compatible, offering a viable model for Ukraine. The integration of advanced analytics, digital monitoring systems, and compliance protocols is essential for increasing transparency, enhancing procurement ethics, and reinforcing the country's Euro-Atlantic integration efforts.

Keywords: national security; corruption; NATO standards; public procurement monitoring; digitalization.

1 Doctor of Economics, Professor, Department of Financial Analysis and Audit, State University of Trade and Economics, 02156, 19 Kyoto Str., Kyiv, Ukraine. https://orcid.org/0000-0002-5019-9244.

2 Doctor of Economics, Professor, Department of Financial Analysis and Audit, State University of Trade and Economics, 02156, 19 Kyoto Str., Kyiv, Ukraine. https://orcid.org/0000-0002-3151-8035.

3 PhD in Economics, Senior Researcher, Research Department, State University of Trade and Economics, 02156, 19 Kyoto Str., Kyiv, Ukraine. https://orcid.org/0000-0003-3117-3281. t.lositska@knute.edu.ua.

NAM, Anno 6 – Special Dossier
DOI: 10.36158/97912566922175
Ottobre 2025

Introduction

The full-scale armed aggression of the Russian Federation has created a significant burden on the defense procurement system of Ukraine, which further necessitated adaptation to new difficulties. In addition, it works during martial law, when the reliability and timeliness of supplies are critical needs. However, existing methods of organizing, planning, and conducting procurement do not take into account several modern problems, such as the high danger of corruption, the requirement to maintain efficiency and secrecy, as well as constant changes in the global market for military goods. This leads to irrational use of resources, delays in supplies, and a decrease in the confidence of foreign partners.

The defense industry is vulnerable to corruption schemes due to improper implementation of procurement policy by the Ministry of Defense of Ukraine, duplication of departmental powers, poor coordination, inadequate legal regulation, and ineffective control. According to Transparency International and the National Agency for the Prevention of Corruption (NACP), despite some improvements, corruption remains the main obstacle to the effective operation of the defense procurement system (Transparency International, 2024). This demonstrates that risk management practices urgently need to be thoroughly reformed and effective accountability and transparency systems introduced.

Digitalization of defense procurement procedures is one of the most potential areas for combating corruption risks. With the help of modern IT solutions, electronic platforms, digital registries, and analytical tools, it is possible to significantly reduce the influence of the human factor, increase control efficiency, guarantee procurement tracking, and quickly eliminate violations. At the same time, digital transformation should be included in a broader system of anti-corruption compliance by NATO standards, which include professional training of personnel, independent monitoring, as well as less freedom of action and responsibility.

The system can be improved by adapting best practices from around the world, especially the anti-corruption programs of NATO member states. This allows you to optimize costs and increase transparency while maintaining important procedural flexibility. By implementing such measures in practice, Ukraine will be able to increase its defense capability, form a favorable image abroad, and attract sponsors and partners.

This study identified important shortcomings in the current system, examined the relationship between the degree of digitalization of defense procurement and the reduction of corruption risks, and provided useful suggestions for the gradual implementation of anti-corruption compliance tools by world standards. In the context of further Euro-Atlantic integration of Ukraine, the full implementation of these technologies has the potential for a revolution in the country's defense procurement system, which will become modern, open, transparent, and honest.

Several scientists have investigated this direction of social relations in particular Pakhachuk et al. (2025) analyzed the experience of NATO, the USA, and the EU in managing the risks of defense procurement and suggested ways to adapt it in Ukraine. Emphasis is placed on digitalization, risk registries, staff training, and increased auditing to increase transparency and compliance with NATO standards. Shkola and Bakin (2024) studied the EU mechanisms for countering modern challenges and threats and outlined the possibilities of their adaptation to strengthen the security and stability of Ukraine. Rusina (2025) investigated the peculiarities of state financial control under martial law, identified key problems of its implementation, and proposed ways to increase efficiency to strengthen financial discipline and national security. Zhuravel (2024) examined the specifics of managing public finances in wartime conditions, identified problems of efficiency and accountability, and proposed ways to solve them to ensure the stability of public finances. Petrunyak (2023) analyzed the legal mechanisms for combating corruption in the financial sector, identified its vulnerability to corruption risks, and emphasized the need to improve legislation, financial control, and international cooperation, especially under martial law.

The aim of the study is to assess how digitalization can reduce corruption risks in Ukraine's defense procurement, to consider NATO anti-corruption standards and financial investigation procedures for the defense industry, and to create effective proposals for the implementation of these strategies in the country's defense procurement system, taking into account the requirements of Euro-Atlantic integration and the conditions of martial law.

Methodological Framework

The approach in this study, which combines traditional general scientific and cognitive methodologies, allowed us to identify in detail corruption vulnerabili-

ties in the defense procurement system of Ukraine and offer practical solutions. The components of the defense procurement system were investigated through analysis in stages, from institutional structure and regulatory control to specific abuse situations. For example, the analysis investigated the situation with the "egg scandal" of 2023 - the actions of officials, the content of the contract, the validity of prices, and the availability of control were separately considered.

Synthesis was used to create a common risk management model that includes digital technologies, compliance initiatives, and anti-corruption audits. The proposal to combine the tasks of risk management, digitalization, and transparency into a single procurement policy architecture was made possible by synthesis. Induction was demonstrated by the development of broad generalizations to study specific cases, such as the acquisition of protective vests, the provision of material goods, and the inefficient use of the Food Catalog. General characteristics of corruption risks were derived based on system defects in each scenario.

Based on NATO's broad risk management guidelines, namely the ARAMP-1 standard, deduction has allowed us to confirm whether Ukrainian processes meet these standards. For example, a critical assessment of Ukrainian procedures for proper verification of contracts was carried out in the light of instructions to maintain risk registers. The study of the dynamics and contradictions of the procurement system - the need for rapid delivery during the war, on the one hand, and the requirements of transparency and control - on the other, became possible thanks to dialectical technology. This allowed us to identify the main conflict between the fight against corruption and procedural flexibility, which became the focus of the study.

The study of world experience (NATO, USA, EU) used analytical techniques; In particular, DFARS standards, Directive 2009/81/EC, and ARAMP-1 were taken into account. To find out if they can be adapted in Ukraine, a thorough analysis of relevant digital platforms such as PIEE in the USA and EBAU in Germany was conducted. Comparison of Ukrainian institutions with relevant organizations in NATO countries became possible thanks to the methodology of analogy. The idea of creating an independent audit unit is based on similar procedures in other jurisdictions, such as the State Audit Service, which is considered a possible analog of DCAA in the United States.

Key ideas and categories such as procurement system, corruption risk, digita-

lization, and compliance were defined through abstraction. As a result, we were able to exclude minor components and focus research on important risk factors. The research process ended with a generalization; Based on the collected facts, studied cases and comparison of world experience, system proposals for the digital transformation of defense procurement and the implementation of anti-corruption compliance have been developed. Using these methods, we were able to guarantee the breadth, consistency, and scientific validity of the research results, which allowed us to propose the proposed strategies as a basis for restructuring the defense industry of Ukraine.

Results

The Ukrainian defense procurement system operates under conditions of extreme regulatory complexity and significant legal uncertainty during martial law, which increases the likelihood of systemic corruption. The presence of a large number of normative legal acts, such as laws, decrees of the Cabinet of Ministers, internal orders, and other documents, as well as frequent changes to them, complicate the understanding of procurement procedures, reduce the transparency and predictability of the process, create opportunities for abuse of power. In practice, special regulations, such as Cabinet of Ministers Resolutions No. 1275 or No. 1178, which specifically allow procurement without the application of legally established competitive procedures, often replace or repeal the Law of Ukraine "On Defense Procurement", even though it was created to regulate the basic principles of planning, conducting and controlling procurement for security and defense needs. Such exceptions may be acceptable as a short-term solution during a conflict, but their extended application favors corruption because it does not provide adequate accountability, control, and competition.

Of particular concern is the combination of the Ministry of Defense's responsibilities to develop and implement procurement policies, as they are contrary to good governance. This means that the same bodies or structural units are responsible for planning, contracting, determining needs, quality assurance, negotiating, and supervising the terms of the contract. This concentration of power leads to conflicts of interest and excessive discretion, which is especially risky when procurement processes are simplified or non-competitive. This has already resulted in certain corruption abuses, especially the purchase of low-quality body armor

for exorbitant funds, which cost the state more than a billion hryvnias. Law enforcement investigations confirm that DOD officials abused their authority by signing contracts with questionable suppliers through procedural loopholes, violating quality standards, and failing to properly verify counterparty qualifications (Zaremba & Lusta, 2021).

Duplication of efforts, belated decision-making, and reduced efficiency during the war is caused by the unclear role of ministries, in particular the Ministry of Defense, the Ministry of Economy, and the Ministry of Strategic Industry, which are involved in the planning and execution of procurement. Effective procurement planning, rapid response to the first requirements, and a high level of integrity and accountability are hampered by the lack of a single coordination structure, a clearly defined organization responsible for defense procurement policy, and a system of interdepartmental communication. The unification of the legislative framework, the creation of a single procurement body, the definition of clear powers, and the introduction of a long-term planning system based on the needs and life cycle of products are among the recommendations developed in cooperation with NATO experts as part of the Strategic Review of Defense Procurement.

In addition, procurement planning in logistics is often based on incomplete or delayed data and is carried out without proper analytics, especially when it comes to tangible assets. The lack of a clear time frame and method for harmonizing technical specifications with state-owned enterprises, such as DOT, leads to poor planning, delays, and cases where purchases are made as urgent without sufficient explanation. This allows you to choose non-competitive methods and contributes to an environment in which suppliers are identified non-transparently. The issue is complicated by the lack of an organized system for coordinating the planning and conduct of procurement, as well as ineffective feedback between the Armed Forces of Ukraine, the Ministry of Defense, and state business.

The use of a food catalog, which serves as the basis for buying food, presents another problem. Since there is no generally recognized mechanism for estimating the estimated cost, suppliers do set prices for each product unilaterally, which makes it difficult for the state to verify their legality. This makes it possible to manipulate prices, especially inflating prices for the most popular goods, advertising the lowest price for what is not ordered. This technique, together with the opacity of calculating the cost of catering services, makes it possible to abuse the official position when signing contracts and creates obstacles for new suppliers.

To reduce the impact of human factors on the development of applications and prevent abuse in the field, public experts have repeatedly called for reforming the food system, in particular for the separation of logistics services from food procurement processes and the introduction of seasonal menus (Antonyuk, 2023).

It is advisable to cite as an example of the current state of defense procurement, the example of the Ukrainian practice of "Egg Scandal". When it turned out that the Ministry of Defense had signed a contract for the supply of eggs at an inflated cost (two to three times higher than the market), in January 2023 a corruption scandal broke out with the purchase of food for the military. Journalists collected supporting documentation and reported facts contrary to martial law. The lack of proper internal control was revealed after additional studies since the responsible persons did not study the market conditions and did not check the accuracy of the supplier's figures. This example demonstrated that in the absence of reliable protection, the danger of inflated costs persists even in cases where procurement is extremely urgent. As a result, the Ministry of Defense began a review of internal pricing processes, and several officials were removed from their posts.

Under the conditions of martial law, the Ministry of Defense of Ukraine has identified serious systemic problems that not only indicate the inefficient management of state resources but also threaten the proper provision of military personnel, which directly affects the state's ability to defend itself. From the very beginning of the full-scale invasion of the Russian Federation, Ukraine had to urgently reconsider the issue of supplying troops. However, the system continued to rely on outdated Soviet processes of bureaucracy, centralization, and irresponsibility rather than moving to a new model of prompt, transparent, and responsible delivery.

One of the most obvious problems was the lack of a single relevant database that would reflect the real needs of military units. Objective information from the front was sometimes not taken into account when choosing material values; in particular, unit commanders were not properly informed of shortages or oversupply. Instead, purchases were often made in response to unstructured demands that arose through the chain of command, or for the remaining funds that needed to be "mastered" by the end of the budget period. As a result, millions of assets were purchased that did not meet the real needs of soldiers, climatic circumstances, or the details of conflicts (Pakhachuk et al., 2025).

In addition, the logistical aspect of providing the actual things remained a very weak point. The acquired assets were distributed slowly, often with months of delays and without a clear process. While centralized warehouses kept surplus purchased goods, often of unknown quality, fighters on the front lines were left to fend for themselves in search of uniforms, shoes, thermal underwear, personal hygiene products, and cold and rain protection components. The lack of a computerized accounting and control system made it difficult to monitor the number, movement, and exact position of assets. A favorable atmosphere for manipulation and abuse was created by the lack of clear instructions in the Ministry of Defense for keeping records in a combat situation and the fact that many units did not keep paper records at all, let alone electronic systems.

Even though certain contracts for the provision of physical property were signed with the understanding that payments would be made in advance, there was not enough control over the performance of contractors' duties. In addition to the fact that suppliers were not financially responsible, suppliers who did not produce property of acceptable quality or overdue deadlines nevertheless received new orders, sometimes at excessively high rates. Contracts were signed with enterprises that seemed fraudulent or did not have the necessary skills to perform such duties. Artificially high prices were the result of a lack of competition in the supplier market, which is especially risky with a limited budget (Shkola & Bakin, 2024).

Another aspect of the problem is the lack of internal control within the Ministry of Defense. There is hardly any system that would guarantee compliance with the terms of contracts, and even in situations of gross violations, the parties concerned are not subject to criminal or disciplinary penalties. Reports of the State Audit Service or internal audits that document many abuses rarely lead to systemic improvements. In addition, the system of the Anti-Corruption Committee of the Ministry of Defense was ineffective; despite numerous high-profile disclosures in the media, decisions regarding responsible persons were either delayed or ignored altogether.

All this points to a serious systemic problem of material support of the army. Every mistake, every pair of shoes or clothes detained during the conflict endangers the life of a serviceman. In addition, it becomes a national security problem, not just a problem of bad governance, when corruption or managerial errors lead

to such results. All stages of the process, from supply, logistics, and contract control to procurement planning and collecting demand from the front, must be quickly reformed by the Ukrainian government. Apart from the fact that transparency, digitalization, public accountability, and punishment of perpetrators are essential for effective governance, they are also core components of the nation's defense capability.

Equally important is the creation of an audit and internal control system. These procedures began to take shape in Ukraine in 2015, but serious shortcomings were revealed during the audit of public procurement in 2024. Problems with risk management and supplier assessment, in particular, indicate the need for significant development of institutional capacity and changes. The actual application of regulatory requirements will continue to be insufficiently effective in the absence of systemic adjustments. Good achievements are associated with the creation of state enterprises DOT and AOZ, which perform the duties of the state customer. If given institutional autonomy, and a proper compliance-control board, they can turn into useful tools for implementing procurement policies. However, at the moment there is a possibility that the active positions of these companies may be attacked, especially due to political influence and cyber threats, so it is necessary to strengthen their organizational and security stability. In the future, Ukraine should create a single national defense procurement organization, which would include both military and civilian experts, to coordinate a strategy in the field of security and defense (Rusina, 2025). Table 1 includes the dynamics of investigations, corruption cases, budget losses, digitalization, anti-corruption audits, and other key indicators of Ukraine's defense procurement.

Table 1. Dynamics of corruption risks, losses and digitalization in Ukrainian defense procurement (2021–2025)

Year	Number of investigations	Loud cases	Budget losses due to violations	Number of audits	Level of digitalization	TI and NACP reports	Number of implementations	Number of suspensions
2021	15	-	0.9	5	15	3	0	2
2022	22	5	1.5	9	20	6	1	5
2023	35	egg scandal	2.7	18	28	9	2	8
2024	50	bulletproof vests	3.4	26	40	12	3	12
2025	40	ammunition	2.5	22	50	11	4	10

Source: based on Rusina (2025)

Thus, corruption risks in defense procurement are the result of deeper systemic problems with organizational structure, regulatory uncertainty, duplication of authority, lack of a unified strategy, and poor planning, as well as individual violations or dishonest officials. The only way to reduce the level of misuse and guarantee the effective and fair use of budget funds in the defense sector is a complete reform based on the ideas of accountability, transparency, distribution of power, and institutional stability. Solving complex problems and relying on world experience are also crucial. The effectiveness of financial control systems, the verification of abuse, and the division of responsibilities between prevention and detection of violations are of particular importance during martial law. Significant budget funding for defense procurement and the huge potential for financial abuse make this issue even more urgent. Thus, in addition to studying institutional reforms, it is crucial to study real examples of financial investigation tools and oversight processes that can be modified by Ukrainian conditions.

The purchase of lower body armor by the Ministry of Defense, which caused

widespread public outrage, is one example of a successful financial investigation in Ukraine. The purchase of almost 11 thousand defective Corsair body armor, which did not meet the criteria for protection and could be fatal for military personnel, was published by the State Bureau of Investigation in 2019-2020. Despite what was known about the flaws, Department of Defense leadership accepted batches for registration despite ballistic analysis that confirmed the devices failed bullet testing. The possibility of real prosecution in defense procurement was demonstrated when the case went to trial and some of the defendants were dismissed.

