

FUNDAMENTALS OF THE THEORY OF INFORMATION WAR

Pronoza I. I.

INTRODUCTION

In today's global context of integration and fierce international competition, the information space is central to the collision and struggle of diverse national interests.

New information technologies make it possible to achieve the realization and functioning of state interests without the use of military methods, to weaken, weaken or even destroy a competing state, without using forceful means, only under conditions, without awareness of the real and potential threats of negative information influences and formation of this country and the proper functioning of an effective defense and response system to these challenges and threats.

Concepts such as: information society, information infrastructure, information space, and information resources – sufficiently define a certain state, level and course of socio-political, socio-economic, scientific and technical and cultural course of the state¹.

The information society also gave birth to its wars - information wars. All previous wars considered had a completely different character. The new concept of information warfare involves replacing the principle of mass destruction with the principle of neutralizing the enemy's army by destroying (isolating, falsifying) critical information, rather than simply by improving the method of warfare.

In the conditions of formation of information society, development and domination of information technologies, the term "information war" not only became a symbolic unit of journalistic and political vocabulary, but also began to be actively used as an independent category in the scientific discourse.

The modern 21st century is increasingly called the "information technology era", in which there is a tremendous contribution to the

¹ Проноза І. І. Інформаційна безпека держави: сутність та основні визначення. *Гілея: науковий вісник. Збірник наукових праць*. 2017. № 127(12). С. 345–349.

development of methods of warfare, as well as the fight against information warfare, in which information security has become almost a panacea for solving problems of the information society. The definition of a modern information society is equivalent to the concept of "post-industrial society", given the increasing political, social and military importance of information confrontation of states, as well as the huge investment in research centers. And a number of post-industrial states attach tremendous importance to the development of their country's science, technology and information security, being well aware of the importance of the impact of the media on the mass consciousness, both regionally and internationally².

Information warfare now pervades all forms of struggle, ranging from diplomatic and economic to armed struggle, developing as an independent sphere of activity. The rapid development of information technology has led to the shifting of conflicts from the traditional physical space into a fundamentally different one - cyberspace. Today, everyday political practices provide many examples of waging a wide variety of information wars, both in democratic states and in transitional political systems.

Ukraine is facing the threat of large-scale actions of the information war, which are aimed at its information resources, the system of decision-making by public authorities, as well as the mass consciousness of the population. Thus, recently the amount of negative information about Ukraine has increased significantly in the world information space. This information is not random but purposeful, created and provided in a specific scenario. The purpose of such information is to manipulate public opinion of Ukrainians.

A characteristic feature of the Ukrainian information space was the presence of internal political wars: information wars between oligarchs, between the authorities and the opposition, as well as staged confrontations between different segments of government.

Thus, the study of the essence of information wars, both external and internal, their basic methods, means, patterns becomes one of the most relevant areas of

² Аюрова А. М. Информационная война как феномен информационного общества. *Экспериментальные и теоретические исследования в современной науке* : сб. ст. по матер. II междунар. науч.-практ. конф. № 2(2). Новосибирск, 2017. С. 67–76.

scientific research of domestic political science, as it is necessary to effectively counteract the threats to the information and psychological security of the individual, society and state and ensuring the security of Ukraine as a whole.

Among the scientists involved in the study of information wars we can distinguish the following: D. Volkogonov, S. Grinyayev, O. Kolinovsky, A. Krutskikh, A. Fedorov, M. Pavlyutenkova, V. Petrov, I. Rabinovich, I. Sharavov, D. Feldman, G. Pocheptsov, G. Karpenko, V. Lipkan, V. Ostroukhov and others. However, they explored only certain aspects of information wars.

1. Theoretical analysis of the definition of "information war"

The essence and role of information warfare is devoted to a large number of publications in which it is interpreted in different ways.

Prominent researchers Zinoviev AA, Dugin AG, Korovin VM say that a new global war is already underway. It is not officially announced and is hidden from the eyes of ordinary citizens, but it is leading humanity to profound changes in the deployment of forces on the world stage. The phenomenon of the described hidden war became possible only in the conditions of development of modern information and communication technologies. The analysis of world experience shows that today direct aggression has ceased to be the only means of domination. In this regard, modern science is gradually focusing on the study of indirect forms of confrontation, with particular attention to information wars.

