DOI: 10.46340/eppd.2023.10.1.6

Andrii Pravdiuk, PhD in Law
ORCID ID: https://orcid.org/0000-0002-5248-8111
Vinnytsia National Agrarian University, Ukraine

INFORMATION SECURITY OF UKRAINE: INFORMATION INFLUENCE AND INFORMATION WARS

The article is devoted to the current problem of information security of Ukraine and the protection of the national information space from negative propaganda and manipulative informational and psychological influences. It is emphasized that the problem is actualized in the conditions of the Ukrainian-Russian conflict, when the provision of information security turns into a factor of preserving the national identity of Ukraine and its functioning as a sovereign independent state. The transition to the information society, the processes of globalization, the development of the latest technologies and the new challenges of modernity have led to the emergence of new ways of waging war and have radically changed the international security system. The principles, resources and means of warfare have changed significantly. Modern challenges and threats to the system of global information security have led to a rethinking of the conceptual and practical foundations of international cooperation in the field of information security. In order to maintain security and stability in the modern world, uniform rules, principles and standards of responsibility must be adopted. The article attempts to analyze theoretical approaches to defining the essence of such concepts as information security and threats to information security. The manifestation of socio-legal nature in such a recent globalization phenomenon as information war is considered. It has been proven that manipulation of information through psychological influence on the opponent has long been a means of waging war. It is indicated that the peculiarity of the information war is not only that the influence is carried out using the latest means, but also that it is an uncontrolled resource that is very weakly amenable to legal regulation, therefore it actively uses false, distorted information as a means of manipulating consciousness. The approaches of scientists who researched certain aspects of the information struggle were analyzed, appropriate conclusions were drawn based on their work, and the conceptual basis of the article was formed.

Keywords: information besiege, information war, means of warfare, information resources, information influence.

Formulation of the problem. In the conditions of modern global and regional information confrontations, destructive communicative influences, the clash of multi-vector national information interests, the spread of information expansion and aggression, the protection of the national information space and the guarantee of information security become the priority strategic tasks of modern states in the system of global information relations. Preservation of information sovereignty, formation of an effective security system in the information sphere is an urgent problem for Ukraine, which is often the object of external information expansion, manipulative propaganda technologies, and destructive information invasion.

After February 24, 2022, the civilized world has changed, security is no longer provided by rational agreements and inviolable state institutions. Unfortunately, modern realities have shown that modern international institutions are not capable of creating obligations for states by virtue of the powers granted to them by statutory documents, even with the direct consent of the state to the obligation of such an obligation, as an example of which can be the resolutions of the UN Security Council, to which states must obey due to their membership in the UN, but the Russian Federation demonstrated all its legal nihilism by its example. The UN is called to promote international cooperation, the purpose of which is to limit threats in the field of international information security and to form an international legal framework to prevent the threat of information wars; creation of an international monitoring system to track threats that appear in the information sphere; creation of a mechanism for monitoring compliance with the conditions of the international information security regime; creation of a mechanism for resolving conflict situations in the field of information security.

In the conditions of the Russian-Ukrainian conflict, the protection of the national information space from negative information and psychological influences, operations and wars, the guarantee of information security and information sovereignty acquire special importance and become factors in the preservation of the national identity of Ukraine and its functioning as a sovereign and independent state[1].

In fact, the unlimited potential of the information space is used by the world's leading states in military conflicts both to optimize the functional capabilities of their own security and defense structures, and to create new means of realizing their own geopolitical interests, including information weapons.

The information security strategy, adopted by the National Security and Defense Council of Ukraine in December 2021, defines the priorities of information security, in particular, defines the current challenges and threats to the national security of Ukraine in the information sphere. The strategy also defines strategic goals and objectives aimed at countering such threats. Russia's unprovoked full-scale invasion of Ukraine on February 24, 2022 shows that the information space is becoming a battlefield in the realities of war. The conflict is fueled by the Russian federal propaganda machine, as well as a high level of support for the brutal actions of the country's President Putin (according to various data, from 51% to 71% of Russians support the war in Ukraine)[2].

Analysis of recent research and publications. Information security, problems of protecting the national information space have been studied by many scientists. In particular, the problem is reflected in the works of U. Ilnytska, V. Pocheptsov, Yu. Lisovska, O. Oleinyk, T. Perun, V. Gurkovsky, K. Zakharenko, V. Zhogov, G. Foros, V. Trinyak, Yu. Muravska, A. Marushchak, A. Pravdiuk and other specialists.

The purpose of the article there is a study of theoretical aspects of information security, information wars, generalization of proposals for countering information wars.

Presentation of materials. The right to information is a fundamental right that ensures the comprehensive development of the individual, the full functioning of the rule of law and democracy, and the formation of civil society. In the modern world, the presence or absence of this right in a person is an indicator of the level of democracy of the state, civility of society, observance and protection of universally recognized rights and freedoms of man and citizen[3].

If the 19th century was called the century of production, the 20th – the century of management, then the 21st century, notes I. V. Aristova, is really the century of information, and information processes become the subject of conscious, purposeful and scientifically based activity. At the same time, law plays an important role in the conscious design of information processes, which not only regulates existing relationships, but also expands the sphere of information activity, which is determined by social needs. Thus, the law affects the implementation of information processes, defining and supporting those directions that form the information society[4].

The Universal Declaration of Human Rights is the main universally recognized document for the declaration of human rights, binding on all participating states as a document belonging to the jurisprudence of international law. Article 19 of the Declaration of Human Rights guarantees not only the right to freedom of expression, but also the right to access information; this provision is set out in the following version: "... Every person has the right to freedom of beliefs and their expression; this right includes the right to freedom of expression and the right to collect, receive and impart information and opinion through the media, regardless of national boundaries ".These freedoms may be limited in the cases specified in Article 29 of the General Declaration, when "it is established by law in order to ensure due recognition and respect for the rights and freedoms of others, to meet the just demands of morality, public order and general welfare in a democratic society." The International Covenant on Civil and Political Rights, ratified by Ukraine

[1] Ільницька, У. (2016) Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision, 2(1)*, 27-32.