Ukraine may adopt some aspects of foreign processes, such as the European Anti-Fraud Office (OLAF), the Government Accountability Office (GAO) in the United States, or the Defense Contracts Audit Agency (DCAA), to increase the effectiveness of controlling defense procurement costs. OLAF conducts both documentary and digital checks and conducts impartial investigations of fraud with EU budget funding. The GAO conducts a thorough analysis of state budget expenditures and issues conclusions that Congress must adhere to. To regulate the financial capacity and cost of the contractor, the DCAA reviews Pentagon contracts before they are completed. Financial investigations are reactive tools for responding to already identified signs of corruption or fraud to document, identify, and prosecute cases. This is in contrast to compliance procedures, which focus on preventing violations (through internal controls, integrity policies, and transparency).

As a structural component of a collective security strategy, NATO places a high priority on risk management in defense procurement. In the context of collective defense, where several countries can participate in joint production or use defense capabilities, risk management goes beyond the internal operations of one state and becomes an important prerequisite for interstate trust, standardization, and cost-effective use of public funds. The most important source in this area is the ARAMP-1 (NATO Risk Management Guide for Acquisition Programs), a comprehensive guide that describes the risk management procedure in the management of defense programs and procurement. From formulating requirements, evaluating alternatives, developing and testing to delivery, maintenance, and decommissioning, it covers the full project life cycle. It is important that in addition to broad recommendations, the ARAMP-1 describes in detail the duties and responsibilities of each party, the frequency of inspections, the risk analysis structure (for example, the

probability/impact matrix), and the response criteria. This strategy guarantees the uniformity of procedures between NATO members, which is especially important for initiatives that are funded or developed jointly and require joint risk assessment and management (Zhuravel, 2024).

Large-scale NATO initiatives, such as the NATO Alliance Ground Surveillance Program (AGS), a joint unmanned reconnaissance system based on the RQ-4 Global Hawk UAV, use ARAMP-1. In addition to pooling the resources of NATO's 15 members, the initiative has taken on significant risks related to cyber defense, real-time data sharing, technology integration, and a multi-year service cycle. Each risk was recorded in a centralized registry and monitored by the joint program management team. Digital risk monitoring modules have also been used in the NATO Support and Procurement Agency (NSPA) program for the maintenance of the A330 MRTT (Multi-Role Transport Aircraft and Refueling Aircraft), focusing on upgrade timelines, maintenance availability, and life-cycle cost control.

It is important to note the function of digital technologies, which are now a key component of NATO's modern risk management system. To predict delays or cost overruns, member countries are increasingly using integrated platforms that include risk registers, contract calendars, budgets, terms of reference, delivery schedules, and analytical modules. In some situations, a centralized project management system is used, such as the MRTT multinational fleet project, to which national representatives of the participating countries have access. This allows you to see the status of implementation in real time, identify critical points, and agree on an action plan without unnecessary bureaucracy. This is an illustration of how digital technologies enable full interaction between states (Baillie et al., 2024).

Although the phrase of anti-corruption compliance is rarely used in Alliance documents in a restrictive sense, NATO places a high priority on the unity of approaches to compliance and integrity. However, supplier enterprises must have internal controls, quality assurance, incident recording, feedback, and response procedures to meet the requirements of the AQAP (Allied Quality Assurance Publications) series of standards, in particular AQAP-2070 (Risk Management). Contracts with the NATO Support and Procurement Agency (NSPA), for example, require suppliers to undergo pre-qualification, which involves not only technical and financial assessment but also verification of their internal policies regarding corporate governance, conflict of interest, processing of confidential

information, and security of supply. Companies may not be allowed to participate in tenders at the Alliance level if they do not have such rules or do not comply with them (Shterma et al., 2025).

To ensure compliance with Alliance rules, NATO member states also use mirror control organizations. For example, the UK Ministry of Defense's Commercial Toolkit contains the necessary rules to curb corruption in all defense procurement. These rules include computerized forms for monitoring transactions, forms for declaring conflicts of interest and publishing contractor integrity policies. Important defense initiatives in Denmark are monitored by the Ministry of Defense's Audit and Risk Management Committee through a consolidated online platform, and the committee's findings are subject to legislative review.

Germany is introducing a digital portal for reporting costs and risks in defense procurement, the EBAU system (Elektronisches Berichtswesen für Ausrüstung und Unterstützung). It is also used to assess compliance with NATO standards. These examples show that risk management, compliance, and digital audit are not formally separated in the Alliance; rather, they are all seen as part of a single procurement security logic, with digital platforms serving as the primary tool for implementing traditional procedures rather than as an adjunct to them. Therefore, in addition to the formal study of ARAMP-1 or AQAP, Ukraine must also build the necessary digital infrastructure, train staff and create institutional conditions for the real use of these tools in the framework of adaptation to NATO standards (Antonyuk & Zinko, 2023).

The experience of the United States and the EU, which are members of NATO, should also be taken into account. This decision was made for several reasons. First, these countries interact with our defense structures most often through international initiatives and are the main suppliers of security assistance to Ukraine. Second, their defense procurement systems are extremely advanced, have evolved over the years, and now represent the highest international standards of digital transformation, risk management, and financial control. Thirdly, Ukraine's approach to the Alliance's standards is influenced by the experience of the United States and the European Union, which is directly included in the NATO regulatory framework and standards (namely ARAMP-1, AQAP, and STANAG). The study of these models makes it possible to choose exactly those tools that can be adapted to Ukrainian realities, taking into account the current

difficulties, martial law, lack of resources, and the requirement for operational but balanced decisions. It also helps to better understand how risk management functions in practice under democratic civilian control (Petrunyak, 2023).

Anchored in FAR, DFARS, and specialized recommendations such as the Risk Management Guidelines for Defense Procurement Programs, risk management in defense procurement is a key component of the United States planning and contracting system. The criteria stipulate that risk management should be included in each phase of the program life cycle, from the definition of operating requirements. All program participants - managers, engineers, and contractor employees - should maintain risk registers, assess the likelihood and impact of risks, appoint those responsible for mitigating them, and carry out ongoing monitoring.

This is achieved through the active use of digital technologies, namely the Earned Value Management technique, which allows you to detect temporary and financial aberrations in advance. Legislative safeguards, such as the Anti-Deficit Act, which prohibits spending beyond allocated funds and establishes personal responsibility, and the Nunn-McCurdy Amendment, which mandates reporting to Congress in the event of significant spending overruns, provide additional discipline. Strong external control is another key component of American strategy: independent inspections of defense contracts are conducted by the Defense Contracts Audit Agency and the Government Accountability Office, which also confirm costs and detect inefficiencies and fraud (Makarenkov & Kosa, 2024).

The United States is experiencing a systemic digitalization of defense procurement. Well-known platforms such as SAM.gov and PIEE (Procurement Integrated Enterprise Environment) automate the processes of announcing, concluding, and monitoring contracts, as well as offering real-time control, analytics, and access to historical data. High-precision audits are made possible by integrating data with other information systems. Contractors must simultaneously have anti-corruption compliance strategies, including integrity rules, internal control systems, conflict of interest detection processes, and frequent training of personnel. The danger of corruption, collusion, or financial abuse is greatly reduced by such programs, which are checked both during the selection process of the supplier and during the execution of the contract. Internal processes, digital technologies, external audits, and years of institutionalized experience in managing defense contracts form the basis of the entire US system (Stetsenko, 2025).

In the EU, competitiveness, openness, and compliance with standardized rules are directly related to risk management in defense procurement. The general European criteria for defense tenders are laid down by the 2009/81/EC Directive, namely on open procedures, even in the style of negotiation, and mandatory public statements on proposed procurement. While allowing national security interests to be taken into account, the directive also introduces several safeguards, including flexible but regulated competitive procedures, requirements for the security of supply and protection of classified information, special conditions for research and development, and mechanisms for promoting competition in supply chains, in particular through the obligation to engage subcontractors (Mik, 2024).

One of the most important risk mitigation tools in modern EU practice is digitalization. Electronic defense procurement systems that offer automatic review of tenders, reporting, submission, and announcement of tenders are used in many countries. Electronic registries of suppliers and contracts made it possible to track previous performance, identify systematic problems, and avoid duplication of procurement and collusion. The best exchange of data between national procurement agencies, in particular about unscrupulous suppliers and cases of collusion on tenders, is facilitated by the assistance of the European Commission in the development of standard IT systems.

Compliance with anti-corruption legislation is also crucial. Firms bidding for contracts must adhere to moral principles, report no conflicts of interest, and show they are a well-run company. Integrity rules, internal controls, and protocols for reporting violations are part of the internal compliance processes that many countries require of contractors. Accounting chambers, inspections, special agencies, and antimonopoly bodies exercise constant control at the federal level. For example, Germany's defense contracts worth more than 25 million euros require parliamentary approval, which guarantees political and financial supervision, while the UK has an independent regulator, SSRO, which monitors the price of non-gender contracts (Kussainov et al., 2023). Although the European model is less technically unified, it is based on the same ideas: interstate cooperation, digital surveillance, legal responsibility and transparency of procedures. Competition, electronic tools, and compliance programs create a tiered system to stop abuse and reduce the risk of monopolization, corruption, and waste.

Discussion

Ukraine is aggressively changing the structure of defense procurement, which is especially important now when a full-scale conflict is brewing. The system is still susceptible to violations and needs a systematic rethinking, even with the adoption of the new Law "On Defense Procurement" and the creation of specialized organizations such as the State Defense Procurement Agency, the Logistics Agency of the Ministry of Defense and the Anti-Corruption Council under the Ministry of Defense. Inadequate digitalization of processes, poor integration of risk management mechanisms into real activities, and inconsistent implementation of the anti-corruption compliance program by the government and suppliers are among the main obstacles.

The most illustrative are cases where formal contractor due diligence procedures lead to the signing of contracts without taking into account objective risks. As an example, consider the case of the purchase of ammunition in 2023, when the corporation did not have enough production capacity, and the product was faulty. Despite the overall risk management criteria, no thorough supplier analysis, technical audit, or financial assessment has been carried out, suggesting a lack of an organized approach to due diligence. Such errors have serious consequences during the war, not only in terms of monetary losses but also because they can directly jeopardize the combat capability of defensive forces (Sobko et al., 2023).

In this regard, the digitization of defense procurement should serve as the basis for the implementation of the most modern standards of risk management, accountability, transparency, and integrity, and not just an automation tool. The first step is to create a single digital cycle that integrates every stage of the procurement process, from planning and analyzing requirements to monitoring contract performance. The creation and adoption of departmental regulations (guidelines) on risk management in defense procurement that meet the NATO ARAMP-1 standard is an important first step. Clear guidance on identifying risks, assessing their effect and likelihood, appointing responsible parties, deciding on appropriate response measures, establishing risk registers, and tracking them over time should be included in such a document. These processes should be incorporated into a digital platform that provides status tracking, analysis of important supply chain points, and real-time risk collection and updating. With data visualization, automated risk indicators, and links to financial and contract data, such a system

should serve as a dashboard for the leadership of the Department of Defense, defense departments, and regulatory agencies. In addition to improving the quality of managerial choices, this will result in individuals being held accountable for their inaction in response to identified dangers (Astramowicz-Leyk et al., 2023).

For non-classified categories, it seems appropriate to simultaneously restore and expand the use of electronic procurement. Having developed a separate module for military procurement with limited access and open fields for important information (product category, quantity, term, and selected supplier), the Prozorro system can already be modified for defense needs. The introduction of such a module will significantly reduce the likelihood of overpricing, collusion, and discrimination of competitors. In addition, analytical methods for assessing supplier integrity should be incorporated into digital systems. These tools should be based on the past participation of suppliers in tenders, the number of terminated contracts, the frequency of victories in the same procedures, and the presence of corruption scandals. Methodical application of anti-corruption compliance should be the main direction of action. This involves not only the creation of official anti-corruption units but also ensuring that participants in defense tenders have independent internal investigation procedures, personnel training, methods of preventing conflicts of interest, and internal rules of integrity. Companies with a dubious reputation or opaque ownership structure may be prohibited from participating if the relevant criteria are included in the tender documentation and automatically verified by an integrated database.

Ukraine should take measures to create an autonomous department for auditing defense contracts at the institutional level. This unit can operate at the Accounts Chamber, the State Audit Service, or even as a separate organization (like the US DCAA). Such a unit should have access to all data of digital contracts, have the technological capabilities to conduct a thorough study of pricing, monitor the correspondence of value to market levels, and identify evidence of collusion or inflated margins. A parliamentary report on the risks of defense procurement could be implemented in the future. The Ministry of Defense will report quarterly or half-year to the Verkhovna Rada Committee on National Security on the most risky programs, complex contracts, and the implementation of previous recommendations (Sanders, 2023). Institutional growth must go hand in hand with digital change. Training on risk management, digital procurement analysis, and compliance should be provided to Ministry of Defense and Defense

staff. This could include unique courses modeled on Ukrainian anti-corruption organizations, training under NATO programs, or Twinning partnerships with EU countries. The training should include both fundamental modules and specific topics such as data analysis, anomaly detection, creation of a monitoring system, and information visualization.

Equally important is the participation of international partners in the development of a single digital infrastructure. G7, EU, and NATO countries through the Comprehensive Assistance Package (CAP) offer ready-made solutions (information platforms, compliance modules, and risk analysis algorithms) that can be adapted to the needs of Ukraine. It is crucial to include foreign aid in current or new digital procedures rather than creating parallel systems. For example, in addition to methodological assistance, the European Defense Agency, the European Anti-Fraud Office (OLAF), and UK defense spending control institutions may offer access to uniform supplier registers, risk indicators, and price anomaly monitoring procedures (Poliova et al., 2024).

In addition to technical cooperation, it is critical to ensure institutional independence and political support for the digital transformation of defense procurement. Only if advanced digital technologies truly influence decision-making, access to complete contact information, and protection from administrative or political pressure can such changes be successfully implemented. For this reason, digital technologies and parliamentary and public monitoring procedures should act in tandem. Public anti-corruption groups such as TI Ukraine and NAKO, as well as the relevant committee of the Verkhovna Rada, can become valuable employees in overseeing the implementation of new policies and practices.

In light of the above, we can say that for the effective adaptation of international standards in the field of military procurement, they must be divided into those that can be fully, partially, or only after significant modification applied in Ukraine. Using this method, the danger of formal use of models that do not meet the requirements of martial law, limited resources, and institutional capabilities is avoided. Individual provisions of the ARAMP-1 (such as the risk assessment matrix and the principles of responsibility allocation) and components of the AQAP-2070 (such as feedback mechanisms, incident management, and internal control of suppliers) are now among the standards that can be applied in practice. Including them in internal instructions for clients or as a necessary qualification

for contractors is a good idea.

Through the development of a digital contract database, pricing monitoring modules, and performance analytics, other standards such as DCAA audits or GAO reporting can be gradually implemented. Since the full implementation of such technologies requires the training of personnel and the creation of technological infrastructure, this is possible in the middle of the future. Last but not least, some standards, which are based on long-term budgeting, legislative reports, and complex multilevel verification (as in the US or Germany), can be used as benchmarks for the future, but cannot be adopted immediately. By using a clear implementation strategy, you can avoid unnecessary bureaucracy and focus on making changes that are feasible and useful right away.

To sum up, the new defense procurement system should have a unified integrated design that will include digitization, risk management, and anti-corruption compliance, rather than individual changes. Transparency, predictability, digital reporting, and automated controls to stop abuse should be its cornerstones. In addition to increasing domestic trust in Ukrainian institutions, this strategy will increase the effectiveness of the use of foreign military assistance, accelerate the country's integration into Euro-Atlantic institutions and, over time, strengthen its defense capability.

Conclusions

We need a comprehensive structural restructuring of Ukraine's defense procurement system with an emphasis on digital transformation, systemic risk management, and the introduction of modern anti-corruption compliance initiatives. Despite this, it is sensitive to inefficiency, corruption threats, and reduced trust from both local and foreign partners, even after a series of changes and the creation of new institutions. This scenario is especially risky during a full-scale conflict when the ability of a state to defend itself depends on the efficiency, caliber, and integrity of its supplies.

Contemporary problems, in particular the need for rapid decision-making without compromising accountability, the need for openness without compromising secrecy, constant price fluctuations, and logistical difficulties, are all problems that the existing paradigm does not solve. However, the organizational structure of the Ministry of Defense is still too centralized, departments perform duplicate

tasks, responsibilities are not clearly defined, and digital technologies are used inconsistently. Delays, overpricing, inefficient use of resources, and arbitrary judgments that are often not properly controlled are all made possible by this.

Only a comprehensive risk management system built on digital analytics, transparency, and compliance can guarantee the effectiveness of defense procurement, as demonstrated by the experience of NATO member countries, including the United States and the EU. Risk registries, centralized supplier databases, real-time audit systems, and mandatory internal integrity rules are all included in the computerized platforms of these countries. They reduce the human factor, identify violations in advance, and ensure that everyone involved in the process is held accountable.

With the adoption of the Law "On Defense Procurement", the creation of specialized institutions, and the political will to change, Ukraine already has the foundation for the implementation of these strategies. Only by moving to a comprehensive digital architecture, from planning to contract execution, can we make further progress. It is necessary to introduce mandatory risk assessment at all stages, digital registers of decisions and risks, independent audits with access to all data, and make the availability of anti-corruption compliance programs for suppliers a mandatory requirement for participation in tenders. Political support, involvement of foreign partners, and development of institutional capacity for their implementation are necessary for these reforms to be successful.

In addition to eliminating the possibility of corruption, a thorough review of the defense procurement system should increase the efficiency of the use of resources, strengthen the country's defense capability and attract sponsors and friends. This is especially true in the light of future Euro-Atlantic integration, when compliance with global norms of accountability, openness and integrity is an extremely important requirement.

