Language – Culture – Politics, Vol. 1/2023
ISSN 2450-3576
e-ISSN: 2719-3217

DOI: 10.54515/lcp.2023.1.227-245

Marianna Gladysh
Ivan Franko National University of Lviv (Ukraine)
ORCID 0000-0003-4236-7110

Sergii Pakhomenko
Mariupol State University, Kyiv, (Ukraine)
ORCID 0000-0003-1137-3585

Oleksandr Kuchyk
Ivan Franko National University of Lviv (Ukraine)
ORCID 0000-0001-9767-9520

The Information Resilience of Ukraine and the EU in Terms of Russian Aggression

Odporność informacyjna Ukrainy i UE w warunkach rosyjskiej agresji

Abstract

This article examines the peculiarities of the information resilience of Ukraine and the EU, and their similarities and differences. Special attention is paid to the transformation of the information resilience of Ukraine before and during Russia's aggression. Information resilience is considered in close connection with information security, with the correlations between them being revealed and the main constituent elements of these phenomena being determined. The authors analyse the communication aspects of information resilience, not taking into account the purely technological perspective of cyberspace protection but concentrating on measures aimed at blocking and disavowing the hostile information content that affects the cognitive stability of Ukrainian citizens.

Key words: *information resilience, information security, propaganda, Ukraine, EU.*

Abstrakt

W artykule podjęty został temat odporności społecznej w przestrzeni informacyjnej Ukrainy i UE z uwzględnieniem podobieństw oraz różnic w tym zakresie. Szczególną uwagę zwrócono na przeobrażenia odporności informacyjnej w związku z rosyjską agresją na Ukrainę. Odporność informacyjna rozpatrywana jest w kontekście bezpieczeństwa informacji; wskazane zostały również zależności między tymi zjawiskami, a także ich podstawowe elementy.

W swoich analizach autorzy uwzględniają komunikacyjny aspekt odporności informacyjnej, pomijając kwestię ochrony informacji w cyberprzestrzeni. Przedmiotem ich zainteresowań są zatem działania mające na celu blokowanie i dezawuowanie wrogich treści informacyjnych, które wpływają negatywnie na procesy poznawcze obywateli Ukrainy.

Słowa kluczowe: *odporność informacyjna, bezpieczeństwo informacyjne, propaganda, Ukraina, UE.*

Introduction

The beginning of Russia's full-scale aggression against Ukraine in February 2022 highlighted, in political and scientific discourse, the need to rethink many processes and phenomena. The identification of the Russian-Ukrainian armed conflict as a hybrid war from 2014 to 2022 revealed certain problematic aspects in the process of resolving the interstate conflict. At the same time, the very interpretation of the conflict as a hybrid war has sharpened the attention of scholars and experts on the non-convective elements of warfare and its widespread use in interstate confrontation in the international arena. In view of this, the problem of effective use of information warfare tools in the field of propaganda, special information operations, information manipulation, and the use of information as another weapon in the information space, is significantly relevant. Therefore, the issue of information security and resilience has taken a key place on the agendas of the political leadership of Ukraine and the EU, and set about the task of developing an effective model for managing the use of information and the protection of information security.

Methodologically, the authors follow a structural-functional approach and consider information resilience as a functional system, the deviation of which, from the optimal level due to Russian aggression, has led to a redistribution of some of its parameters by limiting information needs to the enhancement of information security. This synergetic approach allows one to clarify the interaction and complementarity of the efforts of the state and civil society in providing protection from hostile information influence. Using the case study method, the information and communication problems related to the siege of Mariupol by Russian troops and the causes and consequences of the information vacuum in which citizens found themselves, are studied.

Concepts of information security and information resilience

The role of information and information technologies in the modern world is extremely important. Together with the rapid development of information technologies, new and already existing information risks are arising and pose direct threats to the national security of a state, the security of a society as a whole, and every individual's security. In today's conditions, the information component of a state's national security plays an extremely important role due to the risks and threats present in it, which include cyber terrorism, cybercrime, aggressive propaganda, the spread of anti-constitutional or anti-state slogans, and the limiting of a population's access to public information.

Ensuring the information security of a state includes information and analytical support of the activities of state bodies, information support for the work of internal and foreign policy bodies, a system of protection of information with limited access, and combating offenses in the information sphere and computer crimes. (Bodnar, 2014, p. 69) Ensuring the information security of a state through the consistent implementation of a national information strategy contributes to ensuring success in solving problems in political, military-political, social, economic, and other spheres of state activity. Implementation of information policy can directly affect the solution to domestic, foreign, and military conflicts.