[2] Radiosvoboda (2022). *Незалежні соціологи: 71% росіян відчуває гордість через війну з Україною* <https://www.radiosvoboda.org/a/news-sotsiology-rosiyany-viyna-gordist/31757775.html> (2022, December, 03).

[3] Holubieva, V., Pravdiuk, A., Oliinyk, S. and others (2022). Constitutional and legal provision of the right to access information in Ukraine and the countries of the European Union. *AD ALTA: Journal of Interdisciplinary Research, 12(1)*, 156-159.

[4] Арістова, І. (2011) Наука «інформаційне право» на новому етапі розвитку інформаційного суспільства. *Правова інформатика*, *1(29)*, 3-11.

in 1973, guarantees access to information similar to the Universal Declaration of Human Rights, namely: "...Everyone shall have the right to freedom of thought and expression: this right includes the freedom to collect, receive and to disseminate information and opinions of various kinds in oral, written or printed form regardless of borders..."[1].

The international legal basis for the development of the information society in Ukraine is the Okinawa Charter of the Global Information Society of 2000, the Memorandum of Understanding signed between the General Directorate for the Information Society of the European Commission and the State Committee for Communication and Informatization of Ukraine regarding the development of the information society, the Geneva Declaration "Principles building an information society" in 2003 and the Tunisian commitment "Second stage of the World Summit on Information Society" in 2005, Declaration on European policy in the field of new information technologies, adopted by the Committee of Ministers of the Council of Europe in 1999, Directive of the European Parliament "On system of electronic signatures used within the Community" 1999, UNICITRAL Model Law "On Electronic Signatures",adopted by the UN Commission in 2001, the Recommendation of the Committee of Ministers of the Council of Europe (2004) on e-government, adopted in 2014, and international agreements in the field of cooperation, for example, the Agreement between the Cabinet of Ministers of Ukraine and the Government of the Republic of Latvia on cooperation in the field of informatization[2].

The idea of ensuring international information security was first implemented in UN General Assembly Resolution A/RES/53/70 "Achievements in the field of informatization and telecommunications in the context of international security" dated December 4, 1998. This document initiated a joint discussion of the issues of creating a completely new international legal regime, the structural element of which in the future will be information, information technology and methods of its use[3].

The resolution of the UN General Assembly A/RES/54/49 "Achievements in the field of informatization and telecommunications in the context of international security" dated December 1, 1999, for the first time indicated threats to the international security of the information space in relation not only to the civil, but also to the military sphere[4].

In fulfillment of this Resolution, in 2000, the UN Secretariat presented the "Principles relating to international information security", which were published in the report of the UN Secretary General dated June 10, 2000 for their further joint discussion. The principles determine the rules of behavior of states in the information space, creating corresponding moral obligations for them, and also lay the foundation for international negotiations under the auspices of the UN and other international organizations on information security issues. For the first time, such definitions of the conceptual apparatus of the international information security system as: "information space", "information resource", "information war", "information weapon", "information security", "threat to information security", "international information security" were given[5].

Modern man, his everyday life turned out to be dependent on mass communication. The spread of network computer technologies, mobile communication and the Internet, information resources of modern society can bring not only good, but also be exposed to a growing number of threats that can harm the interests of an individual, society, state, lead to economic losses and endanger security of national information security. In this connection, the issue of society's demand for information security acquires extraordinary importance. The use of the Internet and information technologies not only opens up unlimited opportunities for humanity, but also creates new serious threats. More and more information is moving online, and according to the latest estimates, there are already more than 20 billion devices connected to the Internet in the world, which is

[1] Holubieva, V., Pravdiuk, A., Oliinyk, S. and others (2022). Constitutional and legal provision of the right to access information in Ukraine and the countries of the European Union. *AD ALTA: Journal of Interdisciplinary Research, 12(1)*, 156-159.

[2] Ромащенко, В. (2016). Правове регулювання інформаційного суспільства в Україні. *Підприємництво, господарство і право,* 9, 100-104.

[3] Undocs (1999). *Резолюция A/RES/53/70 ГА ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»* <https://undocs.org/ru/A/RES/53/70> (2022, December, 03).

[4] Undocs (1999). Резолюция A/RES/54/49 ГА ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» *Undocs* <https://undocs.org/ru/A/RES/54/49> (2022, December, 03).

[5] Фролова, О. (2018). Роль ООН в системі міжнародної інформаційної безпеки. *Електронне видання Інституту міжнародних відносин «Міжнародні відносини. Серія: Політичні науки»*, 18 <http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140>. (2022, December, 03).

several times more than the population of the Earth. Also, billions of gigabytes of various information are collected on the servers. The world is becoming open, and such rapid growth requires the formation of "rules of the game." Today, cyberspace has become a very important part of life. With its help, many social problems are solved, it has a great impact on the economy and innovative activities, etc. Because of this, cyberspace is very promising for development, as well as a prime target for attackers. Cyber attacks on information infrastructure have become a real threat, and countering these attacks is one of the main challenges for risk management[1].

A day before the military invasion, operators associated with the GRU and Russian military intelligence carried out destructive attacks on hundreds of systems of the Ukrainian government, IT sector, energy and financial organizations. The activity observed by Microsoft included attempts by attackers to destroy, disrupt, or penetrate the networks of government agencies and critical infrastructure facilities, some of which were subjected to simultaneous ground attacks and missile strikes by the Russian military. These network operations were supposed not only to impair the functions of the institutions to which they were directed, but also to prevent citizens' access to reliable information and vital services, to shake the confidence in the country's leadership[2].

