NAM Studies & Documents

Special Dossier October 2025
Ukraine Military and Wartime Law

Edited by Ganna Sobko

ꙗ҃рославъ
мꙋдрꙑй

NAM Studies & Documents

Special Dossier October 2025
Ukraine Military and Wartime Law

Edited by Ganna Sobko

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)

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.

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:

$$I \cap \Pi = H \ (1),$$

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

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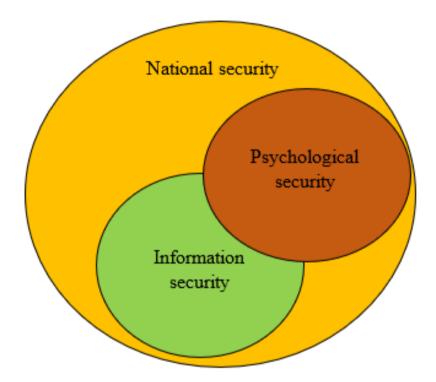

Figure 1. The interrelation of national security factors

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%B-F%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-d%d1%84%d0%be%d1%80%d0%bc%d0%b0%d1%86%d1%96%d0%b9%d0%b-d%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%9
6%D0%B9-%D0%91%D0%96%D0%94-%D0%A6%D0%97-%D0%A4%D0%9-
C%D0%9C-%D1%80%D0%B5%D0%B42020-.pdf

Liu, T., Wang, H.Z., Wang, H.Z., & Xu, H. (2021). The spatiotemporal evolution of eco-
logical security in China based on the ecological footprint model with localization of
parameters. *Ecological Indicators, 126,* 107636. Retrieved from https://www.science-
direct.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 con-
ditions of the state of martial. Retrieved from https://univd.edu.ua/science-issue/is-
sue/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-Informatsiy-
na-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 Secu-
rity 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 Na-
tional 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 identifi-
cation 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

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

Special Dossier October 2025
Ukraine Military and Wartime Law