The term "information war" itself is now more non-fiction and has not yet been recognized. Continuous discussions about what is really covered by this concept, as well as disputes about the correctness and practical applicability of this term to the sphere of social relations, which is called information conflict or conflict of interest in the information sphere of social systems, testify to this. Thus, a separate scientific problem is the development and coordination of scientific and terminological apparatus³.

In domestic and foreign science there are many different and often mutually exclusive approaches to identifying conflicts that take place in

³ Проноза І. І. Інформаційна війна: сутність та особливості прояву. *Актуальні проблеми політики. Збірник наукових праць*. 2018. № 81. С. 79.

the modern information space. Such diversity and inconsistency is a serious obstacle to the development of information war theory.

It is appropriate to analyze the definitions of the information war contained in the papers of foreign experts as well as in official documents. They can be grouped as follows: definitions of information warfare in a narrow sense, ie those that reflect a purely military orientation, and definitions in a broad sense, which reflect a focus on securing national interests in any vital sphere of state and public activity.

Information wars as a phenomenon have existed in one way or another since ancient times. Execution of information influences with the use of information weapons (concealment of information; its submission in part, in some perspective; exaggeration of the consequences) was recorded by chroniclers in the territory of Ukraine in Kievan Rus⁴.

For the first time the term "information warfare" was used by T. Ron in a report "Weapons Systems and the Information Warfare" prepared by him in 1976. He emphasized that information infrastructure is a key aspect of the US economy, and at the same time it is becoming a vulnerable target. in wartime and in peacetime.

According to Panarin I. N. the point of reference should be taken not in 1976⁵, but in 1967, when A. Dulles (the main organizer of the information war against the Soviet Union) published a book called "The Secret Capitulation", devoted to secret separate negotiations between the United States and Great Britain, on the one hand, and the Reichsführer of the SS. Himmler – on the other. It was first introduced the term "information war", which represents personal, intelligence, sabotage actions to undermine the rear of the enemy⁶. Later, the term became actively mentioned in the press, especially after the operation "Operation Desert Storm" in 1991.

Today, the concept of "information war" is defined differently. This is due to the ambiguity of the term "information warfare", which gave rise to many differences in its translations. This concept can be interpreted as "information war", "information confrontation", "information and psychological war". In particular, information warfare is characterized as

⁴ Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу : навчальний посібник. К, 2007. С. 18.

⁵ Гриняев С. Концепция ведения информационной войны в некоторых странах мира. URL: http://www.soldiering.ru/psychology/conception_psywar.php

⁶ Панарин И. Н. Информационная война и третий Рим. М, 2001. 244 с.

information activity undertaken by political education (such as the state) to weaken or destroy other political entities; as an information fight between competitors; an information military conflict between two massive enemies, such as armies, etc⁷.

Information warfare is a total phenomenon where it is impossible to determine its beginning and end. In particular, according to S. Rastorguev⁸, information warfare is the existence of struggle between states with the help of information weapons, that is, open and hidden purposeful informational influences of systems (states) on each other, in order to gain advantage in the material sphere, where informational influences are influences by such means, the use of which allows to achieve the intended goals.

The results of the theoretical analysis make it possible to state that there are many argumentative concepts of information war and there is no generally accepted definition of this concept. This diversity of approaches is due, first of all, to the complexity of the object of study itself, as well as to the theoretical and methodological positions of the authors belonging to different scientific schools. This determines their focus on certain aspects of the issue.

Thus, within the psychological paradigm, information war is understood as the latent influence of information on the individual, group and mass consciousness through the methods of propaganda, misinformation, manipulation in order to form new views on the socio-political organization of society through the change of value orientations and basic attitudes.

Exploring the information war in the context of psychological theories, V. A. Lisichkin and L. A. Shelepin indicate that its object is the cognitive-emotional sphere of individuals, and the main goal is the management of intellectual-psychological and socio-cultural processes, which is a necessary element of which there is a lack of awareness of this influence by those who are prone to veiled influence and the following lines of programmed behavior⁹.