Noting the generally positive role of the transition to the information society (in particular, the Okinawa Charter of the Global Information Society particularly emphasized the potential advantages of information-communication technologies that stimulate competition, contribute to the expansion of production, create and support economic growth and ensure employment of the population), which consists primarily in the transition to new principles of processing and transmission of information in order to increase the efficiency of the functioning of many spheres of activity, it is also necessary to state that the positive properties of information and information technologies can be used not only for the purposes of sustainable development of society, but also for selfish and criminal purposes. The wave of technical progress has also made significant changes in the methods of solving geopolitical, military, economic, trade and other conflicts, so force methods are currently giving way to information methods[3].

If we follow the evolution, then the history of the development of information wars is the history of the development of humanity, the history of the struggle of civilizations. There are many examples of victory and defeat in specific battles, when the situation changed dramatically thanks to some military tricks, purposeful dissemination of disinformation. Bringing information to a certain person or group of persons and receiving "profit" from it is an information operation that is an element of information warfare[4].

With the development of information technologies, the worldwide information network, such a type of warfare as information war is emerging. We are at a historical crossroads, at which the latest technologies can carry both a positive, constructive trend and a destructive one. "The industrial age brought the struggle between states to the fore, and in the 20th century – ideological and political systems. Component victories began to be formed from a complex of economic, moral-political and technological factors. The emergence of microelectronics, which opened up opportunities for mass communication, in combination with information technologies gave rise to network information structures, and with them the concept of information and network wars".[5]

Psychological influence on the opponent is an ancient mechanism of influence on the opponent. After the Second World War, such a field of international law as international humanitarian law began to develop actively. The means and methods of waging war receive legal regulation. However, the war is not always won on the battlefield, it is also won thanks to psychological and informational means. Information warfare is a type of military operations, the weapons of which are information processing equipment and methods, which allow to purposefully, quickly and covertly influence the military and civilian information systems

[1] Pravdiuk, A. (2022) The state and current issues of legal regulation of cyber security in Ukraine. *European Political and Law Discourse, 9(3)*, 19-28. DOI: 10.46340/eppd.2022.9.3.3.

[2] Бондар, Г. (2022). Кібервійна в Україні та виклики національній безпеці: кібернапади на цифрову інфраструктуру (державні установи, обєкти критичної інфраструктури та організації третього сектору). *Публічне управління та регіональний розвиток*, 30-37.

[3] *Окінавська Хартія глобального інформаційного суспільства, 2000* (Верховна Рада України). *Офіційний сайт Верховної Ради України* <http://zakon.rada.gov.ua/laws/show/998_163> (2022, December, 03).

[4] Черватюк, В., Бойко, О. (2021). Інформаційні війни (конфлікти): теоретико-правовий аспект. *Юридичний вісник, 2 (59)*, 62-69.

[5] Шумка, А. В. Черник, П. П. (2013). Інформаційно-мережева війна – нова форма міждержавного протиборства початку XXI ст. *Військово-науковий вісник, 19*, 243-255.

of the enemy with the aim of undermining his politics, economy, military capabilities, and ultimately – national security[1].

In today's context, it is worth recalling the words of Napoleon Bonaparte: "Four newspapers can do more harm than an army of a hundred thousand." The press, Napoleon believed, should write only what it is ordered to do, and keep silent about what it should not say. It is worth noting that Napoleon used the mass media not only during military campaigns, but also to consolidate and maintain power. In particular, the military operations of Napoleon's army were usually preceded by the spread of rumors about the greatly exaggerated number of Napoleon's troops, followed by the distribution of pamphlets and leaflets[2]. In turn, as J. Goebbels determined, "it is not what is written about in the newspapers that is important, but what is not written about in them." According to the materials of R. Herzenstein, one of the main methods of such propaganda was silencing. Similar approaches are widely used today, especially in the Russian mass media[3].

On June 21, 2022, D. Cohen, the chairman of Jigsaw, which is part of Google, delivered a speech at the UN Security Council meeting dedicated to Ukraine. He noted that when the Security Council was created, no one could imagine that almost 65% of the world's population would be connected by such a complex entity as the modern Internet. "For the war in Ukraine, YouTube, TikTok and other platforms have uploaded more hours of video than minutes of the conflict[4].

In turn, we believe that society itself is one of the key elements that consciously or unconsciously performs the function of transmitting information, as users in the process of militarization of networks.

But I would like to emphasize that every war, whether it is mass aggression or information war, has its own rules. The aggressor country violated all possible of them without declaring war, being wary of breaking all relations from economic to political and the rules of information warfare, turning so-called patriotism into racism in cyberspace. The propaganda of the enemy uses all kinds of expressions that spread, incite, encourage or promote racial hatred, xenophobia, anti-Semitism, or other forms of hatred that incite intolerance, that, in particular, manifests itself as warlike nationalism and ethnocentrism, discrimination and oppression of minorities, migrants and other persons of foreign origin. All this leads and has already led to tragedies in the cities of Ukraine (Bucha, Irpin, Borodyanka, Mariupol and many others).

The specifics of armed conflict, as well as the place and role of the military argument in politics, are naturally determined by the level of development of society and technology. The process of the complication of weapons and methods of warfare occurs in a wave-like manner and synchronously with the process of evolution of social organization and consciousness. Competitiveness in the era of industrial society was determined by the state's ability to produce heavy weapons, transport them to the theater of operations, and withstand economic pressure. In the information age, military competitiveness is associated with the ability to process information and integrate it into military operations, thus ensuring their success[5].