Integrating digital technologies into a unified and comprehensive process is crucial for minimizing risks and ensuring accountability across all stages of defense procurement. This approach underscores the direct relationship between digitalization and the mitigation of corruption risks, emphasizing the need for a holistic implementation from initial planning to final reporting rather than a phased or fragmented one. At the planning stage, integration with logistics databases and real-time information from the front line enables the Armed Forces of

Ukraine to collect and assess needs based on verifiable data rather than subjective administrative or political considerations. The use of analytical modules at this stage facilitates the prediction of shortages, prevents duplication of orders, and curbs unjustified budget expenditures.

During the tender announcement phase, digital systems enhance transparency by clearly presenting conditions and automatically verifying conflicts of interest, contractor histories, and potential corruption threats. When qualification requirements and bids are published through open API electronic platforms, the opportunities for manipulation in supplier selection are significantly reduced. In the evaluation of bids, algorithmic tools help identify inflated or irrational pricing by cross-referencing proposed costs with current market rates and automatically flagging anomalies. These systems also integrate with contractor registries to ensure that only qualified and compliant participants are considered.

Supply control is strengthened through real-time digital tracking of delivery statuses using geolocation data and unique identifiers. This allows for visualization of supply chain bottlenecks and generates automatic alerts in the event of delays, thereby reinforcing supplier accountability. Finally, the phase of contract support and audit is enhanced through the integration of contracts with risk registries, integrity indicators, financial monitoring systems, and independent analytical platforms accessible to the Ministry of Defense and legislative oversight bodies. This infrastructure enables the early detection of violations before they escalate. By embedding verification mechanisms throughout the entire procurement process, digital integration reduces reliance on manual decision-making, diminishes the influence of human error or bias, and significantly improves the legitimacy and reliability of each purchase.

REFERENCES

Antonyuk, N., & Zinko, I. (2023). Cooperation between Ukraine and the European Union within the framework of the Common Security and Defense Policy of the EU. *Language – Culture – Politics, 1*(1), 247–270. https://doi.org/10.54515/lcp.2023.1.247-270

Antonyuk, O.I. (2023). *Interaction between government bodies and the private sector in combating corruption under martial law in Ukraine.* Chernivtsi: Yuriy Fedkovych Chernivtsi National University.

Astramowicz-Leyk, T., Nagornyak, T., Natalina, N., Osmolovska, A., & Yurkovsyi, V.

(2023). Anti-corruption policy in Ukraine during the war with Russia. *Prawo i Więź, 3*(46), 551-575. https://doi.org/10.36128/PRIW.VI46.660

Baillie, L., Dion, E., Leroux-Martin, P., Platz, I., Taylor, W.B., & Trenkov-Wermuth, C. (2024). *The future of the security sector in Ukraine.* Washington: United States Institute of Peace. Retrieved from https://eurasia.ro/wp-content/uploads/2024/10/future-security-sector-ukraine.pdf

Kussainov, K., Goncharuk, N., Prokopenko, L., Pershko, L., Vyshnivska, B., & Akimov, O. (2023). Anti-corruption management mechanisms and the construction of a security landscape in the financial sector of the EU economic system against the background of challenges to European integration: Implications for artificial intelligence technologies. *Economic Affairs, 68*(1), 509-521. https://doi.org/10.46852/0424-2513.1.2023.20

Makarenkov, O., & Kosa, V. (2024). Forensic Technique for Identifying Corruption Challenges to National Security through Digital Technologies. *Baltic Journal of Economic Studies, 10*(4), 288-300. https://doi.org/10.30525/2256-0742/2024-10-4-288-300

Mik, T.B. (2024). Corruption in defense procurement: Key threats and mechanisms to overcome them to ensure the national security of Ukraine. *Effectiveness of Public Administration, 1*(78/79), 71-76. https://doi.org/10.36930/507811

Pakhachuk, Ya.Y., Abramov, A.P., & Cherevatyi, T.V. (2025). Prospects for implementing foreign risk management experience in Ukrainian defense procurement legislation. *Achievements of the Economy: Prospects and Innovations, 14*, 1-25. https://doi.org/10.5281/zenodo.15023442

Petrunyak, E.V. (2023). Anti-corruption program as the basis of counteracting corruption in the financial sector. *Academic Visions, 26*, 1-8. https://doi.org/10.5281/zenodo.14950177

Poliova, N., Polova, L., Stepanenko, S., Izmailov, Y., Varenyk, V., & Akimov, O. (2024). Organizational and economic principles of financial monitoring of national business entities in the context of national security. *Edelweiss Applied Science and Technology, 8*(6), 1455-1466. https://doi.org/10.55214/25768484.v8i6.2262

Rusina, Yu.O. (2025). State financial control: Martial law period main challenges. *Actual Problems of Economics, 2*(284), 148-160. https://doi.org/10.32752/1993-6788-2025-1-284-148-160

Sanders, D. (2023). Ukraine's third wave of military reform 2016–2022 – Building a military capable of defending Ukraine against the Russian invasion. *Defense & Security Analysis, 39*(3), 312-328. https://doi.org/10.1080/14751798.2023.2201017

Shkola, V.Yu., & Bakin, M. (2024). In V.Yu. Shkola, & M.D. Domashenko (Eds.), *Mechanisms for countering modern challenges and threats: EU experience for Ukraine: Materials of the international scientific and practical conference* (pp. 197-200). Sumy: Sumy State University. Retrieved from https://essuir.sumdu.edu.ua/handle/123456789/96627

Shterma, T.V., Lukivskyi, A.S., & Lukivskyi, S.D. (2025). Introducing artificial intelli-

gence into economic management models to minimize corruption risks. *Achievements of the Economy: Prospects and Innovations, 15*, 1-22. https://doi.org/10.5281/zenodo.14959270

Sobko, G., Shchyrska, V., Volodina, O., Kurman, O., & Semenohov, V. (2023). International anti-corruption concepts and their implementation in Ukraine. *Novum Jus, 17*(2), 219-249. https://doi.org/10.14718/NovumJus.2023.17.2.9

Stetsenko, I. (2025). Experience of NATO countries and Ukrainian realities regarding the activities of counterintelligence agencies in the state system of information security assurance. *Global Scientific Trends: Economics and Public Administration, 1*(1), 47-56. https://doi.org/10.5281/zenodo.14812097

Transparency International. (2024). Corruption perceptions index. Retrieved from https://www.transparency.org/en/cpi/2024

Zaremba, O.O., & Lusta, A.A. (2021). Anti-corruption audit as a factor of economic growth of the country. In *Modern directions of scientific research development: Proceedings of VI international scientific and practical conference* (pp. 921-925). Chicago: BoScience Publisher.

Zhuravel, V.V. (2024). *Public finance management in wartime.* Zaporizhzhia: Zaporizhzhia National University.

Global challenges in the regulation of international flights: analysis of Ukrainian criminal law in the context of international security and cooperation

by Ruslan Orlovskyi[1], Vasyl M. Kozak[2], Viktoriia Bazeliuk[3]

Abstract. In today's world, where international flights are an integral part of international travel, it is extremely important to coordinate international relations in this area and regulate flight safety. Working together to create international standards and regulations is essential to ensure the efficiency and safety of international flights. Examining Ukrainian criminal law in the context of global security reveals opportunities and risks for preserving airspace security and cooperating with other countries in this area. Systemic and structural analysis, special legal approach and dialectical method were used to study global issues of international flight regulation. These methods made it possible to systematize certain components of aviation security legislation and develop tactics to improve its effectiveness. The goal of the research is to examine Ukraine's criminal legislation in terms of current international aviation security issues. This is aimed at developing effective strategies for managing counter-terrorism and ensuring flight safety. The analysis of legislation will determine its readiness to respond to these challenges.

Keywords: transport, international flights, security, international law, cooperation, legislation.

Introduction

The topic of international flights is particularly significant at this point in the development of transport links since it may be possible to travel large distances rapidly with their assistance. Their importance has led

1 Department of Criminal Law, Yaroslav Mudryi National Law University, 61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine.

2 Central Office of the Security Service of Ukraine, 01601, 33 Volodymyrska Str., Kyiv, Ukraine.

3 Department of Criminal Law, Yaroslav Mudryi National Law University, 61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine.

NAM, Anno 6 – Special Dossier
DOI: 10.36158/97912566922176
Ottobre 2025

to the need for special international legal regulations to guarantee flight safety. Given the great importance of international flights in the world, it can be noted that their role is also important for Ukraine as a subject of international law and a participant in international relations. The developed rules of international air law have also influenced the development of national legislation in this area, including in Ukraine. Given the great importance of international flights, it is necessary to examine the specifics of their regulation by Ukrainian legislation.

The regulation of international flights is a complex and multifaceted process that faces various global challenges. One of the most significant issues is ensuring the safety of international flights. This includes preventing terrorist threats, protecting against hostile acts that may threaten airspace, and ensuring the safety of passengers and crews. Effective regulation of airlines, flight safety, and service standards are necessary due to the quick advancement of aviation technology and the increase in passenger traffic.

The global nature of the aviation industry requires states to cooperate to develop international standards, rules and procedures for international flights and to combat common problems such as terrorism and cross-border crime. Protecting the rights of individual passengers and consumers is another important challenge in regulating international flights. This includes the rights to safety, affordability and adequate service during international travel. These and other global challenges require an integrated approach and cooperation between governments, international organizations, airlines and other stakeholders to ensure the safety, efficiency, environmental sustainability and protection of passenger rights in international flights.

It should not be forgotten that crimes in the field of international flight safety remain relevant not only due to the specifics of the aviation sector (enhanced customs control, qualification requirements for employees, etc.) but also due to the difficult geopolitical situation in which Ukraine finds itself when strengthening the air border is one of the priorities in preserving the national security of the state.

Given the universality of safety standards, an analysis of Ukraine's criminal legislation in the area of aviation safety in the context of international security and cooperation is especially important. International standards reflect the generally accepted principles of fighting crime. Analysis of legislation helps to identify

compliance or gaps that may affect international security.

Many scholars have studied aviation and flight regulations. Vysotska (2023) examined the theoretical foundations of the strategic development of air transport by analyzing contemporary scientific literature, the aviation industry's development, and trends in the global market for air transport services. The main goal was to find the most effective ways to strategically develop and optimize the interaction between airlines and airports. The analysis identified a set of paradigms to maximize the industry's aggregate potential and enhance its development in the face of global challenges. Polishchuk and Hurin (2023) identified sustainable development goals in aviation safety at the international and national levels. Using various research methods, they found that aviation safety is linked to economic and technological development, infrastructure, and environmental aspects. The results point to the need for continuous improvement of the regulatory environment to ensure aviation safety.

The current status of aviation security and strategies for improvement were examined by Filik (2020). The study was conducted using various methods, such as analytical, comparative legal, systemic, and others. It is concluded that in order to guarantee the safety of civil aviation in high-risk countries, it is important to enhance the systems for handling emergencies and to start the process of establishing an international aviation regulator. Banchuk-Petrosova (2020) analyses the problems in international air passenger transportation and suggests ways to improve legislation. In particular, the author points out the need to improve crisis response and amend the Criminal Code of Ukraine regarding air transport safety. The author emphasizes the importance of adopting the Aviation Transport Strategy until 2030 to ensure safety in air transport. Polyanskaya (2021a) completed research on how the government regulates aviation and formulates development plans for the industry. As a result, it was discovered that the legal system plays a crucial administrative role in the advancement of air travel. The discussion focuses on the importance of state policy in this area for achieving strategic goals.

The study's goal is to analyze Ukrainian criminal law in light of global cooperation and security concerns, with an emphasis on the difficulties in enforcing international aviation regulations. The study is aimed at identifying effective strategies for managing these challenges, in particular in terms of counter-terrorism, ensuring security on board aircraft and preventing crime in the aviation

sector. An analysis of Ukrainian criminal law in this context will help to understand how it adequately addresses these global challenges and to what extent it can respond to them.

Materials and Methods

The author employed a number of general scientific and specialized research techniques that are inherent in legal science in order to accomplish the goal and meet the study's objectives. In analyzing global issues of international flight regulation, the dialectical method allows us to consider these issues as a complex system of interacting components.

The complex internal structure of the system of criminal law provisions on liability for crimes against flight safety was made possible by the application of structural and systemic analysis. This approach makes it possible to study not only individual legislative acts but also their interaction and overall impact on the totality of legal provisions. Such analysis helps to identify gaps and contradictions in legislation and suggest ways to resolve them.

The application of the dogmatic method made it possible to thoroughly examine the provisions governing liability for crimes against aviation security contained in the current Criminal Code, as well as to consider amendments to it from the perspective of aviation security. The use of this method allowed us to identify any gaps or inconsistencies in the legislation, as well as to reflect current developments and trends in the field of legal standards of aviation security. It was also possible to conduct a comparative analysis and take into account international norms and recommendations for improving national legislation in this area as a result of studying international aviation security legislation.

The application of the logical and semantic method and the method of "from the abstract to the concrete" helped to formulate and comprehend the terminology used in the field of aviation law. These methods allowed for the formation of derivative terms such as "international flight" and "international air crime", as well as for their clear definitions. As a result of the research, the use of these methods helped to understand some important aspects of aviation law and how it is applied in world practice.

In analyzing certain legal provisions in the field of aviation law, the formal

logical and special legal approaches were used primarily. These methods help to identify and systematize legal provisions and establish their logical sequence. The application of formal logical and special legal analysis has resulted in greater clarity and precision in the interpretation of regulations within aviation law.

The system-functional and system-structural approaches were applied to better understand the fundamentals of flight safety and to create practical solutions to global problems of international flight regulation. These methodologies made it possible to analyze the aviation regulatory system as a whole, with clearly defined functions and interrelationships between its components. The results of this study helped to identify important components of flight safety, as well as to define tactics aimed at improving the efficiency and safety of international transport.

Results

Today, there is no need to prove the importance of aviation in the modern world, as well as the importance of Ukraine's participation in international aviation cooperation. In total, Ukraine is already party to 70 bilateral international air services agreements. It joined the European Civil Aviation Conference (ECAC) in 1999, the International Civil Aviation Organization (ICAO) in 1992, and the European Organization for the Safety of Air Navigation (Eurocontrol) in 2004. In addition, it is a party to the Open Skies Agreement and the Common Aviation Area (CAA) agreement. An agreement on a Common Aviation Area was signed by Ukraine and the EU on October 12, 2021, during the 23rd EU-Ukraine Summit.

This agreement is also known as the Open Skies Agreement, which provides for the opening of the air transport market, new opportunities for consumers and operators, promotion of trade, tourism, investment in Ukrainian aviation, and cheaper tickets. This agreement created an "Air Visa Waiver", which provided for the establishment of close cooperation between Ukrainian airlines and EU airlines and a common aviation area with the EU. This agreement provided for the regulation of Ukrainian aviation law to avoid conflicts with EU aviation law, and obliged Ukraine to bring its aviation legislation in line with EU aviation law (Pagallo & Bassi, 2020).

It is worth noting that before the conclusion of this agreement, the State Aviation Administration of Ukraine, together with Ukrainian legislators, according to the 2020 Aviation Safety Report of the State Aviation Administration of Ukraine,

cooperated with the International Civil Aviation Organization (ICAO) to bring Ukraine's aviation safety legislation in line with international standards. Such cooperation is defined in Section 6, paragraph 46 of the State Program on Civil Aviation Security. There have been times when aviation law reform was carried out with mistakes that cost lives.

First of all, let us note how Ukrainian legislation defines the concept of "international flight". An international flight is defined as a flight that consists of one or more international flight stages, per the Order of the State Service of Ukraine for Supervision of Aviation Safety of the Ministry of Defense of Ukraine "On Approval of the Rules for Granting Operators Permits for Departure from and Arrival at Airports of Ukraine" Nº 897/703 of 2005.

A similar definition can be found in the State Aviation Administration of Ukraine's Order No. 1001 of 2019, "On Approval of the Aviation Rules of Ukraine "Technical Requirements and Administrative Procedures for Monitoring Emissions by Civil Aircraft Operators," which states that a flight qualifies as international if it includes one or more international flight stages.

However, it should be noted that Ukrainian legislation contains other definitions of international flight. For instance, an international flight is defined as one in which an aircraft crosses a state border between Ukraine and another state or one that is conducted in the airspace of another state, per the Order "On Approval of the Rules for Navigational Support of Flights of the State Aviation of Ukraine" (Ministry of Defense of Ukraine, 2016). Thus, even though similar definitions are enshrined in two different legal acts, we still observe a lack of certainty in the understanding of the concept of "international flight", which may be perceived as a legislative imperfection in the relevant issue. It is advisable to include the term under study in the provisions of the Air Code of Ukraine, the primary legislative act in the field of aviation law, in order to systematize legal approaches to its definition, unify approaches to its interpretation, and prevent future contradictions when thinking about issues related to international flights (Bilousov, 2017).

Having analyzed the above definitions, we believe that the most accurate definition is the one set out in the Order of the Ministry of Defence of Ukraine No. 100 of 2016, as it most fully discloses the essence of international flights. In particular, it takes into account the fact that an aircraft crosses the state border of any state, including Ukraine. Therefore, we consider it appropriate to use this

definition for further research.

The concept of maintaining flight safety is the foundation of air law, as it is an essential requirement for aviation. Strict adherence by all states to the principle of safety is an important condition for the further development of international air services, which nowadays play a significant role in strengthening political, economic, cultural and other ties between countries and peoples. One of the aspects of this principle is the prohibition of unlawful interference or criminal encroachment in the field of flight safety. Such crimes are not uncommon in the modern world, often closely intertwined with terrorist acts or international war crimes.