⁷ Маноило А. В. Государственная информационная политика в особых условиях. М, 2013. С. 239.

⁸ Расторгуев С. П. Философия информационной войны. М, 2003. С. 455–456.

⁹ Лисичкин В. А. Третья мировая (информационно-психологическая) война. URL: <http://malchish.org/lib/politics/infwar.htm>

In his turn, V. Karpenko¹⁰, exploring the information space of the Ukrainian state, highlights information expansion of Russia, which, in order to spread neo-imperialist ideas, presents forms of Russian expansion in the information space of Ukraine, using Ukrainian mass media for its purposes.

The geopolitical approach is also noteworthy. According to the provisions of the geopolitical approach, information war is interpreted in the concepts of inter-state confrontation, aimed at solving foreign policy goals, not with the help of physical force, military equipment and weapons, but with the use of sophisticated technologies of coercive control, which has an external expression in the form of diplomacy.

An interesting refinement is the study of the information war I. A. Mikhalchenko in the context of modern geopolitical processes. The researcher defends the position according to which information war is defined as a holistic technology aimed at achieving humanitarian enslavement of one group of people by others. It is a product of post-industrial society and is conditioned by the impossibility of global armed conflicts that can destroy the planet¹¹.

An advocate of such thinking is I. N. Panarin. According to the definition of political scientist, information warfare is "the dominant way of achieving power, the organization of the neosphere and the world of information and psychological space in their interests"¹². In his view, modern statesmen must not only have and possess a

powerful resource and credit of public trust, but also be able to wage effective information confrontation. It is this that enables successful politicians to increase their political capital.

In modern scientific research the circle of scientists who focus their attention on the social-communicative aspect of information wars is distinguished. Their methodological principles of study differ in that the subject field is dominated by information, which becomes dominant in the sms of reality and forms cognitive orientations, not consciousness of people.

¹⁰ Карпенко В. Інформаційний простір як чинник національної безпеки України. *Українознавство*. 2005. № 3. С. 182.

¹¹ Михальченко И. А. Информационные войны на рубеже XXI века. *Безопасность информационных технологий*. 1998. № 3. С. 14–15.

¹² Панарин И. Н. Информационная война и третий Рим. М, 2001. 244 с.

It is of interest to study the problem of P. Spyga and R. Rudnik¹³, where scientists identify 4 approaches to the definition of this concept:

- the first approach treats them as a set of political-legal, socio-economic, psychological actions that involve the seizure of information space, the displacement of the enemy from the information sphere, the destruction of his communications, the deprivation of means of communication, and other similar purposes;

- in the second approach, information warfare is the most acute form of confrontation in the information space, where the qualities of interaction such as uncompromising, high intensity of dispute and short duration of intense rivalry are of paramount importance;

- in the third approach, information warfare is interpreted as a form of providing and conducting military forces through modern electronic means (digital transmitters, satellite transmitters and other similar means used for military tasks);

- the fourth approach identifies information wars with cyber wars (confrontation between technical systems).

The ideas of a conflicting approach cannot be overlooked; it allows us to consider the wars analyzed in the context of military and political confrontation.

Accordingly, R. Shafransky interprets the phenomenon under study as armed action against any part of the system of knowledge and beliefs of the enemy, with the purpose of hidden destructive influence on political decisions of the counterparty, which is expressed in violation of coordination and efficiency of this process.

The author emphasizes that the higher the technological capabilities and the more developed the communicative sphere of the state, the more vulnerable it is in the information war¹⁴.

Through the prism of military-strategic direction, information warfare is viewed by J. Arkill, D. Ronfeldt, and J. Derian. For them, it is a kind of military conflict that acts either as an independent form or as part of an expanded set of hostilities that form a network and cyber war. The possibility of domination in this case is ensured by the

¹³ Шпиґа П. С. Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*. 2014. №8. С. 329.