Information security has a special place in the general system of national security of a state, as it is an element of all components of a security system. Any challenges or threats to a country's national security are directly related to its informational factor.

The general national security system includes several subsystems: state-political, ecological, economic, social, and informational. The information security subsystem has a special place because: (a) information relations and processes permeate all other relations and processes taking place in society, and therefore information security, as a component, is included in all other subsystems of national security; (b) in modern conditions, when various information technologies and processes, by means of computer technology, are intensively and massively implemented in many areas of human activity, the issue of information security acquires an independent social significance; (c) the system of external and internal information security risks has a complex nature.

Public institutions are full-fledged participants in the process of ensuring the information security of a state. As social and political practice shows, the efforts of the state are usually not enough to effectively counter information threats, which determines the need to build dialogue with society. The basic elements of the mechanism of interaction between the government and society in this field has institutional, legal, and practical components. The effectiveness of an entire state information security system depends on the full use of all opportunities and resources available in a society.

The information security of a state should be considered as an important component of state policy in the fields of information protection and the information space, especially in crisis situations when the use of information by an adversary can lead to material and non-material losses. Therefore, it can be assumed that the information sphere of state activity and the formation of information resilience, especially in the conditions of the latest challenges of wartime, are an integral part of a state's strategic goals in the international arena.

The concept of "resilience" is quite multifaceted and is used in different areas. The increase in the level of global threats in ecology and climate change has caused the need to look for new ways to protect against natural disasters and ensure livelihoods in crisis conditions. Since then, terms such as resilience of the ecosystem and infrastructure have become widely used. Subsequently, the range of threats to both states and people has only expanded. The tasks of building a state and society's resilience to terrorist threats, information attacks, and its computer systems to hacking, and promoting the stability of financial systems and ultimately national stability are on the agenda.

We may state that information resilience is an integral part of information security. Acquiring such a characteristic as resilience allows a state and society to effectively counteract threats of any origin and nature, adapt to sudden and unpredictable changes in the security environment, maintain stable functioning before, during, and after a crisis, and quickly recover to a desired balance. This allows a state to endure (sometimes survive) in very difficult, even critical circumstances that cannot be avoided. This is where the difference between security and resilience is manifested: if we have not overcome a threat, we are in danger, and if a threat cannot be overcome completely or is inevitable, lasting for a long period, we must endure and suffer as little losses as possible.

The Information resilience of the EU

Information security within the European Union is considered, first of all, as the condition of information networks and systems that provides a sufficient level of protection for the integrity, availability, and confidentiality of information and an appropriate level of counteraction to external negative influences. Accordingly, one of the priorities of the policy of EU countries in the field of information security is to develop and implement programs and various technical means that allow the maintenance of a certain level of protection of information and communication technologies.

Another priority of EU policy is the information security of its citizens. In particular this includes a high level of public awareness of information risks and technological threats, and the ways to protect information systems/networks from unwanted influence. This includes not only countering cyber-attacks, but also personal data protection and the detection of malicious content on the Internet.

At the current stage, the issues of network and information security are gaining special importance for EU member states. European specialists in the fields of information systems, security, and strategic planning are actively discussing the problems facing the states of the European Union in terms of the possibility of using information weapons. This mainly concerns the means of direct influence on the information resources of a probable adversary in wartime and peacetime. Today, plans for the organizational and technical support of national information security, including units designed to repel "informational aggression", are being created. Governments are taking the role of coordinator of interagency efforts in this area.

In 2001, the European Commission presented a document entitled "Network and Information security: Proposal for a European Policy Approach" which outlined the European approach to the problem of information security and identified the following directions of European information security policy:

- increasing user awareness of possible threats when using communications networks;
- the creation of a European system of warning and informing about new threats;
- the provision of technological support;

- support of market-oriented standardization and certification;
- legal support;
- the strengthening of security at the state level;
- the development of international cooperation on information security issues. (EC, 2001, p. 4).

To strengthen the capabilities of the European community for member states and business circles in the field of prevention of and response to problems related to information security, the European Network and Information Security Agency (ENISA) was established in 2004. In 2008-2009, the Agency created a structure/system entitled Emerging and Future Risks which assists stakeholders to better identify and understand current and future risks. The agency also launched a Forum on security issues and created expert groups that assess and analyse relevant problems.