The Tokyo Convention on Offences and Certain Other Acts on Board Aircraft of 1963, the Hague Convention for the Suppression of Unlawful Seizure of Aircraft of 1970, and the Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation of 1971 are three international conventions that were developed in the 1970s on the initiative and under the auspices of ICAO to organize and develop cooperation between states to combat unlawful interference with civil aviation. In 1988, the Protocol to the Montreal Convention of 1971 was adopted, which is aimed at combating unlawful acts of violence at airports serving international flights. Annex 17 of the 1944 Chicago Convention "Safety. Protection of International Civil Aviation against Acts of Unlawful Interference".

These international documents include the following acts: sabotage of air transport, hijacking of aircraft, blackmail, violent behaviour on board, damage to aircraft equipment, etc. In comparison to the Hague Convention, the Montreal Convention has made it clearer and included more violations that could jeopardize civil aviation safety. These violations include violence against passengers aboard an aircraft while it is in flight, damaging or destroying an aircraft while it is in service, interfering with the operation of ground-based air navigation equipment, and disseminating intentionally false information that could jeopardize aircraft safety. States parties to these conventions are obliged to apply severe penalties to all such crimes (Prushkivska et al., 2023).

Nonetheless, there has been a tendency up until now to mainly analyze these crimes in terms of guaranteeing the security of civil aviation. A whole segment of flights operated by military aircraft remains outside the scope of international legal regulation. Therefore, it is necessary to talk about "ensuring the safety of

flights in the airspace over the high seas", which takes into account the interconnection of all subjects of international aviation legal relations, including military aircraft. We should agree with this opinion since military aircraft can also be used by criminals for purposes dangerous to society and the state.

It is also necessary to define an international crime in the field of air law: these are crimes, the criminal punishment of which is provided for by acts of national legislation and international legal acts, intentionally or negligently committed by individuals or heads of organizations or states acting as their subjects, which encroach on the safety of aviation or, through it, on the interests of interstate communication, several states or the entire international community.

In an international crime, similar to a domestic crime, there is a corpus delicti of an international nature, which is a set of objective and subjective features based on which persons are brought to criminal liability. It should be noted that the elements of an international crime do not always coincide with the elements of a crime in domestic criminal law. The elements of an international crime include:

- the object of an international crime, i.e., the benefits of a material or non-material nature, which are encroached upon by an international criminal offence (international law and order, social relations, human rights and freedoms, etc.);
- the objective side of an international crime is manifested in the form of a socially dangerous, unlawful, guilty act committed by a criminal against the object of the crime, which is regulated by international criminal law;
- a person's perspective on the act they performed afterwards reflects the subjective aspect of an international crime;
- the subject of an international crime is a natural person of sound mind who has reached a certain age of criminal responsibility at the time of the crime. The age of criminal responsibility in Ukraine is 16 years old in general and 14 years old in some cases, a comprehensive list of which is given in part 2 of Article 22 of the Criminal Code of Ukraine (CC) (Verkhovna Rada of Ukraine, 2001). However, in foreign countries, the age of criminal responsibility is defined differently (Vysotskaya, 2023).

Aviation security is defined by Ukrainian law as the safeguarding of civil aviation from acts of unlawful interference, achieved via the use of a series of

procedures including both human and material resources. The concept of an act of unlawful interference with civil aviation serves as the definition of aviation security. A threat to the safety of civil aviation is defined as an act of unlawful interference in Chapter 1 of Annex 17 "Security: Protection of International Civil Aviation from Acts of Unlawful Interference" to the Convention on International Civil Aviation (International Civil Aviation Organization, 1944).

This includes the following actions or attempts to act in this way: 1) forcible entry onto an aircraft, airport, or location of an air navigation facility or service; 2) unlawful seizure of aircraft; 3) destruction of an aircraft while it is in operation; 4) taking hostages on board an aircraft or at aerodromes; 5) placing weapons, dangerous devices, or material intended to achieve criminal purposes on board an aircraft or at an airport. The act of using an aircraft while it is in operation with the intent to cause harm, other health damages, death, or major property or environmental damage; 7) purposeful dissemination of false information that jeopardizes the safety of an aircraft while it is in flight or on the ground, as well as the safety of passengers, crew members, ground staff, and other individuals at the airport or at the location of civil aviation facilities or units.

It should be noted that the Convention for the Suppression of Unlawful Acts Relating to International Civil Aviation adds attempts, threats, organizations, and assistance (complicity) in the commission of unlawful acts against international civil aviation to the list of such acts. National legislation regulates relationships about acts of unlawful interference with civil aviation. Specifically, the definition of an act of unlawful interference is found in Article 86 of the Air Code of Ukraine (Verkhovna Rada of Ukraine, 2011a) and subparagraph 6 of paragraph 2 of Section II of the State Program of Aviation Security of Civil Aviation of March 21, 2017, and includes the same actions as those listed in Annex 17 of the 1944 Convention on International Civil Aviation. Criminal law measures are crucial when it comes to ensuring aviation security against acts of unauthorized interference with civil aviation. There is no relevant part in the Ukrainian Criminal Code that lists any crimes against aviation security. (Polishchuk & Hurin, 2023).

The generalized results of the systematic analysis of the current CC allow us to identify an independent subsystem of criminal law support for the protection of aviation security from illegal interference with aircraft operations. Therefore, criminal responsibility for acts of unlawful interference with civil aviation is es-

tablished by the following articles of the Criminal Code of Ukraine (Verkhovna Rada of Ukraine, 2001):

- Article 278 of the Criminal Code, which states, "Hijacking or seizure of railway rolling stock, aircraft, sea or river vessel" (unlawful seizure of aircraft), based on the elements of the criminal actions;
- Article 147 of the Criminal Code "Hostage-taking" (hostage-taking on board aircraft or at airfields);
- Articles 296 and 257 of the Criminal Code "Hooliganism" and "Banditry" (forcible entry on board an aircraft, into an airport, or into the location of an air navigation facility or service);
- Article 277 of the Criminal Code "Damage to means of communication and vehicles" (destruction of an aircraft in operation);
- Articles 263 of the Criminal Code "Illegal handling of weapons, ammunition or explosives", 265 "Illegal handling of radioactive materials", 267 "Violation of the rules for handling explosives, flammable and caustic substances or radioactive materials", 269 "Illegal transportation of explosives or flammable substances on an aircraft," prohibits bringing weapons, dangerous devices, or materials meant to be used for illegal purposes onto an aircraft or at an airport);
- Article 258 of the Criminal Code "Terrorist act" (usage of an aircraft while it's in operation with the intent to harm someone, injure, or cause other health problems, death, or serious property or environmental damage);
- Articles 195 of the Criminal Code "Threat of destruction of property", 259 "Knowingly false report of a threat to the safety of citizens, destruction or damage to property" (providing willfully false information that jeopardizes an aircraft's safety in flight or on the ground, as well as the security of travelers, crew members, ground personnel, and the general public at airports or other locations housing civil aviation facilities or units), etc.

Since there is a special theme in the corpus delicti of these crimes, the legislators in the Ukrainian SSR of 1960 chose to consign crimes against traffic safety and transport operation to the chapter "Official crimes" rather than classifying them separately. In contrast, the Special Part of the current Criminal Code of Ukraine, which consists of 18 articles that establish responsibility for crimes

related to transportation, has a distinct Section XI titled "Crimes against traffic safety and operation of transport. It is important to note that the Criminal Code of Ukraine's Articles 276, 277, 278, 279, 280, and 291 establish liability for breaking traffic safety laws and operating different kinds of transportation (such as motor vehicles, railroads, water, or air transportation), each of which carries a distinct level of liability. Only persons with additional features, i.e. special subjects, can be held liable for criminal offences under Articles 276, 276-1, 281, 282, 284, 285, 287, 288 of the Criminal Code of Ukraine.

This group of crimes also includes the criminal offence under Art. 269 of the CC of Ukraine (illegal transportation of explosives or flammable substances by aircraft). It is interesting to compare Art. 269 of the CC of Ukraine with the version of the Criminal Code of the Ukrainian SSR of 1960. Both provide for liability for the illegal transportation of explosives or flammable substances by aircraft. The disposition of the article of the Criminal Code as amended in 1960 defines the subject of the crime as a passenger. That is, only a special subject could be held liable for committing this offence. Since the subject of the crime is not specified in Article 269 of the CC of Ukraine, any natural person of sound mind who has reached the age of criminal responsibility - that is, a broad subject of the crime - may be held accountable for committing such a crime (Herman, 2023).

Criminal law support for aviation security is established by the articles of the Special Part of the Criminal Code of Ukraine, which are located in different sections depending on the generic object. The Draft Law of Ukraine "On Amendments to the Criminal Code of Ukraine (regarding the improvement of the effectiveness of ensuring the safety of traffic and operation of transport)" was developed taking into account the provisions of the Convention on International Civil Aviation, documents of the International Civil Aviation Organization (ICAO), the Model Criminal Code, as well as the positive foreign experience of the post-Soviet countries (Baltic States), highly developed European countries (Bulgaria, the Netherlands, Denmark, Sweden, Switzerland).

The draft law aimed to align Ukrainian laws regarding criminal responsibility for traffic safety and transportation operations with globally recognized norms, international legal principles, and international standards, to increase the effectiveness of preventing and combating criminal violations of traffic safety or operation of railway, water or air transport, taking into account the positive foreign

experience of post-Soviet countries and highly developed European countries.

The proposed law states that only true, negligent harm to a person's life or health shall be subject to criminal liability under Article 276 of the Criminal Code of Ukraine. After all, practically every violation of traffic safety regulations and transportation operations (as a source of increased danger) theoretically poses a risk to human life or other serious consequences, as they can cause an accident or catastrophe, according to the current version of the disposition of Part 1 of Article 276 of the Criminal Code of Ukraine (Rye, 2023).

Moreover, significant changes were made to Article 416 of the Ukrainian Criminal Code in 2023, which lays out the consequences for breaking flight regulations or failing to prepare for them. From now on, violation of flight rules or preparation for them, as well as violation of aircraft operation rules, are criminal offences not only if these actions caused a disaster or other serious consequences, but also if these actions caused serious bodily harm or material damage on a large scale. Article 417 of the Criminal Code of Ukraine on violation of the rules of navigation was amended in the same way.

The Criminal Code of Ukraine's Article 334 defines the criminal offense of flying into or out of Ukraine without a permit, as well as the consequences of not adhering to the routes, landing sites, air routes, corridors, or echelons that are specified in the permit. These details should be given more consideration in the study. The literature notes that the prohibition of crossing the borderline without the permission of the competent authorities or outside the established rules is a component of the inviolability of state borders. Both general and specific regulations are established by Ukrainian legislation for crossing state borders, with the latter relating to aircraft crossings.

This article is important for international security and cooperation for two reasons. Firstly, it regulates the flights of aircraft across the state border of Ukraine, and violation of these rules can create a threat to airspace security, which can have serious consequences for international security. Adherence to the established routes and other rules ensures flight safety and prevents possible incidents that could disrupt international stability. Secondly, this article establishes procedures for obtaining permits for flights across state borders, which facilitates cooperation between countries in airspace regulation. Effective cooperation in this area contributes to ensuring safety and equality in international flights, which in

turn contributes to strengthening international relations and cooperation between countries (Filik, 2020).

In particular, Art. 9 of the Law of Ukraine "On the State Border" states that crossing the state border of Ukraine must be done by the established procedure. As for aircraft, they must cross the state border of Ukraine on specially designated air traffic routes (Article 32(1) of the Air Code of Ukraine). According to Article 32 (2) of the Air Code of Ukraine, the authorized civil aviation authority discusses with the General Staff of the Armed Forces of Ukraine and the Administration of the State Border Guard Service of Ukraine before approving the list of air traffic routes for crossing the country's state border. Regarding this, it should be mentioned that aviation regulations set forth the protocol for the operation of state and commercial aircraft and are applicable to all persons and organizations operating in the aviation industry and utilizing Ukrainian airspace, irrespective of ownership or departmental subordination. The safety of aircraft is the primary and main risk that arises from noncompliance with aviation regulations.

Thus, the content of the direct object of the criminal offence under Art. 334 of the CC of Ukraine directly derives from the nature of the act - encroachment on two objects. Firstly, the public relations of inviolability of state borders by aircraft. Secondly, it affects public relations in the field of aircraft safety, which are violated as a result of non-fulfilment or improper fulfilment of aircraft flight rules: failure to comply with the routes, landing sites, air routes, corridors or echelons specified in the permit. Since the primary direct object is a component of the generic object, social relations in the context of the inviolability of the state border of Ukraine should be regarded as the primary direct object of the criminal offense under Art. 334 of the Criminal Code of Ukraine, "Violation of International Flight Rules," which prevents crossing the state border of Ukraine by aircraft without authorization from permitted civil aviation authorities or in violation of the established procedure (rules) for crossing the state border of Ukraine by such aircraft. (Dobrovolsky, 2023).

An additional direct object of this criminal offence is public relations in the field of flight safety of aircraft, which are violated as a result of non-fulfilment or improper fulfilment of flight rules, along with the main direct object - public relations in the field of inviolability of the state border of Ukraine. Article 334 "Violation of international flight rules" of the Criminal Code of Ukraine (CCU)

provides for liability for flying into or out of Ukraine without a permit, as well as for failure to comply with the routes, landing sites, air routes, corridors or echelons specified in the permit. Illegal entry into or departure from Ukraine represents one of the objective aspects of this criminal offense.

The Contracting States recognize that each State has complete and exclusive sovereignty over the airspace above its territory under the terms of the Convention on International Civil Aviation. (Article 1). No State aircraft belonging to a Contracting State may fly over or land on another State's territory unless permitted by a particular agreement or under its terms. (Article 2(c). International treaties, standards, recommended practices of the International Civil Aviation Organization, documents of the European Organization for the Safety of Air Navigation, and EU legislation are used to regulate and legitimize the use of airspace in international airspace.

The procedure for issuing permits to Ukrainian and foreign operators for international scheduled flights departing (arriving) from Ukraine (to Ukraine) is established by the Rules for Issuing Permits to Operators for Departure from and Arrival at Ukrainian Airports (Rules). In particular, the procedure for Ukrainian operators to obtain a permit for departure from and arrival at Ukrainian airports when operating international non-scheduled flights is set out in Section 3 of these Rules. Section 4 of these Rules specifies the process for obtaining a permit for a foreign operator to operate international non-scheduled flights into and out of Ukrainian airports. In addition, for foreign operators, the Rules provide for the procedure for obtaining permits for international scheduled transit flights without landing and with a technical landing at Ukrainian airports (clause 5) and the procedure for obtaining permits for international non-scheduled transit flights without landing and with a technical landing at Ukrainian airports (clause 6) (Banchuk-Petrosova, 2020).

By the Law of Ukraine "On the State Border", the state border of Ukraine is crossed on the routes of communication across the state border in compliance with the established procedure. This Law, additional legislative acts, as well as regulations made by authorized government agencies in Ukraine and published by the specified method, all permit aircraft to cross the state border of Ukraine in specifically designated air corridors. Only with authorization from the approved state bodies of Ukraine it is permitted to fly over the country's state boundary out-

side designated air corridors. (Article 9). Airports (aerodromes) that are available to international flights are where aircraft from both Ukraine and other countries depart and land. These airports also include customs offices and border patrol posts. Additional procedures for aircraft takeoff and landing are only permitted with authorization from Ukraine's relevant authorities. (Article 10) (Dobrovolsky, 2023).

Part Three of Article 29 of the Air Code of Ukraine (Verkhovna Rada of Ukraine, 2011a) states that aircraft departures and arrivals into Ukraine are permitted through international airports housing the country's customs and state border protection agencies. In exceptional circumstances, with the approval of the Ukrainian Cabinet of Ministers, or in the event of an aircraft's forced landing, departure of an aircraft or arrival of an aircraft through other airports and beyond the location of customs and state border protection authorities of Ukraine are permitted.

According to Article 32 of the Tax Code (Verkhovna Rada of Ukraine, 2011b), aircraft must follow the protocol set forth in the Regulation on the Use of the Airspace of Ukraine in order to cross state borders. These procedures apply to specifically defined air traffic routes, the details of which are provided in papers containing air navigation information. Clause 51 of the Regulation on the Use of the Airspace of Ukraine states that aircraft are not allowed to cross state borders outside of specifically established air traffic routes, unless the Air Code of Ukraine provides otherwise (clause 52).

According to Article 2 of the Constitution of Ukraine, the territory of Ukraine within its existing borders is integral and inviolable. The inviolability of the border includes two components: 1) the inviolability of the border line itself on the territory marked by border (boundary) signs; 2) the prohibition of crossing the borderline without the permission of the competent authorities or outside the established rules (Gutsal et al., 2020).

Article 9 of the Law of Ukraine "On the State Border" declares that aircraft and other aircraft that have crossed the state border of Ukraine without proper permission from the competent authorities of Ukraine or have committed other violations of the rules of flight across the state border of Ukraine are violators of the procedure for crossing the state border of Ukraine in airspace (violators of the state border of Ukraine). The regulations governing the crossing of Ukraine's

state boundary are not considered to have been broken by aircraft entering the country under duress or in other exceptional situations. In the event of significant accidents, natural disasters, or other emergencies, emergency rescue teams enter Ukraine through its state borders in order to locate and eradicate these situations in accordance with the protocol established by the Cabinet of Ministers of Ukraine through international treaties.