In turn, we can draw an analogy about the so-called second army of the world. In our opinion, this is nothing more than a myth and psychological intimidation of the military and the civilian population of Ukraine.

It is worth taking into account the conclusions made by N.F. Semen in the course of researching the problems of Russia's information war against Ukraine and Ukraine's opposition to such actions. The researcher notes that countering military aggression will be effective only when Ukraine creates the necessary legal basis for countering Russian propaganda. Moreover, the author believes that propaganda should be understood as the whole set of information messages from Russia, Russian media, even Ukrainian Russian-language media, which have a negative context for Ukraine. "In order to effectively resist

[1] Гриняев, С.Н.(2004). *Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны*. Москва.

[2] Макаров, В. Е., Ступин, С. А. (2015). *Политические и социальные аспекты информационной безопасности: монография.* Москва, Таганрог.

[3] Ходошко, В., Хохлачова, Ю. (2016). Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. Частина 1. *Безпека інформації*, *22(3)*, 283-288.

[4] Cohen, J. (2022). Warning incitement of racial, religious hatred can trigger atrocity crimes, Special Adviser stresses states' legal obligation to prevent genocide. Russian Federation's Disinformation Campaign Aimed to Justify Invasion of Ukraine, Several Speakers Stress. Security Council. June 21, 2022. *Reliefweb.int.* <https://reliefweb.int/report/ukraine/warning-incitement-racial-religious-hatred-can-trigger-atrocity-crimes-special-adviser-stresses-states-legal-obligation-prevent-genocide> (2022, December, 03).

[5] Магда, Є. (2014). Гібридна війна: сутність та структура феномену. *Міжнародні відносини Серія "Політичні науки"*, *4* < http://jurnals.iir.riev.ua/index.php/pol_n/article/wiev/2489>. (2022, December, 03).

the information war and respond adequately to the Russian side, it is necessary to clearly understand that the format of the information war has long gone beyond the scope of violence"[1].

In turn, we can note that the improvement of legal norms will not be able to counteract information aggression, because the information vacuum formed over years and decades, starting from the times of the Soviet Union until now, when information was provided in a limited and, in most cases, fictitious manner, the population of the country perceived any information as reliable. , and such that it is not amenable to criticism or, much less, analysis.

The war in Ukraine is the largest military conflict since the end of the Second World War, but it is also the first war in detail, every soldier and civilian has the opportunity to record on any gadget the everyday life or even every second of the war. Each video will forever remain on the Internet, each war criminal will not be able to escape punishment and will be brought to justice in accordance with the norms of international law. We understand that it is necessary to record war crimes, but the military insists that posting pictures on the Internet of the movement of military units, their location or damaged infrastructure in real time can lead to the loss of an entire unit or to a repeated missile attack on the infrastructure. Unfortunately, regardless of criminal liability, certain citizens.

The theater of information warfare is comprehensive: from the office to the home personal computer. The means of conducting such a war are any means of information transmission that allow purposefully changing (destroying, distorting), copying, blocking information, neutralizing protection systems, limiting access, disinforming, disrupting the functioning of information carriers, disorganizing the operation of technical means, computer systems and information and computing networks of the enemy. Methods of influence determine the peculiarities of the spheres in which the information struggle is conducted. Therefore, the risk of disorganization of society due to artificially created information-organized controlled chaos, due to an excess or deficit of information, misinformation, and, as a result, the general controllability of large social groups is quite achievable[2].

False information is the basis of such a war. Quite often, under the guise of a great goal – patriotism, the protection of indigenous peoples, the protection of human rights and freedoms, the fight against terrorism, etc., military aggression takes place, that is, an undeclared armed conflict, which causes not only the seizure of territories, but also significant human casualties[3].

The term "information war" appeared in the mid-1970s. It was proposed by physicist Thomas Rohn, who was not only the first to understand, but also scientifically substantiated the fact that information is the weakest link in any army[4]. According to the definition of Professor B. Yuskiv, information warfare or "informational and psychological influence is the purposeful production and distribution of special information that directly affects the functioning of the informational and psychological environment of society"[5].

Modern scientists point out that information war (from the English information war) is a term that has two meanings: first, influence on the civilian population and/or military personnel of another state through the dissemination of certain information[6]. Today there are many definitions of information warfare. The definition of information warfare can be found in the works of M. Libiki, in particular, in which the author identified seven types of information warfare: command-and-control, hacking, economic, psychological, intelligence, electronic and cyber warfare. M. Libiki, in turn, noted that attempts to fully understand all aspects of the concept of information war are similar to the efforts of blind people to learn about the world around them[7].

Ensuring the information security of Ukraine and the security of state interests in the information space will be facilitated by the priority development of an appropriate regulatory system for countering threats

[1] Семен, Н.(2018). Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.Ру» та «Российский диалог»): *автореферат дисертації на здобуття наукового ступеня кандидата наук з соціальної комунікації.* Дніпро: Дніпровський національний університет імені Олеся Гончара.

[2] Баглікова, М.(2010). Інформаційні війни і Україна. *Науковий вісник Ужгородського університету: Серія: Політологія. Соціологія. Філософія*, *14*, 158-161.

[3] Жаровська, І., Ортинська, Н. (2020). Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки*", *7(2)*, 56-61.

[4] Короход, Я. (2013). Інформаційно-психологічні війни – зброя XXI. *Актуальні проблеми політики*, *50*, 299-307.

[5] Юськів, Б.(2003). *Опорний конспект лекцій з дисципліни "Інформаційні війни"*. Рівне: РІС КСУ.

[6] Манойло, А.(2003). Информационно-психологическая война как средство достижения политических целей. *Azerilove* <http://www.azerilove.net/ articles/85/1/> (2022, December, 03).