Since the information society has granted every citizen of EU member states the right to access different open data such as laws, government decisions, literary works, scientific works, software, and open information in computer networks and systems, the protection of personal data has become a serious problem for the EU.

In 2017, the European Commission presented a new document entitled “Resilience, Deterrence and Protection: Building Strong Cybersecurity for the EU”, which states that cyber security is crucial for the prosperity and security of member states. If cyber security measures are not taken, the risk of threats will increase according to digital transformations.

Information security is an integral part of EU resilience. Before the beginning of the Ukrainian-Russian crisis in 2014, in conceptual documents of the European Union related to general security issues (European Security Strategy “Secure Europe in a Better World” of 2003 and the Report on its Implementation of 2008) the issue of the EU resilience was not raised.

In the Communiqué of the European Commission on October 3, 2012, resilience was mentioned but related to the worsening situation in North-East Africa caused by the food crisis in that region. At that time, the EU defined resilience as “the ability of an individual, a household, a community, a country or a region to withstand, to adapt, and to quickly recover from stresses and shocks”. (EC, 2012, p. 5)

The annexation of Crimea and the events in the East of Ukraine led the EU to search for a solution to the problem of ensuring the resilience of the state and society in the conditions of modern challenges and threats.

In May 2015, the Council of Ministers of Foreign Affairs of the European Union, in expressing concern about the situation on the continent and in the world, called for “actionable proposals to help countering hybrid threats and foster the resilience of the EU and its Member States as well as partners”. (*Council of the European Union*, 2015, p. 3) This signalled the beginning of the development of a new European Security Strategy. At the same time, the EU Institute for Security Studies published a report entitled “Towards the EU Global Strategy: Background, Process, Recommendations”, in which, based on an analysis of European Union documents, particularly the 2010 Strategic Concept of NATO 2010 and the 2015 National Security Strategy of the USA, the importance of resilience to ensure safety was emphasized.

In April 2016, the High Representative of the European Union for Foreign Affairs and Security Policy, the Vice-President of the European Commission, Federica Mogherini, submitted to the governing bodies of the organization a document entitled “Joint Program to Counter Hybrid Threats: The European Union’s Response” where the need to have resilience potential as one of the main goals of the EU was stated. The document noted that the resilience of the European Union as a whole depends on the resilience of its member states. Most of the 22 announced measures call for an increased resilience in energy and cyber security and countering radicalization and extremism, including through cooperation with external partners. (*High Representative...*, 2016)

In June 2016, the Global Strategy of the EU’s foreign and security policy “Shared vision, shared action: a stronger Europe” was presented and it states that strengthening the resilience of the democratic states of the European Union is one of the most important principles of the organization. It also included a list of strategic priorities of EU activity for ensuring the security of cyber infrastructure, the energy sector, strategic communications, and components of the “European electronic digital space”. (*Global Strategy...*, 2016)

It should be noted that over the past few years, the tendency towards rapprochement in the approaches of NATO and the European Union in ensuring resilience has strengthened. This was caused by complications in the international situation, the commonality of views on security issues, and the fact that most EU countries are NATO members as well.

Cooperation between NATO and the EU has been strengthened in four areas: civil-military planning; cyber protection; information exchange; and analysis and coordinated strategic communication for the purpose of the detection of disinformation and transmission of true information. One of the first results of this was a technical agreement on information exchange between the NATO Computer Incident Response Team and the EU Computer Emergency Response Team, signed in early 2016. (NATO, 2016)

In October 2017, the EU Expert Center for Countering Hybrid Threats was opened in Helsinki to implement the “Joint Program for Countering Hybrid Threats: The European Union’s Response”. On its basis, exchange of experience between the member states of the European Union and NATO and training of specialists in this field are held regularly.

Based on the goals for which NATO and the EU were formed, there are certain differences in their approaches to understanding resilience. For NATO resilience was primarily related to the principles of military cooperation and deterrence. However, due to the large-scale and multifaceted aggressive actions of the Russian Federation in the international arena, NATO is currently striving to the increase resilience of member countries of the Alliance in both the military and civilian spheres, considering the latter as one of the main factors that ensures the combat effectiveness of the military component of the defensive bloc. At the same time, the EU used the concept of resilience in the context of state building, good governance, human rights, and sustainable development. However, recently there has been an effort to develop the security component of the EU’s activities, as well as a tendency to expand cooperation with NATO, with the aim of countering threats in the information sphere.