¹⁴ Szafranski R. Theory of Information Warfare: Preparing For 2020. Official Site of "Airpower Journal". URL: http://www.airpower.au.af.mil/airchronicles/apj/apj95/spr95_files/szfran.htm

computerization of military equipment and the formation of a network organization of the armed forces. The use of electronic technologies, automatic devices that replace humans in combat situations is envisaged. In addition, the destruction of the enemy's information systems, which entails the counterparty's inability to receive, process and use the necessary information, is deemed necessary¹⁵.

As for the second of these directions, in its framework information war is explained as political confrontation.

Thus, in the ideas of A. V. Manojlo, information warfare is a political struggle that is expressed in the form of information-psychological operations with the use of information weapons and acts as an indispensable attribute of political leadership. The implementation of the war is a heightened influence on the contradictions, objectively laid and take place at different levels of the state social system. As a result, external and internal manifestations of confrontation with a given level of intensity and in a consciously determined direction are expected¹⁶.

A systematic view of the nature of information wars is also expressed by S. M. Bukharin and V. V. Tsiganov. They reduce information warfare to a dynamic process that occurs in a complex self-organized system with many elements, the relationship between which are not deterministic but probabilistic in nature. Such a war, according to the authors, arises as a result of the advance development of any

component that requires a redistribution of resources in its favor and increased security. This conflicts with other parts of the system and brings it out of equilibrium. The result of the information war is the transformation of the system or its disappearance and the formation of a new organization¹⁷.

Thus, each of the above approaches gives an opportunity to form an idea of the individual sides of the phenomenon under study. Psychological paradigm allows to study in detail the mechanisms of influence on the intrapersonal processes of individuals, which causes changes in the mental sphere, determines the correction of the logic of worldview and its corresponding political behavior. In the context of the

¹⁵ Der Derian J. Virtuous War / Virtual Theory. *International Affairs*. 2000. № 4 (76). P. 771–788.

¹⁶ Манойло А. В. Государственная информационная политика в особых условиях. М., 2013. С. 245.

¹⁷ Бухарин С. Н. Информационные войны в бизнесе и политике. М, 2007. 336 с.

social-communicative vision of the problem, it is possible to solve the problem of filling the gaps in knowledge about the nature and methods of interactions that arise between subjects of information confrontation. The geopolitical approach allows us to consider the basic methods of contemporary world politics for achieving political and economic power in peacetime. Conflict direction focuses on an adequate assessment of the strategic importance of information in the attainment of dominant positions as a result of the struggle for power, resources and political status. The systematic approach provides relevant tools for a comprehensive study of the information war. This approach takes into account the close interrelation of its individual elements, their reflection on destabilizing factors and tactics within the framework of offensive strategies.

2. The main objectives and classification of information warfare

The information society, by its nature, has caused information wars. Information warfare is a form of information confrontation between different entities (states, non-governmental, economic and other structures), which involves conducting a complex to damage the information sphere of a competing party and protect its own information sphere and has a number of tasks¹⁸.

The objectives of the information war are:

- creating an atmosphere of breathlessness, negative attitude to culture and historical heritage in the company of a competitor or enemy;
- manipulation of public opinion and political orientation of the population of the state in order to create political tension and a state close to chaos;
- destabilization of political relations between parties, unions and movements with the aim of fomenting conflicts, stimulating mistrust, suspicion, aggravation of hostility, struggle for power;
- provoking social, political, national-ethnic and religious clashes;
- provocation, use of repressive actions by the authorities against the opposition;
- reduction of the level of information support of the authorities and management, inspiration of erroneous administrative decisions;

¹⁸ Малик Я. Інформаційна війна і Україна. URL: http://lvivacademy.com/vidavnistvo_1/visnyk15/fail/Malyk.pdf

- misleading the public about the work of state authorities, undermining their authority, discrediting their actions;
- initiating strikes, mass riots, other protests and disobedience;
- undermining the international authority of the state, its cooperation with other states;
- creation or strengthening of opposition groups or movements;
- discrediting the facts of the historical, national identity of the people; changing the value system that determines people's lifestyles and outlook;
- diminishing and offsetting world-recognized achievements in science, technology and other fields, exaggerating the value of mistakes, shortcomings, the consequences of wrongdoing and unqualified government decisions;
- formation of prerequisites for economic, spiritual or military defeat, loss of will to fight and win;
- presenting their lifestyles as behaviors and outlooks of the future that other peoples should follow;
- undermining the morale of the population and, as a consequence, reducing the defense capability and combat potential;
- another destructive ideological influence;
- damage to the security of information and technical infrastructure (hardware, software, tools and mode of protection against unauthorized leakage of information);
- protection against other destructive and informational-psychological and informational-technical influence¹⁹.