Emergency rescue and disaster recovery units may cross the state border of Ukraine in accordance with the conditions set by the UkSATSE in consultation with the Ministry of Foreign Affairs in order to carry out international treaties on aiding other states in the event of emergencies caused by major accidents, catastrophes, and natural disasters. This request may be made by the Ministry of Emergency Situations (Likhitchenko, 2020).

Discussion

The regulation of international flights is a complex, multifaceted process that addresses numerous global issues. Ensuring the safety of international flights is an important aspect of maintaining global airspace security and involves several factors that require careful consideration and in-depth research.

One of the top priorities is to stop terrorist attacks in airspace. Terrorist organizations may attempt to carry out terrorist acts, such as hijacking or bombing aircraft, using aviation as a tool. Developing and implementing security plans is crucial. Some of these include tightening passenger control, updating airport security equipment and increasing cooperation between security services.

Hostile acts such as a military attack, missile strike or other act of violence can also pose a threat to airspace. Several key tactics to ensure airspace protection include the establishment and use of early warning, defence and incident response systems, as well as improved coordination among international security agencies.

In addition, the safety of passengers and crew members requires special attention. This includes protecting them during transport and responding to any incidents, theft or threats. Existing regulatory and supervisory systems are under threat due to the growing number of flights and passengers. It is crucial to develop and implement new approaches and protocols that meet modern requirements and guarantee a high level of security.

Cybersecurity is becoming increasingly important as the aviation sector becomes more and more dependent on digital technologies. The safety of aircraft, passengers and crews can be seriously compromised by hacker attacks on air transport systems. It is important to develop and implement effective cyber defence plans and tools. To ensure their safety and compliance, new technologies such as drones, automation systems and autopilots must be constantly monitored and regulated (Mendala & Tokarska, 2021). Increased competition between airlines may also force them to cut costs and increase productivity, which could negatively impact safety. It is crucial to ensure that savings do not compromise service quality and safety. Airlines, government agencies, aviation associations and other stakeholders should actively cooperate to address these issues. To guarantee the efficiency and safety of international flights, it is crucial to continuously improve the regulatory framework and standards.

As the aviation industry is international, cooperation between states is necessary on many fronts to ensure the sustainability, efficiency and safety of this vital industry. First and foremost, cooperation between states is crucial for the establishment of global norms, policies and guidelines governing international aviation. This includes air traffic control protocols, safety regulations, aircraft technical specifications and cooperation between sovereign airspaces. Secondly, states must work together to address common challenges, such as terrorism and cross-border crime, which can jeopardize aviation security. Coordinating airport and airspace security measures, developing joint tactics to combat terrorism in airspace, and sharing information on suspicious persons or activities are some examples of what such cooperation might include.

The establishment of international cooperation institutions, such as the International Civil Aviation Organization (ICAO), which serves as a platform for the discussion and adoption of standards and recommendations for aviation efficiency and safety, is essential to ensure successful cooperation between states. The interests of all parties, including airlines, airports, international organizations, and other stakeholders, must be taken into consideration while developing and putting into practice international standards and safety measures in the aviation industry (Abeyratne, 2023). In the context of globalization and increasing international travel, the protection of the rights of individual passengers and consumers in the aviation sector is becoming increasingly important. To guarantee the rights of passengers to safety, affordability and an adequate level of service when

travelling internationally, states must cooperate to set and enforce standards.

First, international standards, rules and procedures for aviation safety need to be developed to ensure the safety of every passenger while on board. This includes personnel qualifications, aircraft maintenance standards, safety protocols and regular inspections to ensure that standards are met. Secondly, protecting their rights also means ensuring that passengers are properly served and accessible. This includes ensuring a comfortable stay and onboard services such as food, communication and other amenities, in addition to the availability of tickets and seats on different routes. Setting service quality standards and taking measures to ensure that they are met is crucial to this end.

States should work together internationally to create and enforce appropriate laws and controls to ensure that the rights of every passenger and consumer are effectively protected when travelling internationally. In addition, to ensure that the requirements of individual passengers are taken into account when setting international standards, it is essential to involve airlines and the general public in the policy-making process. As air travel expands and hazardous material emissions increase, it is crucial to reduce the environmental impact of aviation. New standards and technologies need to be created and implemented for the sustainable development of the aviation sector. First and foremost, it is critical to continue developing more environmentally friendly aviation fuels and engine technologies. The use of biofuels and electric or hybrid engines that produce less CO2 and other air pollutants are examples of this. Second, measures need to be taken to reduce noise pollution caused by aircraft engines and flights. This may involve developing acoustically efficient aircraft materials, improving take-off and landing protocols, and using quieter and more efficient technologies.

In addition, it is crucial to encourage the aviation business to take energy-saving and emission-reduction initiatives and to maintain transparency and oversight of the environmental activities of air carriers. Reducing the environmental impact of aviation will require significant international coordination and cooperation. This involves the commercial sector, international organizations, and nations actively participating in the creation and execution of aviation-related environmental strategies and programs.

To guarantee the security, efficiency, environmental sustainability and protection of the rights of passengers of international flights, governments, internation-

al organizations, airlines and other stakeholders must work together to address these global challenges in a comprehensive manner (Polishchuk & Pasko, 2020). The effective fight against crime and the maintenance of civil aviation security depends on the extent to which national criminal law is in line with international standards in the field of international aviation security. The severity of criminal penalties should be sufficiently high to deter the commission of aviation security offences. This may include harsher penalties for acts of aviation terrorism and other risks. Cooperation between countries is crucial in the fight against transnational crimes that threaten aviation security. Information exchange, joint investigations, and extradition of suspects or convicted persons are some examples.

To guarantee the same level of security and fight against crime, countries can cooperate to harmonize their aviation-related criminal codes. Supporting victims and their families is just as important as preventing crime. This may include other services such as psychological assistance and compensation plans. The country's commitment to international cooperation and aviation security is reflected in its efforts to bring national legislation into line with international norms. This promotes international standardization of laws and practices, which reduces the likelihood of criminal acts and increases flight safety.

With the development of globalization and Ukraine's integration into international aviation structures, the relevance of implementing the European Aviation Safety Agency (EASA) standards into the national legal system is becoming an integral part of ensuring the safety of aviation space and maintaining high standards in aviation security. In addition, the martial law that is currently in place in Ukraine presents unexpected challenges in all areas of life, including aviation security. Nonetheless, it is still a top concern to legally translate European Aviation Safety Agency (EASA) regulations into Ukrainian law.

The European Aviation Safety Agency (EASA) plays an essential role in defining and ensuring safety standards for the aviation industry in the European Union. Through its expertise and expert opinions, EASA develops regulations and recommendations aimed at ensuring flight safety and unifying aircraft certification standards. Ukraine, which is actively developing its aviation sector, feels the need to implement EASA standards to maintain high safety standards and compatibility with the European aviation area. This is important to ensure passenger safety, increase the competitiveness of airlines, and facilitate Ukraine's

integration into the European aviation area (Polyanska, 2021a).

Martial law conditions require a strategic approach to the implementation of EASA standards. It is important to ensure continuous monitoring of the compliance of national standards with international requirements and to develop flexible mechanisms to adapt to changes in the context of Russia's aggressive attack. The process of implementing EASA standards into the legal system of Ukraine involves amending national legislation and establishing mechanisms for interaction between national and international aviation authorities. An important step is the harmonization of standards, which involves the adaptation of national legal acts to EASA requirements.

The implementation of EASA standards faces several challenges, such as the need to reform existing legislation, provide staff training and use appropriate technical resources. However, the successful implementation of this process will open up new prospects for Ukraine to cooperate with its European partners and improve safety in the aviation industry. Ensuring high safety standards in aviation is a priority for any country seeking to actively develop the aviation sector. The introduction of the European Aviation Safety Agency (EASA) standards into the Ukrainian legal system is a strategic step in this direction. This ensures a high level of safety for passengers, improves the quality of air transport services and facilitates the country's integration into the common aviation area.

The martial law conditions underline the importance of international cooperation. Ukraine should actively engage with international organizations, including EASA, to share best practices and receive support in times of war (Polyanska, 2021b). There are challenges in implementing EASA standards in Ukraine, but they can be addressed through careful study and adaptation of legislation, engagement of highly qualified personnel, and use of appropriate technical resources. The process of harmonization of standards contributes to the establishment of a unified security system that meets international requirements and standards, which contributes to the increase of confidence in the aviation sector of Ukraine.

Successful implementation of EASA standards in Ukraine opens up prospects for in-depth cooperation with European partners, exchange of best practices and participation in European aviation safety programs. This stimulates the development of the aviation sector, ensuring a high standard of living for the national population and supporting the country's economic growth.

Conclusions

Ensuring flight safety, which is the cornerstone of international aviation law, is essential for the growth of global air traffic. The Tokyo, Hague, and Montreal agreements are examples of international agreements that oversee multiple aspects of aviation safety and prohibit unauthorized interference with civil aircraft. Nevertheless, many aspects, in particular the activities of military aircraft, continue to be outside the scope of global legal regulation and need to be addressed to ensure comprehensive safety and security of flights. About overall safety and security, the importance of "ensuring the safety of flights in the airspace over the high seas", including military aircraft, must be taken into account.

According to Ukrainian law, aviation security is the process of protecting commercial aircraft from unauthorized interference by various means and methods. International regulation of this issue is of great importance. The Convention on International Civil Aviation's Annex 17 provides a more detailed and precise definition of unlawful interference. Ukrainian criminal law establishes liability for such actions, in particular, through the provisions of the Criminal and Air Codes. Aviation security depends on the implementation of criminal law procedures.

The provisions of the Special Part of the Criminal Code of Ukraine, which is divided into several sections, as well as draft laws brought in line with international standards and norms, define Ukrainian legislation in the field of criminal law enforcement of aviation security. This kind of legislation aims to increase the effectiveness of preventing and prosecuting criminal offenses of air traffic safety regulations or air transport operations. The Criminal Code of Ukraine has recently been amended to expand the scope of criminal liability for violation of flight rules, operation of an aircraft without a permit and causing significant harm to health or material damage.

Due to several global issues, the regulation of international flights is becoming increasingly challenging in the modern world. Creating and implementing plans to stop terrorist attacks, protect against hostile actions and compromised air transport systems, and reduce the environmental impact of aviation are all necessary to ensure the safety and efficiency of international flights. Addressing these issues requires active cooperation between states, international organizations and other stakeholders. The creation and execution of global standards and agreements that protect passengers' rights and reduce aviation's environmental

effects are necessary to guarantee the aviation sector's safety, efficacy, and long-term growth. For the Ukrainian aviation system to be safe and integrated into the European aviation sector, it is necessary to implement the requirements of the European Aviation Safety Agency (EASA). While martial law conditions require a balanced approach, the effective application of these recommendations creates new opportunities for cooperation and national growth.

References

Abeyratne, R. (2023). Competency Framework for Civil Aviation Legal Advisers: A Way Forward. *Air & Space, 35*(2), 4-18.

Banchuk-Petrosova, O. (2020). Problems of regulation of international air transportation of passengers and ways to improve the legislation. *Entrepreneurship, Economy and Law, 2,* 351-355.

Bilousov, E.M. (2017). Globalization challenges and their overcoming in the context of ensuring the economic security of the state. In *Innovation System and Information Technology in Modern Science* (pp. 12-20). Kharkiv: Pravo.

Dobrovolsky, A.M. (2023). Shows of foreign subjects of prevention of criminal offenses in the field of aviation. *In the 6th International Youth Scientific Legal Forum* (pp. 226-229). Kyiv: National Aviation University.

Filik, N.V. (2020). Flight safety and issues of improving the mechanism of providing it. *Air and Space Law, 1*(54), 14-19.

Gutsal, I. Yu., Luchok, A.M., & Mironets, O.M. (2020). Theoretical and legal aspects of civil aviation protection against illegal intervention acts. *Legal Scientific Electronic Journal,* (1), 285-287.

Herman, A.L. (2023). *Development of international aviation transportation in crisis*. Kyiv: National Aviation University.

International Civil Aviation Organization. (1944). Convention on International Civil Aviation - Doc 7300. Retrieved from https://www.icao.int/publications/pages/doc7300.aspx

Kleshnya, G.M. (2023). Prospects for overcoming the global challenges of the 21st century in postmodern reality. *Cultural Studies, 37*(1), 28-35.

Likhitchenko, I.G. (2020). Legal regulation of civil aviation flight safety in Ukraine. In *Materials of the All -Ukrainian Conference of Young Scientists and Students "At Air - 2020. Air and Space Law"* (pp. 187-189). Kyiv: National Aviation University.

Mendala, O. & Tokarska, K. (2021). Aviation criminal law regulations of the Tokyo Convention and the penal code to counteract terrorist acts. *Journal of KONBiN, 51*(2), 43-62.

Ministry of Defense of Ukraine. (2016) Order "On Approval of the Rules for Naviga-

tional Support of Flights of the State Aviation of Ukraine". No. 100. Retrieved from https://zakon.rada.gov.ua/laws/show/z0418-16#Text

Pagallo, U. & Bassi, E. (2020). The Governance of Unmanned Aircraft Systems (UAS): aviation law, human rights, and the free movement of data in the EU. *Minds and Machines, 30*(3), 439-455.

Polishchuk, I. & Hurin, A. (2023). Sustainable Aviation Transport Sustainable Development Goals: International and National Legal Regulation. *Air and Space Law, 4*(69), 21-29.

Polishchuk, I.V., & Pasko, A.A. (2020). *Features of legal regulation in the field of civil aviation security*. Kyiv: Air and Space Law.

Polyanskaya, A. (2021a). State Safety of Civil Aircraft Flight Safety. *Scientific Bulletin of Uzhgorod National University,* (68), 190-194.

Polyanskaya, A. E. (2021b). Functionality of legal regulation in the field of air transport. Scientific works of National Aviation University. *Air and Space Law, 1*(58), 23-28.

Prushkivska, E., Prushkivsky, V., & Koptev, O. (2023). Trends in the development of the aviation industry in the conditions of global challenges. *Adaptive Management: Theory and Practice, 15*(30). https://doi.org/10.33296/2707-0654-15(30)-05

Rye, D. (2023). *European integration of the aviation industry of Ukraine*. Kyiv: National Aviation University.

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. (2011a). Air Code of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/3393-17#text

Verkhovna Rada of Ukraine. (2011b). Tax Code of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2755-17#Text

Vysotskaya, M.P. (2023). Conceptual foundations of experiment-strategic development of air transport-Noah's industry in the context of global challenges. U*krainian Applied Economy Journal and Techniques, 8*(4), 352 - 358.

Public administration reforms under martial law in Ukraine: International experience of adapting to hybrid threats

by Oleksandr Kurilets[1], Kateryna Manuilova[2], Oleksii Malovatskyi[3], Olena Pavlova[4]

Abstract. The aim of the study is to analyse the transformations of public administration in Ukraine in wartime under the influence of hybrid cyber threats, taking into account international experience in adapting public authorities to new challenges. The relevance of the study is determined by the surge in cyberattacks against public authorities in Ukraine in 2022-2023, which demonstrated the vulnerability of digital infrastructure and the limitations of interagency coordination. The research methodology is based on systemic and comparative legal approaches, typology of hybrid threats and political effects, and empirical analysis of cyberattacks in 2021-2023. Data visualisation tools and scenario analysis of specific incidents were used. The comparative analysis of international cyber defence models in the USA, Israel, Poland, Ukraine was used to verify the results. As a result, three types of new hybrid threats are identified. Moreover, the authors' model of cascading instability is suggested which demonstrates how cyber threats can transform into political destabilisation. In addition, a classification of the political effects of cyberattacks is offered. International experience shows that effective cyber deterrence models are based on centralised coordination, public-private partnerships, and preventive threat management. The conclusions emphasise the

1 PhD Student, Department of Theory and History of the State and Law «KROK» University, 03113, 30-32 Tabirna Str., Kyiv, Ukraine. https://orcid.org/0009-0005-7855-5297.

2 Doctor of Public Administration, Associate Professor, Department of Public Administration and Regionalism, Educational and Scientific Institute of Public Service and Administration, Odesa Polytechnic National University, 65044, 1 Shevchenko Ave., Odesa, Ukraine. https://orcid.org/0000-0002-0721-7232.

3 PhD in Law, Post-Doctoral Researcher, Section of International Private Law, Academician F.H. Burchak Scientific-Research Institute of Private Law and Entrepreneurship of the National Academy of Legal Science of Ukraine, 03150, 11 Kazymyr Malevych Str., Kyiv, Ukraine. https://orcid.org/0000-0002-6370-8028.

4 PhD in Sociology, Associate Professor, Department of Psychology, Pedagogy and Social Sciences, State Tax University, 08200, 31 Universitetska Str., Irpin, Ukraine. https://orcid.org/0000-0002-3624-2525.

NAM, Anno 6 – Special Dossier
DOI: 10.36158/97912566922177
Ottobre 2025

need to rethink Ukraine's cyber strategy from a technocratic document to an integrated component of public policy aimed at strengthening digital sovereignty, institutional resilience, and post-war recovery.

Keywords: public administration; war; cybersecurity, hybrid threats; cascading instability; sovereignty.