The full-scale aggression against Ukraine also created new challenges to the EU in the sphere of information security and resilience. As a response to this, on April 23, 2022 an extremely important event for the digital services market took place in the European Union: a political agreement was reached between the European Parliament and EU member states on establishing rules for ensuring a safe and secure online environment and, as a result, the Digital Services Act (DSA) was adopted. (EC, 2020) According to a press release from the European Commission, the DSA sets an unprecedented new standard for the liability of online platforms for illegal and harmful content. This should provide a better protection for Internet users and their fundamental rights, and define a single set of rules in the internal market, thus helping smaller online platforms expand. In fact, the purpose of the DSA is to set the rules for conducting online business. However, the introduction of clear and transparent rules should not be equated with “tightening the nuts”. Indeed, until recently, the Internet space seemed limitless in terms of its possibilities and, at the same time, free from strict legal regulation. The DSA will be precisely the starting point when search engines, online platforms, and social networks will have to take responsibility for the quality and content of the information at their disposal and the digital services they provide directly or as intermediaries.

The Information resilience of Ukraine

The formation resilience of Ukraine is considered as part of national security. As stated in Article 17 of the Constitution of Ukraine: "Protecting the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the entire Ukrainian people." (*Supreme Council of Ukraine*, 1996) Mention of information security in the legislation of Ukraine and its development within a legal framework can be traced back to the time of independence, however, a separate block of national strategy refers to more modern documents when Ukraine faced the hybrid aggression of the Russian Federation.

Considering the period from Ukraine's regaining of independence in 1991 until 2014, following legal documents can be singled out in which the information security of Ukraine is mentioned or has a separate place.

In 1992, the Law of Ukraine "On the Security Service of Ukraine" and the Law of Ukraine "On Information" were adopted, in which information security was indirectly mentioned. In the first Law, it was stated that the Central Department of the Security Service of Ukraine is responsible for state security, in particular in the field of information security. The Law "On Information" states that one of the main directions of state information policy is to ensure the information security of Ukraine.

In the National Security Strategy of Ukraine, which was approved by the decree of the President of Ukraine in 2007 and expired in 2015, the key tasks of national security policy in the internal sphere of ensuring information security are defined as the development and implementation of national standards and technical regulations for the use of information so that communication technologies are harmonized with the relevant standards of EU Member States, including the requirements of the Convention on cybercrime. In modern realities, such tasks cannot satisfy all the needs of Ukraine's informational sovereignty.

In 2007, the Law of Ukraine "On the Basic Principles of the Development of the Information Society in Ukraine for 2007-2015" was adopted, in which for the first time in Ukrainian legislation the concept of information security is separately considered and the ways of solving problems related to it are determined. According to this Law: "Information security is a state of protection of the vital interests of a person, society and the state, in which harm is prevented due to: incompleteness, untimeliness and implausibility of the information used; negative information impact; negative consequences of the use of information technologies; unauthorized distribution, use and violation of integrity, confidentiality and availability of information". (*Supreme Council of Ukraine*, 2007)

The Law of Ukraine "On Access to Public Information", which was adopted in 2011, states that limiting access to information is carried out exclusively in the interests of national security, territorial integrity, and public order.

The decision of the National Security and Defence Council of Ukraine dated April 28, 2014, "On measures to improve the formation and implementation of state policy in the field of information security of Ukraine", contains a list of actions that Ukraine had to take in connection with the start of the hybrid war of the Russian Federation against Ukraine. Here, for the first time, Ukrainian legislation raises the issue of ensuring information security against the negative influence of foreign countries, which is described as: "countering the informational aggression of foreign countries, determining the mechanism for countering negative informational and psychological influence, including by banning the retransmission of television channels, as well as regarding the introduction for foreign mass media systems of information and protection of journalists who work in places of armed conflicts, terrorist acts and during the liquidation of dangerous criminal groups". (*National Security and Defence Council of Ukraine*, 2014)