[7] Libicki, M. (2007). *Conquest in cyberspace. National security and information warfare*. Cambridge.

to these interests and streamlining the law-making process in the field of analysis, generalization, use and dissemination of information[1].

The need for such development of the system of regulatory and legal support is determined by certain factors. First, in the conditions of the functioning of the legal state and civil society, the main functions of state authorities, which are entrusted with the main responsibility for national security, should be regulated by certain legal norms aimed at ensuring civil constitutional rights and freedoms. Law-making in this context is aimed at the normative consolidation of the tasks of countering threats to the national security of Ukraine, the means and methods of their implementation, ensuring the conciliatory policy of the authorities. Secondly, Ukraine's course towards integration into the international community significantly expands the possibilities of consolidating the conceptual foundations of state information security by participating in the development of international legal norms in this area, formation of an international system for ensuring information security on a global scale and within the framework of each individual country. Thirdly, the implementation of guarantees of civil rights and freedoms, protection of state interests of our country involves a significant increase in the role of authorities in regulating relevant social relations, the presence of a transparent and understandable state policy[2].

The peculiarities of the state's implementation of information security functions are that the activities of each state body are carried out by using the information infrastructure of society, forming and consuming information resources, and establishing relations with citizens. In view of this, state bodies as the owners of such resources and representatives of the relevant infrastructure must apply a range of measures aimed at ensuring the preservation of resources and the security of information, telecommunications, management and communication systems[3].

However, the reality is the opposite. As O. Belorus ironically observes, researching globalization and the national strategy of Ukraine: "Our legislative field is exemplary, thanks to it, anyone can work in the information field as they wish. We actually lost informational sovereignty, because we have only 10% of the state share, while France, Poland, Germany have up to 40%, and some of our neighbors have 60%. They each have 3-5 state radio channels, 2-3 TV channels, and in our country, especially in cable networks, another state actually sits”[4]. However, as is known, the problem of ensuring information security as an integral component of the general national system of state security and protection of the fundamentals of the constitutional order must be directly resolved by state structures whose duties include ensuring, observing and protecting the Constitution of Ukraine. Of course, this is logical, because from a state-legal point of view, the protection of the Constitution and ensuring the stability of the constitutional system of Ukraine should occupy a special place in the national security system. It is no accident that Prof. Yu. M. Todyka considered the indicated problem as a complex political and legal one, which acquires special importance in the period of the formation of statehood, economic, political and social instability, the formation of the legal system of the state on a conceptually new basis[5].

In every information war, there is a subject, that is, the one or those who control the information flows. The subjects of activity in the information space of society implementing the state information policy include:

1) bodies of state power and management that have stable interests in the information space; form and control the national information space; create structural units whose functions and tasks include conducting information warfare;

2) international organizations that have stable interests in the information space and participate in the formation of the information space; use national structures integrated into international organizations; create their own scientific and technical potential and use the potential of countries;

3) non-governmental organizations that have interests in the information space; create their own segment of the information space; create units within their structures whose functions and tasks include information warfare; create and use their own scientific and technical potential and use the potential of allies,

[1] Черниш, Р., Ігнатюк, М, Заріцький, Ю. (2022). Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти. *Юридичний науковий електронний журнал*, *1*, 213-216.

[2] Почепцов, Г. (2015). *Сучасні інформаційні війни.* Київ: ВД Києво-Могилянська академія.

[3] Політанський, В.С. (2017). Світові моделі та фундаментальні принципи інформаційного суспільства. *Науковий вісник Ужгородського національного університету. Серія «Право», 43(1),* 34-39.

[4] Мануйлов, Є.М., Калиновський, Ю.Ю.(2016). Роль і місце інформаційної безпеки у розбудові сучасної української держави. *Вісник Національного юридичного університету «Юридична академія імені Ярослава Мудрого», Серія: Політологія*, *2 (29)*,144-153.

[5] Дзьобаня, О.П. (ред.) (2021). *Національна безпека: світоглядні та теоретико-методологічні засади: монографія*. Харків: Право.

as well as supporting countries, which in one way or another are related to the activities of this subject; develop and consolidate certain values and ideals at the level of their official ideology;

4) media corporations, the main function of which is the dissemination of knowledge, ideas and values, the formation of certain views, ideas and emotional states of people and, through them, influencing their behavior[1].

Undoubtedly, the state, even if it uses the experience of foreign countries, will not be able to cope with the information influx of the enemy on its own, in our opinion, this is possible only if the government, business, army, society, self-government and religious organizations consolidate.

Formation of public consciousness with the help of subjects of information war using methods of psychological influence becomes the most effective way of control and manipulation both inside the state and outside it. It all depends on who actually determines the information content. Thus, our attitude to problems and phenomena, even the very approach to what is considered a problem or phenomenon, is largely determined by those who control the world of communications[2].

Media researcher J. Bryce published a book in which he revealed the mechanisms of influence on public opinion.

First, a "plurality of opinion" is constructed with the help of "facts or stories" in order to disrupt the feeling in the human soul, which flows out of the mouth by itself, creating the impression that everyone is talking about the chosen fact.

At the second stage, newspapers (morning and evening) express a more certain opinion about the events, providing it with "expected results" and, thus, "the opinions of ordinary citizens begin to condense into a solid mass".

At the third stage – in debates and discussions – unnecessary arguments are rejected in favor of one definite and unchanging decision.

The fourth stage is the introduction of a fact or an assessment of an event, which is passed off as a "conviction that has developed" in the form of "the tendency of people to "unanimity"" in the interests of ordinary citizens.

The whole process of processing public opinion was compared to the action of a roller on a road, when "clumsiness is suppressed, and the road becomes smooth and even takes on a uniform appearance"[3].