1. Introduction

Hybrid warfare is a serious challenge for public administration in the 21st century. It transforms perceptions of security, sovereignty, and administrative efficiency, going far beyond traditional military operations. Cyberspace, information influence, economic blackmail, and stability undermining affect the political stability and social security of states (Zvezdova & Vakalyuk, 2022). In this context, the state ceases to be an exclusively political and administrative structure and becomes a system that functions in interaction with global digital flows, geopolitical risks, and unstable network threats (Yagunov et al., 2023).

The experience of recent decades shows that the effectiveness of public administration in conditions of hybrid aggression is determined by the ability to integrate institutional response mechanisms with technological solutions in cyber defence and information security. Interagency coordination, strategic communication, and the participation of the private sector and civil society are particularly important. As a state experiencing protracted hybrid aggression, Ukraine is a unique case for researching public administration effectiveness in a new type of war (Okunovska & Prymush, 2024). Since 24 February 2022, the high rate of attacks on the digital infrastructure of state authorities, the paralysis of critical services, the spread of disinformation campaigns, and the destruction of institutional coordination have highlighted the need for a radical update of approaches to public administration.

However, the domestic regulatory model of cyber defence proved to be unprepared to counter multi-level threats. The lack of interagency coordination, the low level of readiness of regional infrastructure, and the limitations of the regulatory framework, and the insufficient transparency of response processes created conditions for the consistent destabilisation of public administration. Meanwhile, the experience of the USA, Israel, and Poland demonstrates the effectiveness

of integrated cyber deterrence strategies that combine institutional centralisation, preventive thinking, and active participation of the private and civil sectors. This creates conditions for cascading destabilisation of management processes through targeted cyber pressure. At the same time, global institutions such as NATO and the European Union emphasise the need to develop resilience-based governance models that simultaneously take into account military, cyber and information threats (Cherep et al., 2025).

Despite the growing number of studies of hybrid warfare and cybersecurity, most of them address these issues from the perspective of military science, informatics, or law enforcement (Bondarenko et al., 2025). However, there are gaps in research on the relationship between hybrid cyber threats and the effectiveness of public administration, institutional coordination in crisis situations, and models of public authority adaptation to new types of threats. The aim of the study is to analyse the transformations of public administration in Ukraine in wartime under the influence of hybrid cyber threats, taking into account international experience in adapting public authorities to new challenges. In this regard, the research questions of what are the typologies of the latest threats in the system of public administration, how would the effectiveness of response change if Ukraine had a specialised cyber incident crisis management centre, and how the basic functions of the state are transformed in conditions of permanent digital pressure are raised. Within this aim and research questions, the following objectives are set:

- to develop a typology of hybrid threats that arise in cyberspace during wartime;
- to suggest a hypothetical model of interaction between cyber threats and political governance;
- to compare cyber deterrence models in the United States, Israel, Poland, and Ukraine;
- to assess the effectiveness of Ukraine's cybersecurity strategy in the context of restoring governance capacity in wartime.

The novelty of the study lies in the fact that a comprehensive analysis of the impact of hybrid cyber threats on public administration in Ukraine in wartime is carried out on the basis of empirical data. Moreover, a classification of threat types and political effects is developed. A hypothetical model of cascading destabilisation of management processes through cyber influence is proposed, and structural limitations of the Ukrainian cyber defence system are identified in comparison with advanced international models.

2. Methodological framework

The methodology is based on the interdisciplinary approaches that allow for a comprehensive understanding of the transformations of the public administration system during hybrid warfare. Given the interaction of cyberspace, institutional coordination, and political processes, several research methods were applied. In particular, a systematic method enabled the analysis of public administration as a complex socio-political system functioning in conditions of multidimensional external threats, including cyberattacks. It made it possible to identify key structural nodes (institutional, informational, and procedural).

The comparative legal analysis involved the study of cyber strategies and regulatory models in the United States, Israel, Poland, and Ukraine. The criteria for comparison were the degree of centralisation, the availability of crisis protocols, the interaction with the private sector, and the speed of response. The typological method was used to classify hybrid cyber threats and political effects. This method helped to construct a logical matrix of the impact of cyber incidents on management processes. The empirical analysis is based on open sources (CERT-UA reports, State Service of Special Communications and Information Protection of Ukraine (SSSCIP) reports, analytical publications, government communications).

Quantitative data on cyberattacks in 2021-2023 was collected, presented in the form of time series, a heat map of the most vulnerable points, and systematised in an incident table. An analytical database was created with over 50 cases of attacks on state structures, coded by type of threat, target, duration, institutional response, and political consequences. Verification of the authors' model of cascading instability was carried out by comparing the typology of attacks with the responses of state bodies. A scenario analysis of three incidents (the attack on Diia, the attack on the Ministry of Defence, and the hacking of interagency channels) was conducted, which demonstrated how the absence of a single coordination centre intensifies political and administrative fragmentation.

A modelling method was used to model a hypothetical situation: how would the effectiveness of response change if Ukraine had a specialised cyber incident crisis management centre? The model was developed by analogy with the structures of CISA (USA) and INCD (Israel), considering Ukrainian realities. Cross-verification of data was carried out by comparing official reports with me-

dia reports, independent analytical platforms, and public statements by government representatives. Individual elements were verified through expert assessments in open sources. The study of specific cases of cyberattacks on Ukrainian government structures (2022-2023), such as attacks on the Diia portal, the Ministry of Defence of Ukraine, and the Security Service of Ukraine (SSU), was used to illustrate the identified typologies and verify the suggested model. The study also uses examples of rapid response in other countries (INCD, CISA, Cyber Command) as a reference for assessing the effectiveness of the Ukrainian case.

Thus, the combination of these methods allowed for a comprehensive study of the impact of hybrid cyber threats on Ukraine's public administration system in wartime. The methods used facilitated analytical depth, and the constructed model of cascading instability visualised the complex interrelationships between digital attacks and political processes. Such methodological tools open up opportunities for further research in the field of adaptive public administration under conditions of hybrid threats.

3. Results and Discussion

3.1. Empirical observations: time series of attacks and heatmap of vulnerable points

According to official data, 1,237 incidents related to cyberattacks on Ukrainian government structures were recorded in 2021. With the start of the full-scale Russian invasion in 2022, the number of attacks doubled to 2,474. In 2023, 3,198 incidents were recorded, which is 29,3% more than in 2022. These data indicate a consistent escalation of cyber war against Ukraine, accompanying military actions on the frontline. The highest peaks of malicious activity were recorded in February 2022 (invasion), October 2022 (missile strikes on critical infrastructure), and January and June 2023 (Ukrainian army taking the initiative on the frontline) (State Service of Special Communications and Information Protection of Ukraine, 2024a).

The analysis of quarterly and annual reports from the SSSCIP, the CERT-UA team, and official government communications for 2022-2023 confirms a steady increase in the intensity of cyberattacks and a gradual sophistication of adversary tactics. At the end of 2023, CERT-UA reported 2,543 cyber incidents, reflecting

an increase in the number of intrusion attempts and an improvement in the ability to detect and document them (State Service of Special Communications and Information Protection of Ukraine, 2024b). Moreover, in Q4 2023, state monitoring tools processed about 1,4 billion events, indicating noise from attacks and attempts to probe security perimeters (State Cyber Protection Centre State Special Communications, 2024).

Furthermore, the timeline of attacks shows the synchronisation of cyberattacks with key political or military events. For instance, in January-March 2022, there was a wave of attacks on government resources (defacements, DDoS), which accompanied the start of a full-scale invasion and was aimed at undermining the availability of government websites and services (Polityuk, 2022; Ministry of National Defence of the Republic of Poland, 2022). In October-November 2022, there was a combination of cyberattacks on energy facilities and missile strikes (attempts to influence ICS/SCADA and energy networks) (Greenberg, 2023). Moreover, throughout 2023, phishing and espionage campaigns against the public sector (UAC group cluster, spear-phishing) were frequent, accompanied by periodic waves of DDoS attacks against e-government services (Cert-EU, 2023; Cyber Incident Response Operations Centre, 2024). This tendency indicates a high level of coordination of cyberattacks with other forms of hybrid influence, such as disinformation campaigns, in order to influence public sentiment and management processes. They are part of the enemy's strategic plan to destabilise Ukraine in the areas of governance, information space, and the economy.

The types of attacks varied. Thus, approximately 47% were DDoS attacks aimed at disabling government portals; 32% were attempts at phishing or compromising the accounts of officials; 11% were malware attacks (programmes such as WhisperGate and HermeticWiper); and 10% were attacks on cloud environments or attempts to interfere with internal IT infrastructures. In terms of their structure, in 2022-2023, these incidents were concentrated in the sectors of public administration, security, defence, telecommunications, and energy. Numerous malicious activities were also recorded against financial, logistics, and media resources as part of broader information operations (National Cybersecurity Coordination Centre, 2024). Some waves targeted judicial and notary authorities, with the aim of complicating transactions and legal procedures during wartime (National Cybersecurity Coordination Centre, 2023). However, it is concerning that some of the cyberattacks went undetected for a long time. According to open data, at least

8% of attacks detected in 2023 lasted more than 48 hours before being detected, indicating limitations in the early detection and response capabilities operations (National Cybersecurity Coordination Centre, 2024). In this regard, the spatial heat map of vulnerable points has a two-tiered structure (Table 1).

Table 1. Spatial heat map of vulnerable points

Target of attack	Type of services/ infrastructure	Number of incidents (2023)	Attack aim
Ministry of Digital Transformation of Ukraine and digital service platforms	E-government, digital identification, public services	**580+**	Massive DDoS attacks, defacements, attempts to compromise user accounts
State Tax Service of Ukraine and financial data exchange platforms	Financial and administrative services, tax registers	**470**	Phishing, espionage campaigns, interference with transaction data
Ministry of Defence of Ukraine and military command systems	C2 systems, military communications, secure networks	**410+**	Attempts to infiltrate military networks, targeted phishing attacks
Central Election Commission of Ukraine and local government bodies	Electoral registers, municipal services, local domains	**~300**	Website defacement, attempts to compromise local accounts
Prozorro, eHealth and other digital platforms	Public procurement, healthcare, critical databases	**250+**	Attacks on supply chains, access to personal and commercial data

Source: Cert-EU (2023).

The first tier consists of central government bodies and national registries in Kyiv. In this case, cyberattacks target nodes with a high concentration of critical services and interdepartmental integrations. The second tier is regional and local authorities and critical infrastructure nodes (telecommunications and energy), including on the frontline and border areas. As a result, vulnerabilities are aggravated by physical threats, staff turnover, and uneven defence capabilities. The early period of the war saw massive compromises of local and regional government websites, which evolved into more targeted espionage campaigns against key institutions (Canadian Centre for Cyber Security, 2022).

3.2. Typology of hybrid threats in public administration

In contemporary wartime, Ukraine confronts not only direct military threats but also a complex set of hybrid challenges targeting its political and administrative capacity. Hybrid warfare combines military, economic, informational, social and technological factors (Voloshchuk et al., 2025). Since cyberattacks take place in digital space, identifying the aggressor is complicated, which in turn limits the applicability of traditional international legal response mechanisms. Therefore, it is necessary to rethink the conceptual foundations of public administration.

The asymmetry is an important element of hybrid threats, meaning that relatively insignificant resources directed at disinformation campaigns or cyberattacks can cause damage comparable to the consequences of large-scale military operations (Legenkyi et al., 2025). Meanwhile, states have become dependent on digital infrastructure and e-governance as resource management systems, coordination of military and civilian structures, and effective communication with the population are based on digital technologies, making them a priority target for the enemy. Apart from that, a distinctive feature of hybrid threats is their systemic nature. In most cases, they do not function in isolation but form a complex political shock effect (Stokel-Walker, 2022). This means that simultaneous pressure on infrastructure, the information space, and administrative institutions creates a synergistic effect. As a result, even a technically prepared and formally protected state may be unable to restore stability quickly.

The cumulative effect is another characteristic feature of hybrid threats. Thus, cyberattacks are combined with information manipulation, economic sabotage, and the provocation of social tension (Yakymchuk, 2019). This creates a crisis of confidence because society begins to doubt the ability of state institutions to ensure a basic level of security and stability. Moreover, the cross-border nature of hybrid warfare is an additional complicating factor as cyberattacks are often coordinated from outside the state, using the infrastructure of third countries or global digital platforms (Simons et al., 2020). As a result, hybrid threats go beyond the scope of national security alone and require international cooperation and the adaptation of state institutions to new realities.

Hence, the analysis of contemporary hybrid threats shows that their impact on public administration in wartime is observed in three key areas: technological vulnerability of digital infrastructure, manipulative pressure on public consciousness, and organisational destabilisation of public authorities. On the basis of these

characteristics, a new typology of hybrid threats in the digital age is developed. They are divided into three interrelated types: infrastructure threats, information and psychological influences, institutional and network attacks, and systemic effects (Table 2).

Table 2. Typology of hybrid threats in public administration in wartime

Type of hybrid threat	Content and target	Key tools and methods	Effects on public administration	Examples
Infrastructure threats	Disruption of Ukraine's digital and administrative infrastructure, blocking of basic services	Cyberattacks on critical government services, DDoS attacks, malicious software injections, unauthorised access attempts, data substitution	Paralysis of access to e-services, decline in trust in the digital state, additional burden on administrators during wartime	In 2023, more than 3,198 attacks on the digital infrastructure of state bodies were recorded (29% more than in 2022).
Information and psychological influences	Undermining the legitimacy of the authorities, creating an atmosphere of chaos and panic	Disinformation and propaganda campaigns, deepfake imitations of speeches, targeted attacks on social networks	Decline in public trust, destabilisation of the political environment, creation of an image of incompetent administration	Fake messages on behalf of the Ministry of Defence of Ukraine in 2022-2023; cyberattacks on media resources
Institutional and network attacks	Violation of interdepartmental coordination and decision-making process	Disabling government communication channels, infecting internal systems, imitating official communications	Delays in response, reduced effectiveness of strategy implementation, undermining of trust between institutions	Attacks on the internal systems of the Cabinet of Ministers of Ukraine, the SSU, and SSSCIP in early 2023
Systemic effects	Combination of several types of threats that reinforce each other	A combination of infrastructure attacks, information manipulation, and network destabilisation	Political shock, paralysis of governance, and intensification of internal crises	Estonia (2007, cyberattacks), the United States (2016, election interference), Israel (2021, attacks on government services)

Source: compiled by the authors

This typology demonstrates that the key vulnerability occurs at the intersection of three interrelated dimensions: technical, informational, and institutional. In other words, infrastructure attacks undermine the technical basis of public administration, limiting the state's ability to provide administrative and social services. Information and psychological influences target public consciousness and political trust, creating conditions for the delegitimisation of authority. Institutional and network attacks destroy the mechanisms of interagency coordination.

3.3. Evaluating cyber defence models from the USA, Israel, Poland, and Ukraine

To identify potential directions for reforming Ukraine's cyber strategy, it is useful to compare the Ukrainian model with the approaches of the USA, Israel, and Poland. Their experience shows that it is possible to build an effective regulatory and institutional framework that integrates operational response, strategic planning, and the participation of diverse security actors. Table 3 summarises these countries' legislative measures, organisational models, and levels of effectiveness, while highlighting the implications of the identified differences for Ukraine.

Table 3. Key approaches to cyber defence in the USA, Israel, Poland, and Ukraine

Country	Legislation	Cyber defence model	Effectiveness	Meaning for Ukraine
The USA	National Cybersecurity Strategy (The White House, 2023); Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Cybersecurity and Infrastructure Security Agency, 2022)	Network federalism, active opposition, private partners	High dynamism, fast response	It demonstrates the importance of engaging the private sector and municipalities and developing shared responsibility for cybersecurity. Ukraine should integrate business and the civilian sector into its defence system.
Israel	Israel National Cyber Directorate (INCD)	Proactive disruption strategy	Successful warning logic	It provides an example of the creation of a coordination centre and the transition from reactive actions to preventive threat modelling. For Ukraine, this means centralising responsibility and implementing crisis scenarios in advance.
Poland	Cybersecurity strategy of the Republic of Poland for 2019-2024 (Ministry of Digital Affairs, 2019),	Cyber Command establishment	Effective civil-military cooperation	It demonstrates the value of integrating cyber strategies into military doctrine and engaging civilian structures simultaneously. It is important for Ukraine to develop a mechanism for multilevel cooperation, especially with NATO and EU partners.
Ukraine	Cybersecurity Strategy of Ukraine (President of Ukraine, 2021), plans of the Cabinet of Ministers, orders of the SSU	Reactive model, fragmented coordination	Lack of a unified system model	Differences with the leading models indicate the need to create a unified coordination centre, specify responsibilities in legislation, integrate business and civil society, and strengthen preventive mechanisms.

Source: compiled by the authors

The United States is a leader in shaping global cybersecurity policy, offering a model based on the principles of public-private partnerships, multi-level governance, and strategic foresight. The US legislative framework is constantly updated. In 2022-2024, more than 10 new regulations on cyber incidents, supply chain security, and cyber education were adopted (Lee & Chua, 2023). The key regulatory document is the National Cybersecurity Strategy (The White House, 2023), which envisages a shift from reactive to proactive threat deterrence. It also establishes the responsibility of the private sector for the protection of critical infrastructure. The strategy is based on the concept of shared responsibility of the state, business, and citizens for digital security (Weaver, 2022). The US Congress also passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Cybersecurity and Infrastructure Security Agency, 2022), which requires infrastructure operators to report incidents within 72 hours.