The Decree of the President of Ukraine dated May 26, 2015: "On the implementation of the decision of the National Security and Defense Council of Ukraine", and dated May 6, 2015: "On the National Security Strategy of Ukraine", approved a very important document concerning the regulatory and legal determination of the state of information security in Ukraine. Threats to Ukraine's information security include: the waging of an information war against Ukraine; the lack of a coherent communication policy of the part of the state, and an insufficient level of media culture within Ukrainian society. The priorities of ensuring information security were determined, among which, in the active information war that is being waged by the Russian Federation against Ukraine, it is very important to counter information operations against Ukraine, the manipulation of public consciousness, the spread of distorted information, protect of national values, and strengthen the unity of Ukrainian society, and identify entities in the Ukrainian information space that were created and/or used by Russia to conduct information warfare against Ukraine and prevent their subversive activities. Among these priorities were also identified the following ones: ensuring the offensiveness of information security policy measures based on asymmetric actions against all forms and manifestations of information aggression; the creation of an integrated system of information threat assessment and prompt responses to such threats; the development and implementation of a coordinated information policy by state authorities; the creation and development of institutions responsible for information and psychological security, taking into account the practices of NATO member states; improvement of professional training in the field of information security; and the implementation of nationwide educational programs on media culture with the involvement of civil society and businesses.

The Law of Ukraine "On the National Security of Ukraine" of 2018 also defines information security as a component of Ukraine's national security. It is noted here that one of the functions of the Security Service of Ukraine is counterintelligence protection, and in particular when considering the information security of the state. "The National Security Strategy of Ukraine of 2020" states that this is the basis for the development of such planning documents in the spheres of national security and defence, which will determine the ways and tools of its implementation, including the Information Security Strategy.

In 2021, the Information Security Strategy was approved by the Decree of the President of Ukraine. It is noted that ensuring the information security of Ukraine is one of the most important functions of the state. According to the Strategy, the information security of Ukraine is an integral part of the national security of Ukraine; it states that the protection of state sovereignty, territorial integrity, democratic constitutional order, and other vital interests of an individual, a society, and the state, in which the constitutional rights and freedoms of each person to collect, store, use, and distribute information are fundamental, are guaranteed through access to reliable and objective information. It is worth noting that this definition is much more extended and, accordingly, more adapted to the modern needs of the information society than the one provided in the Law of Ukraine "On the Basic Principles of the Development of the Information Society in Ukraine for 2007-2015". The Strategy also states that the main areas of ensuring Ukraine's information security are resilience and interaction. In this Strategy, for the first time in Ukrainian legislation, the concept of information resilience is used, the provision of which should serve to achieve the goal of the Strategy, namely the provision of information security for the state, its information space, support of social and political stability, state defence, protection of state sovereignty, territorial integrity with informational means and measures of Ukraine, the democratic constitutional system, and ensuring of the rights and freedoms of every citizen. The achievement of this goal will be carried out by taking measures to deter and counter threats to the information security of Ukraine, neutralizing information aggression, ensuring the information stability of society and the state, creating an effective system of interaction between state authorities, local self-government bodies, and society, and development of international cooperation in the field of information security practiced on the basis of partnership and mutual support.

A Decree of the President of Ukraine in 2021 approved the Decision of the National Security and Defence Council of Ukraine "On the introduction of the national resilience system". It is noted that the implemented national resilience system should provide for social resilience, in particular, to informational threats.

The Decision of the National Security and Defense Council of Ukraine on December 30, 2021, "On the Strategy for Ensuring State Security", was put into effect by the Decree of the President of Ukraine dated February 16, 2022. This document supports the concept of information security and states that: "information security is a state of protection of the national interests of a person, a society and the state in the information sphere, in which it is impossible to cause harm due to: incompleteness, untimeliness and implausibility of the information used, negative informational influence; leakage of state secrets and official information; negative consequences of the use of information technologies; unauthorized dissemination, use and violation of the integrity, confidentiality and availability of information by conducting special information operations and destructive informational influences by foreign special services, individual organizations, groups, and individuals, as well as ensuring timely detection, prevention and neutralization of real and potential threats to national interests and national security of Ukraine. Information security is a component of Ukraine's national security". (*National Security and Defence Council of Ukraine*, 2021b)

This definition is even more extensive than the one provided in the 2021 Information Security Strategy of Ukraine. However, it is worth noting that the three different definitions of information security in the current Laws of Ukraine are a certain manifestation of a terminological definition that has not been finally adopted. The lack of a comprehensive information policy of the state, an insufficient development of the national information infrastructure, and the weakness of the strategic communications system make it difficult to neutralize this threat against the background of the information expansion of the Russian Federation, in particular in expanding its own information infrastructure and the structures controlled by it in the temporarily occupied territories of the Autonomous Republic of Crimea and the city of Sevastopol, as well as in certain areas of the Donetsk and Luhansk regions.