The goal of information warfare is to influence the decisions of an adversary or competitor, and as a result, his behavior in such a way that he does not know that he is being influenced[4]. Such informational influences are able to fully or partially cause destabilization processes in the information space of sovereign states, provoke unrest and internal confrontation.

The variety of possible tools leads to the fact that the aggressor state surrounds the enemy with a swarm of seemingly unrelated actions: provocations, disinformation, diplomatic demarches, actions of various foundations, committees, authoritative leaders, movements, TV channels, Internet sites, etc. But in reality, these actions are well coordinated among themselves based on a single strategic concept. This not only increases the power of influences due to coordination, but also contributes to ensuring their suddenness and the complexity of countermeasures, since only an intellectually well-prepared state elite can resist complex systemic influences from all sides[5].

The most dangerous manifestations of such influences can be informational influences, the object of which is a direct attack on the constitutional system and the rights and freedoms of a person and a citizen, since one of the main tasks of the state in the information sphere is to observe the constitutional rights and freedoms of a person and a citizen when receiving information and using it, preserving and strengthening the moral values of society[6].

[1] Богуш, В., Юдін, О. (2005). *Інформаційна безпека держави*. Київ: МК-Прес.

[2] Brzhevska, Z., Dovzhenko, N., Kyrychok, R.and others (2019). Інформаційні війни, загрози та протидія. *Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка&quot, 3(3)*,. 88-96. DOI: https://doi.org/10.28925/2663-4023.2019.3.8896.

[3] Ходошко, В., Хохлачова, Ю. (2016). Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. Частина 1. *Безпека інформації, 22 (3)*, 283-288.

[4] Szafranski, R. (2020). A theory of information warfare. Preparing for 2020. *Cryptome* <https://cryptome.org/jya/af-infowar.htm> (2022, December, 03).

[5] Бочарніков, В., Свєшніков, С. (2017). Погляди на характер сучасних воєнних конфліктів. *Наука і оборона*, *1*, 3-8. DOI: https://doi.org/10.33099/2618-1614-2017-0-1-3-8.

[6] Савин, Л. (2011). *Сетецентричная и сетевая война. Введение в концепцию.* Москва: Евразийское движение.

In our opinion, the information policy of Ukraine needs to be adapted to new conditions, to act in advance and continuously monitor the impact on the domestic media market. In turn, the concept of information war involves the use of information weapons by conducting information operations, they can be of both an information-technical and information-psychological nature, covering all directions of information conflict, it is also necessary to state the fact that modern international law does not determine the relationship between cross-border the nature of information networks and the principle of state sovereignty.

Most of the countries of the world have a clear understanding that information security is an integral component of national security, which necessitates the development and improvement of national legislation, the creation of appropriate specialized structures, the main task of which is to ensure the information security of the state. Today's realities have shown that only joint and well-coordinated actions give the opportunity to oppose the military and information war on the part of the Russian Federation and its satellites. The society must understand that this is our joint responsibility – both the state, media and civil society.

In conflicts where the decisive action may be the opening of a virus-infected e-mail, the retweeting of a message from a software agent mistaken for a human, or the invisible contribution of a hijacked computer (or digitized refrigerator) to a large botnet, we are in the realm of Marx's "they do it, but they do not know it.' "Even if you don't see the war, the war sees you" is the logic of the blind gaze of cyber war, a regime in which, although "the subject does not see where this regime leads, he follows it"[1].

Conclusions. Information protection or, better said, ensuring security is no longer just a technological problem. Issues related to information, its protection, information security and confidentiality become one of the measures to protect state sovereignty. Information has become the most important asset needed by a person, the state and society in general. Ensuring information security and protection of information sovereignty, forming one's own protected information space is one of the main tasks of the country.

In order to solve these problems in a timely manner, Ukraine still has a lot to do in terms of legal, organizational, and organizational and technical aspects. In particular, in order to protect the information space, it is necessary to create systems for managing national information resources, reliable protection of state administration channels, and countering information threats. In the conditions of war, the problem of guaranteeing information security due to the spread of cyber threats of various types becomes a matter of state security, a matter of every citizen and society as a whole, therefore it is a strategic problem of the state, which requires the creation of a comprehensive system for ensuring cyber security and information sovereignty, establishing strategic communications of national subjects cyber security systems, building capabilities to counter cyber threats, formation of the appropriate infrastructure of the domestic information space.

The legislator is obliged to carry out a policy of anticipation and to immediately respond to dynamic changes occurring in cyberspace, to develop and implement effective means and tools for a possible response to aggression in cyberspace, which can be used as a means of deterring military conflicts and threats in cyberspace. In our opinion, the adoption of the law on media, which received generally positive conclusions from the European Commission, was an important step to ensure information security. There are quite a lot of comments, but the media norms are clearly outdated and do not fully meet the requirements of modern times.

References:

1. Aristova, I. (2011). Nauka «informatsiine pravo» na novomu etapi rozvytku informatsiinoho suspilstva [The science of "information law" at a new stage of development of the information society]. *Pravova informatyka* [Legal informatics], *1(29)*, 3-11. [in Ukrainian].
2. Bahlikova, M. (2010) Informatsiini viiny i Ukraina. [Information wars and Ukraine]. *Naukovyi visnyk Uzhhorodskoho universytetu: Seriia: Politolohiia. Sotsiolohiia. Filosofiia* [Scientific Bulletin of Uzhhorod University: Series: Political Science. Sociology. Philosophy], *14*, 158-161. [in Ukrainian].
3. Bocharnikov, V., Svieshnikov, S. (2017). Pohliady na kharakter suchasnykh voiennykh konfliktiv [Views on the nature of modern military conflicts]. *Nauka i oborona* [Science and defense], *1*, 3-8 [in Ukrainian].
4. Bohush, V., Yudin, O. (2005). Informatsiina bezpeka derzhavy [State information security]. Kyiv: MK-Pres. [in Ukrainian].
5. Bondar, H. (2022). Kiberviina v Ukraini ta vyklyky natsionalnii bezpetsi: kibernapady na tsyfrovu infrastrukturu (derzhavni ustanovy, obiekty krytychnoi infrastruktury ta orhanizatsii tretoho sektoru) [Cyber warfare in Ukraine and challenges to national security: cyber attacks on digital infrastructure (state institutions, critical infrastructure