The Cybersecurity and Infrastructure Security Agency (CISA) is the central coordinator, which operates within the Department of Homeland Security. The CISA performs the functions of rapid response, standardisation, risk analysis, training, and technical assistance. Its strategy is based on proactive actions, active use of AI to monitor threats, and close coordination with the IT sector. Moreover, the National Security Council and the Department of Defence, and the US Cyber Command coordinate actions in case of state-level cyberattacks. Grant support programmes for cyber resilience for municipalities, states and educational institutions were introduced. A distinctive feature of the US model is the focus on cyber research by the National Institute of Standards and Technology and leading universities (Weaver, 2022).

The Israeli model is an example of a centralised integrated approach to cybersecurity in the face of the constant threat of terrorist attacks. Back in 2011, the Israel National Cyber Bureau was established, and later its functions were transferred to the Israel National Cyber Directorate (INCD), which is directly subordinated to the Prime Minister of Israel. The INCD combines operational functions with political and strategic planning, control of cyber infrastructure, development of standards, and coordination with the army, intelligence, and the private sector. A specific feature of the

Israeli system is the model of responsibility at the point of threat. It means that organisations that own digital assets are responsible for their protection but are obliged to act in accordance with the INCD standards (Hassib & Shires, 2024).

Israel carries out centralised detection and prevention of attacks, using traditional analytical tools and AI. However, prevention is a key element; the focus is not only on incidents but on potential attack scenarios modelled in real time. Moreover, legislation provides a framework for cooperation between the state and IT companies in terms of information exchange, confidentiality, and personal data protection. In addition, military education in cybersecurity (e.g., the Unit 8200) provides highly qualified personnel for further use in the civilian sector (Tabansky, 2020).

Poland strengthened its cyber infrastructure significantly in recent years. In 2019, the Cybersecurity Strategy of the Republic of Poland for 2019-2024 was approved (Ministry of Digital Affairs, 2019), prioritising cyber defence, the development of a national early warning system, and closer cooperation with allies. In this regard, the Cyberspace Defence Forces were established within the Armed Forces of Poland. They are responsible for responding to cyber incidents promptly, ensuring information resilience, and protecting military infrastructure (Kitler, 2021). Moreover, the Government Centre for Security functions as a civilian coordinator responsible for early detection and warning. Furthermore, the annual cyber deterrence exercises involving NATO, business, and academic institutions are conducted. In addition, Poland implemented the EU NIS2 Directive (European Parliament and of the Council, 2022) and adopted a number of acts on critical infrastructure, e-government cyber defence, cyber hygiene, and cyber education. These initiatives are implemented in parallel with the increased involvement of the private sector in creating solutions by the Polish Institute for Cybersecurity and support for innovative start-ups (Sulowski, 2023).

As compared with these models, Ukraine looks vulnerable. Despite being in a state of full-scale war, it still does not have a unified coordination body in cybersecurity. Moreover, its legislative framework remains fragmented, while strategic documents are mostly declarative. Although the

Cybersecurity Strategy of Ukraine was approved in 2021 (President of Ukraine, 2021), it is limited by the lack of a coordination centre, imperfect mechanisms of interaction between authorities, and weak institutional structure. The regulatory framework lacks a separate law on cyber defence and legal mechanisms for involving civil initiatives in the cyber defence system. The existence of incident response centres (CERT-UA) does not compensate for the actual distrust between agencies and excessive centralisation with a lack of resource autonomy (Shypilova, 2019). Therefore, in 2022-2023, cases of duplication of functions, delays in decision-making, and lack of transparent communication were recorded (Kravchuk et al., 2024).

The large-scale cyberattacks of 2022-2023 exposed serious structural deficiencies in the response and coordination system between key institutions, i.e., the SSU, the SSSCIP, and the Cabinet of Ministers of Ukraine. The Ukrainian cyber defence model is designed to disperse responsibility between different structures, which reduces the effectiveness of decision-making and slows down the response time to threats (Abibok, 2022). Despite the integrated model of risk management and coordination declared in the 2021 Strategy, the interaction remained fragmented. This is confirmed by independent analytical reports and specific crisis incidents. Thus, in January 2022, a cyberattack took down more than 70 government websites, such as the Cabinet of Ministers of Ukraine website and the Diia portal. In 2022, CERT-UA also recorded more than 2,000 incidents. However, a significant number of them were handled only after the fact, without signs of preventive deterrence (State Service of Special Communications and Information Protection of Ukraine, 2024b). This indicates the absence of an effective crisis protocol and a single cyber incident management centre in the context of hybrid warfare (CERT-UA, 2022; Scroxton, 2023).

Nevertheless, the Ukrainian experience has unique features. Ukraine is the first country to implement large-scale digitalisation of public services during active warfare (Holovkin et al., 2023). Second, Ukrainian society demonstrates a high level of digital competence, readiness for self-defence, and mobilisation of volunteer cyber initiatives (Nizovtsev et al., 2022). These factors should be integrated into a formalised cyber

deterrence system. However, without a clear regulatory framework and organisation, Ukraine risks remaining vulnerable to multi-pronged hybrid threats. Durin the post-war recovery, such threats could have critical consequences for the sustainability of public administration.

The comparison reveals distinct approaches to cybersecurity management. Thus, the USA emphasises a decentralised system with strong private sector involvement; Israel prioritises centralised preventive threat management; Ukraine remains fragmented and reactive; while Poland achieves a balance between military and civilian structures, enabling multi-level coordination. For Ukraine, the Polish experience is especially relevant for improving cooperation between the Ministry of Defence, the SSU, the SSSCIP, and civilian institutions. At the same time, Ukraine must move beyond excessive state-centricity by creating conditions for IT business participation and empowering local governments.

International experience offers several adaptable solutions. The US model suggests establishing a single coordinating body with real-time analytical and response capacities. The Israeli model underscores the value of formalised partnerships with IT volunteers and civil cyber initiatives. The Polish model demonstrates the effectiveness of regional CERT centres, which could be replicated through a network of regional cyber resilience centres within Ukraine's administrations. Overall, Ukraine needs to synthesise these three elements: public-private integration from the USA, centralised prevention from Israel, and military-civilian cooperation from Poland. Such a model would provide a comprehensive framework for cyber deterrence, tailored to the conditions of martial law and the demands of post-war recovery.

Empirical data confirms the need for a profound transformation of the public administration system, considering constant cyber threats as a factor of political influence. Therefore, digital infrastructure should be viewed as a strategic resource of public authority, the vulnerability of which directly affects the legitimacy and effectiveness of the state in conditions of war and post-war recovery. The study results confirm the need to rethink Ukraine's cyber strategy as an integrated component of public policy. In the context of hybrid warfare, cyberspace ceases to be merely a vulnerable

environment and becomes an impetus for political transformation, requiring appropriate institutional, legal and strategic changes. Ukraine has the potential to implement the best practices of Israel and Poland, but to do so, it must overcome fragmentation in governance and formalism in responding to threats.

Having analysed cases from Ukraine, Poland, Israel, and the United States, it is possible to classify the political effects of cyberattacks on public administration. Destabilisation effects include short-term disruptions in the work of government bodies, which undermine the state's ability to respond quickly to crises. Fragmentation effects refer to consequences that erode administrative unity and weaken the synchronisation of actions by key public authorities. A striking example is the large-scale attack on financial infrastructure in February 2023, i.e., despite the clearly coordinated nature of the attack, interagency coordination began only 48 hours later. Transformation effects are manifested in long-term changes in institutional practices, the regulatory framework and strategic approaches in the field of public administration. Such consequences can be positive (strengthening cyber infrastructure, creating new institutions) and negative (excessive centralisation, restricting citizens' rights under the pretext of strengthening security). Delegitimisation effects are linked to the undermining of trust in government structures and digital interaction tools. A telling example was the mass complaints about the performance of the Diia portal after the cyberattack in November 2022. Inertia effects are manifested in delayed decision-making or in the reproduction of outdated and ineffective cyber defence models.

3.4. A hypothetical model of interaction between cyberspace and political processes

Empirical observations help to identify four key trends that are important for modelling. First, there is an escalation in the number of incidents and an increase in the density of events in state SOCs. This reflects an increase in the intensity of threats and improvements in the ability to detect them (State Service of Special Communications and Information Protection of Ukraine, 2024b; State Cyber Protection Centre State Special Communi-

cations, 2024). Secondly, there is a noticeable event- and season-related wave-like pattern to the attacks. Their peaks coincide with significant military and political events (in particular, energy strikes), which indicates a convergence of cyber activity with kinetic operations (Greenberg, 2023). Thirdly, the dominant tactics are changing: instead of high-profile destructive actions, the emphasis is shifting to persistent reconnaissance, phishing, and compromise of communication chains, while DDoS attacks have become merely a tool of information pressure (Cert-EU, 2023; Cyber Incident Response Operations Centre, 2024). Fourthly, a two-domain vulnerability space is forming. It means that attacks are directed at central registries and portals, and at regional or local nodes that ensure the continuity of administrative and life-support services (Canadian Centre for Cyber Security, 2022).

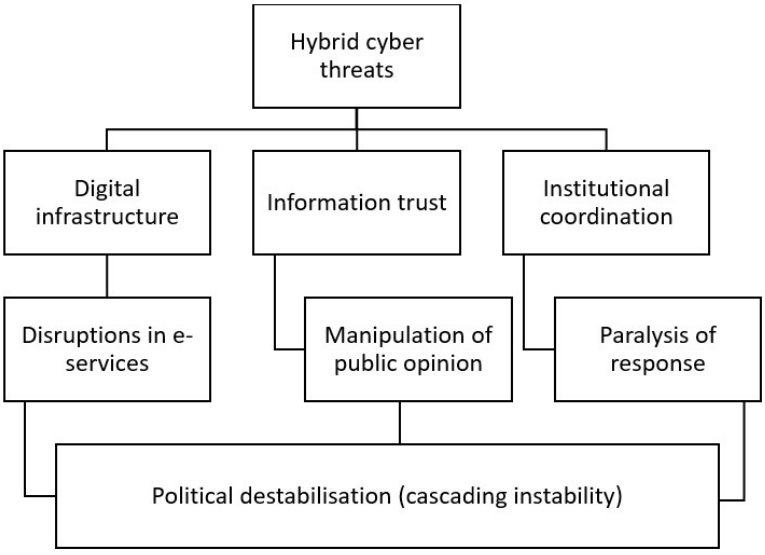
For visualization purposes, it is advisable to build time series based on monthly or weekly intervals of CERT-UA/SSSCIP incident publications, while overlaying event markers such as missile strikes, announcements of mobilization or reform decisions, and visible service failures. The cartographic heat map should reflect the concentration of incidents or attempted attacks in the following areas: central government domains and registries, regional state administrations and city councils, and energy and telecommunications facilities, highlighting corridors of increased risk in the East and South of Ukraine. The combination of temporal and spatial data confirms the provisions of the hypothetical model of cyber convergence of management vulnerabilities. In other words, the synchronisation of attacks in the technical, informational, and institutional dimensions increases the likelihood of cascading instability in public administration (Cert-EU, 2023).

The CERT-UA/SSSCIP open data is partially aggregated and does not always contain complete geographical attribution of incidents. Therefore, the spatial analysis reflects a conservative assessment of risk concentration and requires validation on extended telemetry samples, such as SOC data or ICS event logs, in further research. Moreover, not all recorded attacks were publicly confirmed by state authorities, which is partly explained by political expediency. The geospatial distribution of attacks poses another

threat. According to the heat map, regional digital services in the Kharkiv, Dnipropetrovsk, Odesa, Zaporizhzhia, and Mykolaiv regions are also vulnerable. This is explained by the technical limitations of local infrastructure and the growing role of regional military administrations in implementing state policy in wartime.

In hybrid warfare, cyberspace appears as a technical tool for ensuring the functioning of state services and a multidimensional environment that influences political processes (Kortukova et al., 2023). In other words, political processes are integrated into cyberspace and depend on its stability. For example, technical failures turn into administrative delays, distorted information reduces trust in official communications, and coordination failures between agencies complicate the development of consolidated decisions (Rabinovych et al., 2025). This gives rise to the phenomenon of cascading instability, when the simultaneous action of several types of threats creates the effect of political shock. As a result, public administration faces a double challenge, i.e., the need to restore digital services and restore public confidence in the effectiveness of the authorities. The suggested hypothetical cyber convergence of management vulnerabilities model illustrates this interconnection (Figure 1).

Figure 1. Cyber convergence of management vulnerabilities model



Cyberattacks on digital infrastructure lead to disruptions in the provision of public services, which creates fertile ground for manipulating public opinion. In turn, the loss of trust in information causes imbalances in interagency coordination and paralysis in responding to crisis situations. The combination of these factors creates political destabilisation, which can affect the internal legitimacy of the government and the international image of the state. This model demonstrates how attacks in cyberspace affect the functioning of the state apparatus, public trust and the decision-making process simultaneously, creating cascading instability.

Thus, the interaction between cyberspace and political processes during wartime should be viewed as a single dynamic system. Its key characteristic is the interdependence of technical and political vulnerabilities, which reinforce each other. Understanding this interaction facilitates creating new approaches to public administration, where cyber defence is seen as a political function that determines the stability and resilience of the state in hybrid warfare.

3.5. Management reforms in wartime: key areas

The Russian full-scale aggression against Ukraine has highlighted the need for situational measures to respond to hybrid threats and systemic reforms of public administration. The pre-reform public administration was designed for peacetime and thus faced the challenge of adapting to anti-crisis regimes. This was facilitated by the introduction of martial law, the expansion of the powers of the President of Ukraine, the National Security and Defence Council of Ukraine, and military administrations, which were given special functions and status (Nehara et al., 2025). In legal terms, this was accompanied by the introduction of military procedures, such as accelerated procurement, simplified budgeting, and temporary restrictions, which are assessed in terms of necessity and proportionality.

At the same time, even during the war, reforms continued, particularly decentralisation. Despite martial law, support for local self-government reform grew. Thus, 63% of respondents approved of it in 2021, compared to 77% during martial law (Centre of Expertise for Multilevel Governance, 2022). Decentralisation ensured local capacity and adaptability (Oliychenko et al., 2024). Moreover, digital transformation became a key component of crisis management through the introduction of electronic government services, digital registries and platforms

proved key to maintaining the continuity of public services, logistics chains and communications (Gustafsson et al., 2025). In the defence procurement sector, a new state logistics operator (DOT) emerged with a transparent DOT-Chain platform, which reduced costs by 25% and ensured that 95% of contracts for requested goods are fulfilled in accordance with NATO standards (Kullab, 2024).

Furthermore, anti-corruption reform remained a priority (Hudz, 2024). The Verkhovna Rada of Ukraine abandoned attempts to subordinate the main anti-corruption bodies (NABU, SAP) to the Prosecutor General thanks to active civic response (Halushka, 2025). In the judiciary, Ukraine continued to implement reforms, including the creation of high specialised courts to resolve political disputes in order to fulfil the IMF's conditions for continuing financing in the amount of $15,6 billion (Peleschuk & Lewis, 2025). Overall, the judicial reform included the creation of the High Council of Justice, the High Qualification Commission of Judges, the Public Integrity Council, and the Anti-Corruption Court.

Civil society continues to support reform implementation strategies even during wartime. As Chatham House notes, war can be a period for establishing institutions that will gain the trust of donors and society (Lutsevych, 2024). Transparency International Ukraine (2024) highlights key areas such as an anti-corruption environment, effective reconstruction, reform of the Accounting Chamber and the State Audit Service, which are critical for the military and post-war stability. European analysts emphasise that the war destroyed previous reform blocks. As a result, Ukraine must take advantage of this opportunity by preserving pluralism, by not concentrating excessive power in the hands of the Presidential Administration or security forces, and continuing judicial reform and the fight against oligarchs (Wilson, 2023).

Moreover, institutional reform took place in the area of cybersecurity coordination: the powers of the SSSCIP was expanded and new mechanisms for interaction between the Ministry of Digital Transformation of Ukraine, the SSU and sectoral management bodies were created (Ponomarov et al., 2023). This helped to shift from a fragmented response to more centralised risk management models and had a positive impact on the speed of response during large-scale attacks. However, excessive centralisation continues to pose risks of reduced flexibility and delays in decision-making at the regional level. Furthermore, the war stimulated the integration of the private sector and the IT community into the state

cyber defence system. While such cooperation was mostly informal until 2022, it gradually became institutionalised during martial law. For instance, platforms for sharing information about incidents were created, and stable networks of interaction between state bodies and technology companies were formed.

In addition, there is ongoing digitalisation of management under martial law. Owing to the Diia portal and other digital services, government services remained accessible during massive attacks. This proves a transition from paper bureaucracy to a digital administrative model being more resilient in during the crisis. A reform of strategic planning in security was also initiated, which considers cyber threats a key element of national security alongside military and economic components. Finally, the war provoked decentralisation in cyber defence, as there was a need to transfer some powers and resources to the regions. The establishment of local incident response teams and the development of regional resilience centres created the conditions for a more flexible management model in the future.