Due to the beginning of the full-scale war in Ukraine on February 24, 2022, the state's information security regulatory framework had to adapt to new challenges. The National Security and Defence Council of Ukraine (NSDC) adopted the Decision "On neutralizing threats to the information security of the state" on March 18, 2022, which was put into effect by the Decree of the President of Ukraine on March 19, 2022. The NSDC decided to ensure the Administration of the State Service of Special Communications and Information Protection of Ukraine and the Radio Broadcasting, Radio Communications, and Television Concern together with Zeonbud LLP. This included the stable operation of digital broadcast facilities, the uninterrupted broadcast of television channels in MH -1, -2, -3, and -5; the continuous monitoring of broadcast networks, the equipping of the main multiplexing station, satellite, and terrestrial communication channels; the reservation of satellite channels for the delivery of programs and the equipping of the main multiplexing station; and the backup delivery of TV channels to digital transmitters with the involvement of an alternative satellite operator.

Also, on March 18, 2022, the National Security Council of Ukraine adopted the Decision "On implementation of a unified information policy under martial law", which was also implemented by the Decree of the President of Ukraine on March 19, 2022. The National Security Council decided to establish in the conditions of martial law the implementation of a unified information policy as a priority issue of national security, the provision of which was implemented by unifying all national TV channels, the programming content of which consists mainly of informational and/or analytical programs on a single information platform of strategic communication This being a 24-hour informational marathon of "The only news #Uatogether".

It is worth adding that Ukrainian analytical centers (ex. the Razumkov analytical centre) are considering the problem of Ukraine's security environment and emphasizing the military, economic, and political spheres, but not the cyber security sphere. The issue of information security is mentioned only indirectly in the documents thereof and is almost never studied separately. However, as the Razumkov Center notes in its 2021 study "Ukraine-EU Partnership in the Security Sphere: Current State and Prospects", the absolute majority of Ukrainian and foreign experts believe that Ukraine is capable (to a full extent or to a limited extent) of being an important partner of the EU in the sphere of security. In particular, these experts stress Ukraine's ability to share its experience in practical participation of countering Russian propaganda and disinformation.

In the analytical document of the Centre for Global Studies "Strategy XXI" "Strategic communications in the focus of Ukraine-EU-NATO cooperation in modern conditions", main attention is paid to information security.

The study claims that effective countermeasures against threats in Russia's hybrid war against Ukraine require the formation of information messages necessary to counter Russian aggression, which is important not only for Ukraine but also for NATO and the EU, as they all need a clear vision and definition of such threats. It is also noted that the threats to Ukraine, the EU, and NATO are similar and the source of their origin is the same – the Russian Federation. Therefore, for Ukraine, which has already achieved some success in the development of strategic communications at the national level, it is very important to deepen its cooperation in strategic communications both with each of the previously mentioned organizations separately and in the context of their security cooperation.

We may state that the development of the normative and legal framework of Ukraine on the problem of information security took place under the influence of external factors, namely, the hybrid aggression of the Russian Federation. An increasing number of new challenges force the legislation of Ukraine to adapt, which makes the state informationally resilient and modern in the field of information security.

The issue of ending the Russian-Ukrainian war lies within a complex solution of a number of parameters. First of all, it concerns the restoration of the territorial integrity and sovereignty of Ukraine. It is clear that the recovery of the economy and post-war reconstruction remain a priority area of state building. At the same time, the importance of strengthening the information security of the state through the expansion of cooperation with international structures within the framework of cooperation programs with NATO and the European Union should not be dismissed.

Conclusions

It can be stated that information security is one of the key elements of state security policy, which is carried out in at least two dimensions, technologically through ensuring the technological process of accumulation, storage, protection, and transmission of information, as well as humanitary through the production, distribution in the information space, and formation of an appropriate information picture of the world. Information resilience is an integral part of the information security of any state.