The main task of the information war between the states is to exert a direct negative destructive influence on the political power of the state by weakening its real and potential capabilities for ensuring its own security, creating difficulties in internal development and conducting active foreign activity, as well as maintaining international relations, causing damage. political image, that is, the weakening of the ruling elite, the socio-political regime established by it, or even the promotion of the latter's removal from power²⁰.

¹⁹ Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: <http://www.justinian.com.ua/article.php>.

²⁰ Малик Я. Інформаційна війна і Україна. URL: http://lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf

Of great importance is the definition of the objects of information warfare. In general, an object is something that is directed at an activity, that is, an information warfare entity is trying to influence in order to achieve a positive result for it. Thus, the main focus of direct information destructive influence in the context of information warfare is the public opinion and consciousness of the individual.

The main objects of destructive information influence are:

- resources that reveal the spiritual, cultural, historical, national values, traditions, property of the state, nation in the spheres of society;
- the ideological and psychological environment of society associated with the use of information, information resources and information infrastructure to influence the psyche and behavior of people;
- the information infrastructure, ie absolutely all intermediate points between information and the person;
- the system of formation of public consciousness (outlook, political views, generally accepted rules of behavior, etc.);
- the system of political decision making and decision making;
- the system of forming public opinion;
- human consciousness and behavior²¹.

Purposeful informational influence on the population implies the dominant position of the subject of information war in all spheres of life of another state: economic, political, psychological, religious, scientific-technical, artistic, as well as inter-national and international relations. The process of increasing the effectiveness of direct undermining measures, including information warfare, is achieved by establishing control over the information space of a foreign country, the accuracy and purposefulness of such actions, taking into account the required volume and level of reliable information that is proven, the degree of differentiation of the population by material and spiritual values. It also manifests itself in the ability to adequately perceive and respond to information, as well as political, economic, ethno-religious and other situations in the country and in the region.

Today, there are many different technologies of negative impact on the spiritual and ideological sphere of life of society, which can be used by special services of foreign states, terrorist organizations, politicized

²¹ Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: [http:// www.justinian.com.ua/article.php](http://www.justinian.com.ua/article.php).

radical organizations, criminal structures, transnational corporations and other formal and informal participants in modern international legal relations.

Therefore, in the conditions of transformation of information war its forms will also change. Yes, the first generation information fight is:

- fire suppression (in wartime) of elements of infrastructure of state and military management;
- conducting electronic warfare;
- obtaining intelligence by intercepting and decrypting information flows;
- unauthorized access to information resources with their subsequent falsification or abduction;
- mass submission in the enemy information channels or global misinformation networks to influence decision-makers;
- obtaining information from the interception of open sources of information²².

The information generation of the second generation involves:

- creation of a system of spirituality and immorality, negative attitude to the enemy's cultural heritage;
- manipulation of the social consciousness of social groups of the population in order to create political tension and chaos;
- destabilizing political relations between parties, unions and movements in order to provoke conflicts, foment distrust, suspicion, intensify political strife, provoke repression against the opposition and even civil war;
- reduction of the level of information support of the authorities and management, inspiration of erroneous administrative decisions;
- misinformation of the population about the work of state bodies, undermining their authority, discrediting government bodies;
- undermining the international authority of the state, its cooperation with other countries;
- damage to the vital interests of states in political, economic, defense and other spheres²³.

It is a well-known fact that information warfare is inherent in information weapons - it is a type of weapon, the main elements of which

²² Інформаційна війна. URL:uk.wikipedia.org/wiki/

²³ The same resource.

are information, information technologies (including technologies of information influence), information processes and technical means used in information warfare²⁴.