Despite the progress made, there are still structural problems that need to be addressed. Particular attention should be paid to the fragmentation of the regulatory framework, a significant part of which is of Soviet origin and does not correspond to new hybrid threats. Although the Cybersecurity Strategy of Ukraine (President of Ukraine, 2021) was adopted, Ukraine's regulatory framework remains fragmented and only partially harmonised with European standards (NIS2, GDPR). The absence of a specialised law on cyber defence and clear procedures for interaction between authorities limits the effectiveness of strategic planning and reduces the state's ability to counter multi-level hybrid threats. The shortage of highly qualified personnel in cybersecurity in the public sector remains the key challenge. During the war, this problem is partially resolved by the mobilisation of IT volunteers and the development of public cyber initiatives. Excessive centralisation of cyber defence management limits the ability of regions to respond to attacks quickly, while the low level of digital literacy among officials creates a favourable environment for successful attacks using social engineering.

The SSSCIP, CERT-UA, the Ministry of Digital Transformation of Ukraine, and sectoral CERT structures demonstrated their ability to shift from preventive to crisis management of cyber incidents. Despite massive attacks (up to 15-20 major incidents per day during peak periods), it was possible to avoid a systemic collapse of the digital infrastructure. This demonstrates a high level of operation-

al coordination. Despite the intensity of the attacks, key digital services (Diia, Prozorro, tax services) continued to function. The use of cloud technologies, server geospatial distribution, and international support (Microsoft, Amazon Web Services, Google) helped to maintain the availability of administrative services even during massive missile and cyberattacks. This increased citizens' trust in the state in conditions of uncertainty.

In the post-war period, when the reconstruction of the state will be accompanied by increased geopolitical risks and internal political transformations, the role of cyberspace will grow. Therefore, it is important to shape digital sovereignty, considering the best practices of allies and the specifics of the Ukrainian context. In this regard, it is worth offering a number of recommendations that could increase the effectiveness of the cybersecurity strategy and restore administrative capacity. Thus, it is necessary to update the regulatory framework, bringing it into line with NATO and EU standards and removing archaic provisions.

Furthermore, it is essential to invest in human resource development by creating specialised educational programmes for the public sector and raise cyber awareness of civil servants. It is also advisable to expand decentralisation in cyber defence by creating regional cyber resilience centres with resource and organisational autonomy. In addition, integration with international response systems should be intensified by expanding participation in joint exercises. Finally, a key focus should be on engaging the private sector and institutionalising cooperation with the IT community, which will increase the flexibility and technological effectiveness of the national cyber defence system. In summary, the results of the study indicate the need to transform Ukraine's cyber strategy from a predominantly technocratic tool into a full-fledged component of national security policy and modernisation of management practices. In summary, the study results indicate the need to transform Ukraine's cyber strategy from a predominantly technocratic tool into a full-fledged component of national security.

4. Conclusions

The study identified key features of the transformation of public administration in Ukraine in hybrid warfare and under massive cyber threats. The analysis showed that contemporary challenges in the digital sphere went beyond technical incidents and affected institutional stability, public trust, and the state's ability

to implement management decisions. Moreover, a typology of the latest hybrid threats was suggested, covering the infrastructural, informational-psychological and institutional-network dimensions, which created a political shock effect and could paralyse the functioning of the state apparatus.

The developed model of interaction between cyberspace and political processes showed that cyberattacks had a cascading nature. In other words, local technical incidents could escalate into a crisis of confidence and cause managerial destabilisation. This was confirmed by empirical data on the temporal dynamics of attacks and the spatial concentration of hot spots in the public sector. Observations revealed patterns of peak waves of attacks associated with critical phases of war and the vulnerability of key digital platforms.

The assessment of the effectiveness of Ukraine's cybersecurity strategy demonstrated its ability to ensure the continuity of key government functions during periods of large-scale attacks. At the same time, the strategy had a number of structural problems: fragmentation of the regulatory framework, staff shortages, excessive centralisation and insufficient digital literacy among civil servants. These factors limited the potential of the cyber defence system to restore full administrative capacity.

The practical significance of the results lies in the formulation of recommendations for improving the cyber resilience of public authorities. These include modernising the legislative framework, developing professional human resources, creating regional cyber resilience centres, institutionalising cooperation with the IT community, and integrating it into international security networks. The implementation of these measures can enhance the security and ensure the stability of public administration during wartime and the post-war period.

Despite the warfare, the ongoing reforms lay the foundation for the modernisation of the public administration in the post-war period. The institutional consolidation in cybersecurity, partnerships with the private sector and the IT community, accelerated digitisation of services, development of strategic planning, and decentralisation of security functions are shaping a new management model that will be more flexible, transparent, and sustainable. These developments will make it possible to combine reconstruction tasks with the modernisation of public administration. They in turn will ensure Ukraine's integration into the European space as a state capable of countering hybrid threats effectively.

Nevertheless, the study has several limitations. Firstly, the analysis mainly covers short- and medium-term effects, while long-term consequences remain uncertain, particularly regarding the risk of institutionalising excessive centralisation after the war and a possible imbalance between the branches of government. Secondly, the lack of empirical data limits the quantitative assessment of the effectiveness of reforms, as the available observations are mainly descriptive and normative. Thirdly, the study focuses on the national level, leaving out local specifics and the impact of reforms on communities that bear a significant burden in providing basic services.

Therefore, the results should be considered an interim analysis that requires further research of positive effects and potential risks of military reforms. In this regard, further research should focus on studying the long-term political consequences of hybrid cyber threats, developing models of interagency coordination in crisis situations, and comparing the experiences of countries that have been in a state of hybrid confrontation. Finally, it is important to study the cyber strategy integration into the broader national security system as a tool for protecting digital sovereignty and strengthening state capacity in the 21st century.

References

Abibok, Yu. (2022). Cyberattacks undermine Ukraine's security. *Institute for War & Peace Reporting*. Retrieved from https://iwpr.net/global-voices/cyberattacks-undermine-ukraines-security

Bondarenko, S., Niziaieva, V., Kravchenko, M., Kaliuha, Ye., Kolisnichenko, R., & Tsumariev, M. (2025). Modernization of Administrative Control over the Legality of Decisions of Local Self-Government Bodies of Ukraine. *Evropský Politický a Právní Diskurz, 12*(1), 31-44. https://doi.org/10.46340/eppd.2025.12.1.4

Canadian Centre for Cyber Security. (2022). Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine. Retrieved from https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf?utm_source

Centre of Expertise for Multilevel Governance. (2022). Ukraine: in wartime support to decentralisation reform increased. Retrieved from https://www.coe.int/en/web/centre-of-expertise-for-multilevel-governance/-/ukraine-in-wartime-support-to-decentralisation-reform-increased?utm_source

Cert-EU. (2023). Russia's war on Ukraine: one year of cyber operations 24 February 2022 – 24 February 2023. Retrieved from https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf?utm_source

CERT-UA. (2022). First annual report on the results of the vulnerability detection system and response to cyber incidents and cyberattacks. Retrieved from https://cert.gov.ua/article/17696

Cherep, O., Kaliuzhna, Y., Mykhailichenko, L., Markova, S., & Naumenko, Y. (2025). Formation of a strategy for countering and identifying AI technologies in the fight against disinformation under martial law. *Technology Audit and Production Reserves*, *2*(2(82), 74-79. https://doi.org/10.15587/2706-5448.2025.327157

Cyber Incident Response Operations Centre. (2024). 2024 Annual report: Vulnerability detection and cyber incident / cyberattack response system. Retrieved from https://scpc.gov.ua/api/files/4560c0ba-c6c0-4935-b48d-0232dd659df3?utm_source

Cybersecurity and Infrastructure Security Agency. (2022). Cyber Incident Reporting for Critical Infrastructure Act of 2022. Retrieved from https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

European Parliament and of the Council. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Retrieved from http://data.europa.eu/eli/dir/2022/2555/oj

Greenberg, A. (2023). Sandworm hackers caused another blackout in Ukraine - During a missile strike. *Wired.* Retrieved from https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/?utm_source

Gustafsson, M., Matveieva, O., Wihlborg, E., Borodin, Y., Mamatova, T., & Kvitka, S. (2025). Adaptive governance amidst the war: Overcoming challenges and strengthening collaborative digital service provision in Ukraine. *Government Information Quarterly, 42*(3), article number 102056. https://doi.org/10.1016/j.giq.2025.102056

Halushka, O. (2025). Ukraine's anti-corruption reforms are more vital than ever during wartime. *Atlantic Council.* Retrieved from https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-anti-corruption-reforms-are-more-vital-than-ever-during-wartime/?utm_source

Hassib, B., & Shires, J. (2024). Digital recognition: cybersecurity and internet infrastructure in UAE–Israel diplomacy. *International Affairs, 100*(6), 2399-2418. https://doi.org/10.1093/ia/iiae233

Holovkin, B., Cherniavskyi, S., & Tavolzhanskyi, O. (2023). Factors of cybercrime in Ukraine. *Relacoes Internacionais no Mundo Atual, 3*(41), 464-488.

Hudz, V. (2024). Expert conclusion as a key source of evidence in cases of corruption offenses by officials. *Legal Horizons, 22*(3), 34-45. https://doi.org/10.54477/LH.25192353.2024.3.pp.34-45

Kitler, W. (2021). The Cybersecurity Strategy of the Republic of Poland. In Chałubińska-Jentkiewicz, K., Radoniewicz, F., & Zieliński, T. (Eds.), *Cybersecurity in Poland* (pp. 137–153). Cham: Springer. https://doi.org/10.1007/978-3-030-78551-2_9

Kortukova, T., Kolosovskyi, Y., Korolchuk, O.L., Shchokin, R., & Volkov, A.S. (2023). Peculiarities of the legal regulation of temporary protection in the European Union in the context of the aggressive war of the Russian Federation against Ukraine. *International Journal for the Semiotics of Law, 36*(2), 667-678. https://doi.org/10.1007/s11196-022-09945-y

Kravchuk, M., Kravchuk, V., Hrubinko, A., Podkovenko, T., & Ukhach, V. (2024). Cyber security in Ukraine: Theoretical view and legal regulation. *Law, Policy and Security, 2*(2), 28-38. https://doi.org/10.62566/lps/2.2024.28

Kullab, S. (2024). Ukraine's reformed military procurement agency drives the country's NATO ambitions. The Associated Press. Retrieved from https://apnews.com/article/russia-ukraine-war-nato-reforms-military-procurement-f0483561c9d402697d7a67dd43ae844d

Lee, C.S., & Chua, Y.T. (2023). The role of cybersecurity knowledge and awareness in cybersecurity intention and behaviour in the United States. *Crime & Delinquency, 70*(9), 2250-2277. https://doi.org/10.1177/00111287231180093

Legenkyi, M., Piankivska, L., & Tolbatov, A. (2025). Legal basis for cybersecurity in Ukraine under martial law. *Ceur Workshop Proceedings, 3925*, 334-342.

Lutsevych, O. (2024). *Ukraine's wartime recovery and the role of civil society. Chatham House survey of Ukrainian CSOs – 2024 update.* London: Chatham House. Retrieved from https://www.chathamhouse.org/sites/default/files/2024-06/2024-06-05-ukraine-wartime-recovery-role-civil-society-lutsevych.pdf.pdf?utm_source

Ministry of Digital Affairs. (2019). Cybersecurity strategy of the Republic of Poland for 2019-2024. Retrieved from https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/PL_NCSS_2019_en.pdf

Ministry of National Defence of the Republic of Poland. (2022). Analysis of the cyberattack on Ukrainian government resources. *CSIRT of the Ministry of National Defence.* Retrieved from https://csirt-mon.wp.mil.pl/aktualnosci/analysis-of-the-cyber-attack-on-ukrainian-government-resources/?utm_source

National Cybersecurity Coordination Centre. (2023). Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber war. Retrieved from https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2023/Cyber%20digest_August_2023_EN.pdf?utm_source

National Cybersecurity Coordination Centre. (2024). Cybersecurity Threat Landscape of Ukraine in 2023. Retrieved from https://understandingcyberwar.org/wp-content/uploads/2024/09/Proekt_3_en.pdf?utm_source

Nehara, R., Kalchuk, O., Riabchenko, O., Kapitanets, S., & Marusiak, O. (2025). System of public administration entities in times of war: the Ukrainian experience. *CERIDAP, 2*, 170-190. https://doi.org/10.13130/2723-9195/2025-2-20

Nizovtsev, Y.Y., Lyseiuk, A.M., & Kelman, M. (2022). From self-affirmation to national security threat: Analyzing Ukraine's foreign experience in countering cyberattacks. *Revista Cientifica General Jose Maria Cordova, 20*(38), 355-370.

Okunovska, Yu., & Prymush, M. (2024). Local self-government in Ukraine in the context of a full-scale invasion. *Evropský Politický a Právní Diskurz, 11*(3), 43-50. https://doi.org/10.46340/eppd.2024.11.3.4

Oliychenko, I., Ditkovska, M., & Klochko, A. (2024). Digital transformation of public authorities in wartime: The case of Ukraine. *Journal of Information Policy, 14*, 686-746. https://doi.org/10.5325/jinfopoli.14.2024.0020

Peleschuk, D., & Lewis, B. (2025). Ukraine to set up high-level courts as part of reform drive. *Reuters*. Retrieved from https://www.reuters.com/world/europe/ukraine-set-up-high-level-courts-part-reform-drive-2025-02-26/?utm_source

Polityuk, P. (2022). Massive cyberattack hits Ukrainian government websites as West warns on Russia conflict. *Reuters*. Retrieved from https://www.reuters.com/technology/massive-cyberattack-hits-ukrainian-government-websites-amid-russia-tensions-2022-01-14/?utm_source

Ponomarov, O.A., Pyvovarchuk, S.A., Kozubtsova, L.M., Kozubtsov, I.M., Bondarenko, T.V., & Tereshchenko, T.P. (2023). Hybrid construction of cyber security system: Administrative and legal principles of military-civil cooperation. *Cybersecurity: Education, Science, Technique, 3*(19), 109-21. https://doi.org/10.28925/2663-4023.2023.19.109121

President of Ukraine. (2021). Decree No. 447/2021 on the decision of the National Security and Defence Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine". Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#n12

Rabinovych, M., Brik, T., Darkovich, A., Hatsko, V., & Savisko, M. (2025). Ukrainian decentralization under martial law: challenges for regional and local self-governance. *Post-Soviet Affairs*, 1-25. https://doi.org/10.1080/1060586X.2025.2520167

Scroxton, A. (2023). Ukraine cyber teams responded to more than 2,000 attacks in 2022. *Computer Weekly*. Retrieved from https://www.computerweekly.com/news/252529292/Ukraine-cyber-teams-responded-to-more-than-2000-attacks-in-2022

Shypilova, Yu. (2019). *Legal framework for Ukrainian cybersecurity: overview and analysis*. Arlington: International Foundation for Electoral Systems.

Simons, G., Danyk, Y., & Maliarchuk, T. (2020). Hybrid war and cyber-attacks: creating legal and operational dilemmas. *Global Change, Peace & Security*, *32*(3), 337-342. https://doi.org/10.1080/14781158.2020.1732899

State Cyber Protection Centre State Special Communications. (2024). Q4 2023 Report. Retrieved from https://scpc.gov.ua/en/articles/341?utm_source=

State Service of Special Communications and Information Protection of Ukraine. (2024b). The CERT-UA Team has processed 2,543 cyber incidents over 2023. Retrieved from https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti?utm_source=

State Service of Special Communications and Information Protection of Ukraine. (2024a). Russian cyber operations: Analysis for the second half of 2023. Retrieved

from https://cip.gov.ua/services/cm/api/attachment/download?id=68775

Stokel-Walker, C. (2022). Ukraine's cyberwar chief sounds like he's winning. *Wired.* Retrieved from https://www.wired.com/story/yurii-shchyhol-urkaine-cyberwar-russia/?utm_source

Sulowski, S. (2023). *Security challenges at the dawn of a new international order.* Berlin: Peter Lang Verlag.

Tabansky, L. (2020). Israel Defence Forces and national cyber defence. *Connections: The Quarterly Journal, 19*(1), 45-62. https://doi.org/10.11610/Connections.19.1.05

The White House. (2023). National Cybersecurity Strategy. Retrieved from https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Transparency International Ukraine. (2024). Wartime and post-war resilience: Reform fundamentals in Ukraine. Retrieved from https://ti-ukraine.org/en/news/wartime-and-post-war-resilience-reform-fundamentals-in-ukraine/?utm_source

Voloshchuk, Y., Lavruk, N., Derlytsia, A., Havryliuk, V., & Kulii-Demianiuk, Y. (2025). The role of public investment in innovative projects during martial law. *Economics of Development, 24*(1), 45-46. https://doi.org/10.63341/econ/1.2025.45

Weaver, J.M. (2022). *The U.S. cybersecurity and intelligence analysis challenges.* London: Palgrave Macmillan Cham.

Wilson, A. (2023). Reformation nation: Wartime politics in Ukraine. *European Council on Foreign Relations.* Retrieved from https://ecfr.eu/publication/reformation-nation-wartime-politics-in-ukraine/?utm_source#summary

Yagunov, D., Polovyi, M., Melnychuk, T., Starenkyi, S., Sokalska, O., Chernousov, A., Trokhymchuk, V., & Anishchenko, V. (2023). The phenomenon of informal prison hierarchies and the simulacrum of prison subculture in contemporary power relations. *Evropský Politický a Právní Diskurz, 10*(4), 5-51. https://doi.org/10.46340/eppd.2023.10.4

Yakymchuk, O. (2019). State management of cyber security in hybrid war conditions. *Pressing Problems of Public Administration, 1*(55), 35-40. https://doi.org/10.34213/ap.19.01.04

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

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