The EU considers its main task in ensuring information security through the introduction of measures that will make it possible to prevent and change the consequences of external informational influence. Understanding the importance of a unified system of information protection, the European Union is trying to organize a collective and wide-ranging approach to ensure the information security of both individual EU member states and the Union as a whole. Political priorities in the field of information security, determined by the governing bodies of the European Union, are implemented at the national level by state bodies, authorities, and non-governmental organizations.

Over the past decades, Ukraine has formed a fairly thorough regulatory and legal framework for the protection of the information space, the preservation and transmission of information, and the functioning of state and non-state institutions within the context of a single system of information activity. Normative and legal regulation meets democratic standards and respect for the rights and freedoms of citizens in the field of obtaining and accessing information.

The introduction of martial law, beginning with the full-scale aggression of the Russian Federation against Ukraine in February 2022, introduced certain adjustments and restrictions to the rights and freedoms of citizens in the field of information circulation. At the same time, as evidenced by an analysis of legal norms and the practice of information use, this is aimed at strengthening control over the circulation and use of information materials and flows in order to ensure the information security of the Ukrainian state from external destructive influences. The improvement of the legislative provision of information activity has a promising character in the context of expanding cooperation with civil society institutions and the development of mutually beneficial interstate cooperation within the framework of the European and Euro-Atlantic integration of Ukraine, which is one of the priorities of Ukraine's foreign policy.

The positive experience and development of NATO and the EU in the course of their development of conceptual and strategic documents on strengthening the resilience of the member states of these organizations should be taken into account in the course of reforming the security and defence sector of Ukraine, strengthening its own resilience, and approaching the standards of the Euro-Atlantic and European communities.

Bibliography

Bodnar, I. (2014). "Information security as a basis of national security". In: *Mechanism of Economic Regulation*, no. 1.

Centre for Global Studies "Strategy XXI". (2019). *Strategic communications in the focus of Ukraine-EU-NATO cooperation in modern conditions.* https://geostrategy.org.ua/analityka/analitychna-zapyska/strategichni-komunikaciyi-u-fokusi-spivrobitnyctva-ukrayina-yes-nato-v-suchasnyh-umovah1, 20.03.2023.

Council of the European Union. (2015). *Council Conclusions on CSDP.* https: // www.consilium.europa.eu/en/press/press-releases/2015/05/18/council-conclusions-csdp/, 20.03.2023.

EC. (1994), *Europe and Global Information Society. Recommendations of the High-Level Group on the Information Society to the Corfu European Council (Bangemann Group).* https://cordis.europa.eu/article/id/2730-bangemann-report-europe-and-the - global - information - society, 20.03.2023.

EC. (2001). *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for A European Policy Approach.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from = EN, 20.03.2023.

EC. (2012). *Communication from the Commission to the European Parliament and the Council the EU approach to resilience: Learning from food security crises.* http://ec.europa.eu/echo/files/policies/resilience/com_2012_586_resilience_en.pdf, 20.03.2023.

EC. (2017). *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU: adopted by the European Commission on 13 September 2017.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN, 20.03.2023.

EC. (2020). *Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.* https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020 % 3 A825%3AFIN, 20.03.2023.

Global Strategy for the European Union's Foreign And Security Policy. (2016), *Shared Vision, Common Action: A Stronger Europe.* https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf, 20.03.2023.

High Representative for Foreign Affairs and Security Policy. (2016), *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response*, https://ccdcoe.org/sites/default/files/documents/EU-160406-JointFrameworkOnCounteringHybridThreats.pdf, 20.03.2023.

Horbatyuk, O. (1999). "Current state and problems of information security of Ukraine at the turn of the century". In: *Bulletin of T. Shevchenko Kyiv University. International relations*, issue 14.

Missiroli, A. (ed.). (2015). *Towards an EU Global Strategy: Background, processes, references. Paris: European Union Institute for Security Studies.* https://europa.eu/globalstrategy/en/towards-eu-global-strategy-%E2%80%93-background-process-references, 20.03.2023.

National Security and Defence Council of Ukraine (2014), *Decision of the National Security and Defence Council of Ukraine on April 28, 2014 "On measures to improve the formation and implementation of state policy in the field of information security of Ukraine"*, https://zakon.rada.gov.ua/laws/show/n0004525-14%20#Text, 20.03.2023.

National Security and Defence Council of Ukraine. (2015). *Decision of the National Security and Defence Council of Ukraine on May 6, 2015 "On the National Security Strategy of Ukraine"*. https://zakon.rada.gov.ua/laws/show/287/2015#Text, 20.03.2023.