At the same time, the purpose of an information war is to weaken the moral and material forces of the opponent or competitor and to strengthen their own. It envisages measures of propaganda influence on human consciousness in ideological and emotional fields. After all, information warfare is an integral part of the ideological struggle. It does not lead directly to bloodshed, destruction, no casualties during its conduct, no one is deprived of food, a roof over his head. And that creates dangerous security for her. At the same time, the destruction caused by the information wars in social psychology, personality psychology, in scale and importance is quite commensurate, and sometimes exceeds the consequences of the armed wars.

It should be noted that the main task of information wars is to manipulate the masses. The purpose of such manipulation is often to:

- introducing into the public and individual consciousness hostile, harmful ideas and views;
- disorientation and misinformation of the masses;
- weakening of certain beliefs, devices;
- intimidation of his people as an enemy;
- intimidating the enemy with his power.

Finally, the last but not least task is to provide a market for its economy. In this case, information warfare is an integral part of competition. The purpose of the information war is to disrupt the exchange of information in a competitor's camp. It is easy to understand that this type of weapon is generally not aimed at the task of losing manpower. In this sense, the technology curve finally led to a bloodless and at the same time extremely effective weapon. It does not destroy the population but the state mechanism²⁵.

A completely different problem with the use of the term "information war" is the constant variation or interchangeability of the first word: often in the sense of "information" refers to the war "psychological", "communication", "information technology",

²⁴ Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: [http:// www.justinian.com.ua/article.php](http://www.justinian.com.ua/article.php).

²⁵ Маруненко О. Зовнішні і внутрішні інформаційні війни у медійному просторі України. *Освіта регіону. Політологія, психологія, комунікації*. 2011. № 4. С. 92.

"unconventional" (unrelated to the use of traditional weapons), "irregular", "virtual", etc. In most cases, such nominations only outline the main types and subspecies of the information war.

The typological ranks of information wars that M. Libiki started talking about are expanding every year. The division into species is carried out mainly by a number

of criteria: it is usually taken into account what the impact is directed to, for what purpose, through which tools. In general, the following types of information wars are distinguished:

1) command and control (confrontation for capture or disturbance of command and control mechanisms in the armed forces of the state);

2) intelligence (confrontation with the help of intelligence and counterintelligence information);

3) financial and economic (information and economic wars for control of trade, mastering of information necessary for superiority over competitors);

4) electronic, hacker, cyber-war (impact on electronic communications - radio, television and computer networks)

5) psychological (carried out through propaganda and manipulation with the purpose of undermining the public spirit, demoralizing the armed forces, discrediting the culture, disorienting the command of military forces or heads of the legislative and executive power); psychological wars have their subspecies by the nature of the influences used²⁶.

a) information-psychological (propagate certain ideas, views, ideas, beliefs, create the basis for positive or negative mass psychic reactions);

b) psychogenic (accompanied by the effects of physical factors - sound, lighting, temperature, as well as the generation of a state of shock from certain tragic events - deaths, destruction, etc.; consequences - irrational behavior, emotional affect, depression, panic);

c) psychotropic (influence - lateral programming - is carried out by the transmission of information through unconscious perception; in the case of neurolinguistic programming - by means of special linguistic programs for changing the motivation of people and their behavioral reactions);

²⁶ Чистоклетов Л. Г. Інформаційно-психологічні впливи як невід'ємна складова парадигми інформаційної. *Науковий вісник Львівського державного університету внутрішніх справ.* 2012. №2(1). С. 186–187.

6) networking (a set of information influences between social groups in social and professional networks to gain certain advantages in economic, military, political, cultural and public confrontations):

a) high-tech networking (modern, high-tech digital communications based on television, radio, Internet, messenger, cellular, satellite and other modern communications and based on gadgets such as fixed computer devices, tablets, smartphones, personal and group devices);

b) high-tech networking (modern, high-tech humanitarian technologies for creating, storing, disseminating and retrieving information; these include SMM, SEO, targeting, contextual advertising, media viruses);

c) High-Sensor Networking (modern high-tech psychology that allows to regulate and manage social communication processes at the level of social groups and individuals; typical in this aspect are social psychology, applied psychoanalysis and NLP)²⁷

G. Pocheptsov, citing U. Schwartau's research, in his book "Information Policy", cites another classification of information wars, built "on the level of objects: from one person to the whole state". According to this criterion distinguish:

1) personal information war, where different types of manipulations with personal electronic information belong;

2) corporate information warfare, where information systems attack situations are classified;

3) a global information war, where information is regarded as a national asset that can be hunted by other countries²⁸.