[1] Dyer-Witheford, N., Matvienko, S. (2019). *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism.* Minneapolis-London: University of Minnesota Press.

objects and third sector organizations)]. *Publichne upravlinnia ta rehionalnyi rozvytok* [Public administration and regional development], *15*, 30-67. [in Ukrainian].

6. Brzhevska, Z., Dovzhenko, N., Kyrychok, R.and others (2019). Informatsiini viiny, zahrozy ta protydiia. [Information wars, threats and countermeasures]. *Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika&quot* [Electronic professional scientific publication "Cybersecurity: education, science, technology"], *3(3)*, 88-96. [in Ukrainian].
7. Chernysh, R., Ihnatiuk, M, Zaritskyi, Yu (2022). Protydiia destruktyvnomu informatsiinomu vplyvu v Ukraini: pravovi ta orhanizatsiini aspekty [Countering destructive information influence in Ukraine: legal and organizational aspects]. *Yurydychnyi naukovyi elektronnyi zhurnal* [Legal scientific electronic journal], *1*, 213-216. [in Ukrainian].
8. Chervatiuk, V., Boiko, O. (2021). Informatsiini viiny (konflikty): teoretyko-pravovyi aspekt [Information wars (conflicts): theoretical and legal aspect]. *Yurydychnyi visnyk* [Legal Bulletin], *2(59)*, 62-69. [in Ukrainian].
9. Cohen, J. (2022). Warning incitement of racial, religious hatred can trigger atrocity crimes, Special Adviser stresses states' legal obligation to prevent genocide. Russian Federation's Disinformation Campaign Aimed to Justify Invasion of Ukraine, Several Speakers Stress. Security Council. June 21, 2022. *Reliefweb* <https://reliefweb.int/report/ukraine/warning-incitement-racial-religious-hatred-can-trigger-atrocity-crimes-special-adviser-stresses-states-legal-obligation-prevent-genocide > (2022, December, 03).
10. Dyer-Witheford, N, Matvienko, S. (2019). *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism.* Minneapolis-London: University of Minnesota Press.
11. Frolova, O. (2018). Rol OON v systemi mizhnarodnoi informatsiinoi bezpeky [The role of the UN in the system of international information security]. *Elektronne vydannia Instytutu mizhnarodnykh vidnosyn «Mizhnarodni vidnosyny. Seriia: Polytychni nauky»* [Electronic edition of the Institute of International Relations "International relations. Series: Political science"] <http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140> (2022, December, 03). [in Ukrainian].
12. Grinjaev, S.N. (2004). *Pole bitvy – kiberprostranstvo. Teorija, priemy, sredstva, metody i sistemy vedenija informacionnoj vojny* [The battlefield is cyberspace. Theory, techniques, means, methods and systems of information warfare]. Moscow. [in Russian].
13. Holubieva, V., Pravdiuk, A., Oliinyk, S. and others (2022). Constitutional and legal provision of the right to access information in Ukraine and the countries of the European Union. *AD ALTA: Journal of Interdisciplinary Research, 12(1)*, 156-159.
14. Ilnytska, U. (2016). Informatsiina bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnym informatsiino-psykholohichnym vplyvam [Information security of Ukraine: modern challenges, threats and countermeasures against negative informational and psychological influences] *Humanitarni viziii* [Humanitarian vision], *2(1)*, 27-32. [in Ukrainian].
15. Khodoshko, V., Khokhlachova, Yu (2016). Informatsiina viina. ZMI yak instrument informatsiinoho vplyvu na suspilstvo. Chastyna 1 [Information war. Mass media as a tool of information influence on society. Part 1.] *Bezpeka informatsii* [Information security], *22(3)*, 283-288. [in Ukrainian].
16. Korokhod, Ya. (2013). Informatsiino-psykholohichni viiny – zbroia XXI [Informational and psychological warfare is a weapon of the 21st century.] *Aktualni problemy polityky* [Actual problems of politics], *50*, 299-307. [in Ukrainian].
17. Libicki, M. (2007). *Conquest in cyberspace. National security and information warfare.* Cambridge.
18. Mahda, Ye. (2014). Hibrydna viina: sutnist ta struktura fenomenu [Hybrid war: the essence and structure of the phenomenon]. *Mizhnarodni vidnosyny Seriia "Politychni nauky"* [International relations Series "Political sciences], *4* <http://journals.iir.kiev.ua/index.php/pol_n/article/view/2489/2220> (2022, December, 03). [in Ukrainian].
19. Makarov, V. E., Stupin, S. A. (2015). *Politicheskie i social'nye aspekty informacionnoj bezopasnosti: monografija*. [Political and social aspects of information security: monograph]. Moscow: Taganrog. [in Russian].
20. Manojlo, A. (2003). Informacionno-psihologicheskaja vojna kak sredstvo dostizhenija politicheskih celej [Information and psychological warfare as a means of achieving political goals]. *Azerilove* <http://www.azerilove.net/ articles/85/1/> (2022, December, 03). [in Russian].
21. Manuilov, Ye, Kalynovskyi, Yu.Iu. (2016). Rol i mistse informatsiinoi bezpeky u rozbudovi suchasnoi ukrainskoi derzhavy [The role and place of information security in the development of the modern Ukrainian state]. *Visnyk Natsionalnoho yurydychnoho universytetu «Iurydychna akademiia imeni Yaroslava Mudroho», Seriia: Politolohiia* [Bulletin of the Yaroslav the Wise National Law University, Series: Political Science], *2(29)*, 144-153. [in Ukrainian].
22. Dzobania, O.P.(ed.) (2021). *Natsionalna bezpeka: svitohliadni ta teoretyko-metodolohichni zasady: monohrafiia* [National security: worldview and theoretical and methodological foundations: monograph]. Kharkiv: Pravo. [in Ukrainian].
23. Okinavska Khartiia hlobalnoho informatsiinoho suspilstva, 2000 (Verkhovna Rada Ukrayiny). [Okinawan Charter of the Global Information Society, 2000] (Verkhovna Rada of Ukraine)]. *Ofitsiynyy sayt Verkhovnoyi Rady Ukrayiny* [Official site of the Verkhovna Rada of Ukraine] < http://zakon.rada.gov.ua/laws/show/998_163> (2022, December, 03). [in Ukrainian].