National Security and Defence Council of Ukraine. (2020). *Decision of the National Security and Defence Council of Ukraine on September 14, 2020 "On the National Security Strategy of Ukraine"*. https://zakon.rada.gov.ua/laws/show/392/2020#Text, 20.03.2023.

National Security and Defence Council of Ukraine. (2021a), *Decision of the National Security and Defence Council of Ukraine on August 20, 2021 "On the Introduction of the National Resilience System"*. https://zakon.rada.gov.ua/laws/show/479/2021#Text, 20.03.2023.

National Security and Defence Council of Ukraine. (2021b). *Decision of the National Security and Defence Council of Ukraine on December 30, 2021 "On the Strategy for Ensuring State Security"*. https://zakon.rada.gov.ua/laws/show/56/2022#Text, 20.03.2023.

National Security and Defence Council of Ukraine. (2021c). *Decision of the National Security and Defence Council of Ukraine on October 15, 2021 "On Information Security Strategy"*. https://zakon.rada.gov.ua/laws/show/685/2021#Text, 20.03.2023.

National Security and Defence Council of Ukraine. (2022a). *Decision of the National Security and Defence Council of Ukraine on March 18, 2022 "On neutralization of threats to the information security of the state"*. https://zakon.rada.gov.ua/laws/show/151/2022#Text, 20.03.2023.

National Security and Defence Council of Ukraine. (2022b). *Decision of the National Security and Defence Council of Ukraine on March 18, 2022 "On implementation of a unified information policy under martial law"*. https: // zakon.rada.gov.ua / laws / show / n0004525-22#Text, 20.03.2023.

NATO. (2016). *NATO Resilience: a core element of collective defence.* https: // www.nato.int/docu/review/2016/Also-in2016/nato-defence-cyber-resilience/EN/index.htm, 20.03.2023.

President of Ukraine. (2007), *Decree of the President of Ukraine "On the National Security Strategy of Ukraine" on February 12.* https:// zakon.rada.gov.ua/laws/show/105/2007#Text, 20.03.2023.

Supreme Council of Ukraine. (1992a). *Law of Ukraine "On Information".* https://zakon.rada.gov.ua/laws/show/2657-12#Text, 20.03.2023.

Supreme Council of Ukraine. (1992b). *Law of Ukraine "On the Security Service of Ukraine".* https://zakon.rada.gov.ua/laws/show/2229-12 #Text, 20.03.2023.

Supreme Council of Ukraine. (1996). *The Constitution of Ukraine on June 28, 1996 (with amendments).* https://zakon.rada.gov.ua/laws/show/ 254%D0%BA/96-%D0%B2%D1%80#Text, 20.03.2023.

Supreme Council of Ukraine. (2007). *Law of Ukraine "On the Basic Principles of Information Society Development in Ukraine for 2007-2015".* https://zakon.rada.gov.ua/laws/show/537-16#Text, 20.03.2023.

Supreme Council of Ukraine. (2011). *Law of Ukraine "On Access to Public Information".* https://zakon.rada.gov.ua/laws/show/2939-17#Text, 20.03.2023.

Supreme Council of Ukraine. (2018). *Law of Ukraine "On National Security of Ukraine"* https://zakon.rada.gov.ua/laws/show/2469-19#Text, 20.03.2023.

Acknowledgements: 30% of this paper's text written by Sergii Pakhomenko has been included in the framework of project 31160 (O-006): "Strategic communication in context of the war in Ukraine: lessons learners for Estonia" (30.01.2023-30-12.2025), Estonian Military Academy.

Correspondence concerning this paper should be addressed to Dr. Marianna Gladysh, Associate Professor of the Department of International Security and Crisis Management, Ivan Franko National University of Lviv, Ukraine.
E-mail: marianna.hladysh@lnu.edu.ua

Dr. Sergii Pakhomenko, Visiting Associate Professor of the Department of Communication Studies, Faculty of Social Sciences, University of Latvia; Associate Professor of the Department of Political Science and International Relations, Mariupol State University, Kyiv, Ukraine.
E-mail: pakhomenko.s@ukr.net

Dr. Oleksandr Kuchyk, Associate Professor of the Department of International Security and Crisis Management, Ivan Franko National University of Lviv, Ukraine.
E-mail: oleksandr.kuchyk@lnu.edu.ua