24. Pocheptsov, H. (2015). *Suchasni informatsiini viiny* [Modern information wars]. Kyiv: VD Kyievo-Mohylianska akademiia. [in Ukrainian].
25. Politanskyi, V.S. (2017). Svitovi modeli ta fundamentalni pryntsypy informatsiinoho suspilstva. [World models and fundamental principles of the information society]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia «Pravo»* [Scientific Bulletin of the Uzhhorod National University. Law series], *43(1)*, 34-39. [in Ukrainian].
26. Pravdiuk, A. (2022). The state and current issues of legal regulation of cyber security in Ukraine. *European Political and Law Discourse, 9(3)*, 19-28. DOI: 10.46340/eppd.2022.9.3.3.
27. Radiosvoboda [Radio Freedom] (2022). *Nezalezhni sotsiolohy: 71% rosiyan vidchuvaye hordist' cherez viynu z Ukrayinoyu* [Independent sociologists: 71% of Russians feel proud because of the war with Ukraine] <https://www.radiosvoboda.org/a/news-sotsiology-rosiyany-viyna-gordist/31757775.html> (2022, December, 03) [in Ukrainian].
28. *Rezoljucija A/RES/53/70 GA OON Dostizhenija v sfere informatizacii i telekommunikacii v kontekste mezhdunarodnoj bezopasnosti, 1999* (Organizatsiya Obyedinennykh Natsiy) [Resolution A/RES/53/70 UNGA Advances in the field of informatization and telecommunications in the context of international security (United Nations)]. *Undocs* <https://undocs.org/ru/A/RES/53/70> (2022, December, 03). [in Russian].
29. *Rezoljucija A/RES/54/49 GA OON Dostizhenija v sfere informatizacii i telekommunikacii v kontekste mezhdunarodnoj bezopasnosti, 1999* (Organizatsiya Obyedinennykh Natsiy) [Resolution A/RES/54/49 UNGA Advances in the field of informatization and telecommunications in the context of international security (United Nations)] *Undocs* <https://undocs.org/ru/A/RES/54/49> (2022, December, 03). [in Russian].
30. Romashchenko, V. (2016). Pravove rehuliuvannia informatsiinoho suspilstva v Ukraini [Legal regulation of the information society in Ukraine]. *Pidpryiemnytstvo, hospodarstvo i pravo* [Entrepreneurship, economy and law], *9*, 100-104. [in Ukrainian].
31. Savin, L. (2011). *Setecentrichnaja i setevaja vojna. Vvedenie v koncepciju* [Network-centric and network warfare. Introduction to the concept]. Moscow: Evrazijskoe dvizhenie. [in Russian].
32. Semen, N. (2018). Rosiiski internet-resursy yak chynnyk informatsiinoi viiny proty Ukrainy (na prykladi saitiv «Pravda.Ru» ta «Rossyiskyi dyaloh») [Russian Internet resources as a factor in the information war against Ukraine (on the example of the websites "Pravda.Ru" and "Russian Dialogue")]: *avtoreferat dysertatsiyi na zdobuttya naukovoho stupenya kandydata nauk z sotsial'noyi komunikatsiyi* [thesis abstract for obtaining the scientific degree of candidate of sciences in social communication]. Dnipro: Dniprovskyi natsionalnyi universytet imeni Olesia Honchara. [in Ukrainian].
33. Shumka, A. V. Chernyk, P. P. (2013). Informatsiino-merezheva viina – nova forma mizhderzhavnoho protyborstva pochatku XXI cт st [Information and network warfare is a new form of interstate confrontation at the beginning of the 21st century]. *Viiskovo-naukovyi visnyk* [Military-scientific bulletin], *19*, 243-255. [in Ukrainian].
34. Szafranski, R. (2020). A theory of information warfare. Preparing for 2020. *Cryptome* <https://cryptome.org/jya/af-infowar.htm> (2022, December, 03).
35. Yuskiv, B. (2003). Opornyi konspekt lektsii z dystsypliny “Informatsiini viiny” [Reference synopsis of lectures on the discipline "Information Wars"]. Rivne: RIS KSU. [in Ukrainian].
36. Zharovska, I., Ortynska, N. (2020). Informatsiina viina yak suchasne hlobalizatsiine yavyshche [Information warfare as a modern globalization phenomenon]. *Visnyk Natsionalnoho universytetu “Lvivska politekhnika”. Seriia: “Iurydychni nauky”* [Bulletin of the Lviv Polytechnic National University. Series: "Legal Sciences"], *7(2)*, 56-61. [in Ukrainian].