The IT revolution has opened up vast opportunities for influencing peoples and power, manipulating people's consciousness and behavior, even in remote spaces. Given the globalization of communication networks in the world, it can be assumed that it is the information types of aggression that will be given priority in the future.

Information wars are taking place in modern Ukraine. In particular, the well-known Russian politician B. Nemtsov described the information war, which is the information support for the aggression of the Russian

²⁷ Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник. Київ, 2016. С. 46–50.

²⁸ Почепцов Г. Г. Інформаційна політика : навчальний посібник. Київ : Знання, 2008. С. 564.

Federation against Ukraine, as a war of the Nazi regime against a democratic state.

Information war as an aggressive interaction of the opposing parties in the information sphere has a negative impact on the state of political communications of the society as a whole. The use of such campaigns by political actors is associated with increased risks, resulting in a rapid change in statuses and positions in power relations. Due to the high intensity of disputes, information wars are poorly managed and deliberately regulated and therefore act as a two-pronged weapon for the opposing parties. Achieving goals in such ways enhances political confrontation, reduces the possibility of spreading a consensus culture, undermines stability in society.

CONCLUSIONS

The concept of "information war" is not an allegorical image, it reflects a kind of war, a form of warfare which is an information struggle. Its high efficiency was confirmed by the scale and results of the Cold War, which was the most striking in comparison with the previous world wars, although it was carried out without the resolution of the armed struggle, as well as the experience of local wars and armed conflicts of our time. The essence and role of information warfare is devoted to a large number of publications in which it is viewed differently. The definition of information warfare can be grouped as follows: the definition of information warfare in a narrow sense - reflects a purely military orientation, and the definition in the broad sense - the focus on ensuring national interests in any vital sphere of state and public activity.

Factors of origin and vitality of ideas of information war, according to various estimates are as follows:

- the world economy dictates and its world laws are increasingly humane. The main one is simple: war (in the traditional sense) is not economically viable. This is one of the systemic factors contributing to the spread and development of humanistic tendencies;
- the cost-effectiveness of information weapons, which will, on the one hand, reduce to some extent the military budget and, on the other, create highly effective weapons of the 21st century, the use of which will have promising results;

– the mass use of information weapons, according to Western experts, will allow relatively quickly to suppress the enemy, paralyze him, to force surrender without the involvement of the armed forces, without the usual battles typical of classic wars, without the death of people and the destruction of civilian infrastructure, and finally without loss of personnel.

Due to the fact that information warfare is a multifaceted and complex phenomenon, it is conducted in various dimensions, involves the use of a conglomerate of techniques, raises the question of overcoming the framework's limited individual theoretical constructs. On this basis, the author concludes that it is necessary to apply a polyparadigmatic approach to the study of information war as one of the aspects of contemporary socio-political reality.

SUMMARY

The article defines the essence of the concept of "information warfare" and reveals the reasoned concepts of information wars. The main attention in the work focuses on the theoretical and methodological positions of scientists belonging to various scientific schools and defining information warfare through specific aspects of the problem.

The concept of information war, forms and types of information wars, their action against society are revealed.

It has been proven that information weapons are emerging as the main the information warfare tool cannot be used on its own; there are necessarily entities seeking to exploit, for useful and criminal purposes, the positive properties of information and information technology that have been created for the benefit of man, society and the state.

REFERENCES

1. Бухарин С. Н. Информационные войны в бизнесе и политике. М, 2007. 336 с.
2. Гриняев С. Концепция ведения информационной войны в некоторых странах мира. URL: http://www.soldiering.ru/psychology/conception_psywar.php
3. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу : навчальний посібник . К.: КНТ, 2007. 260 с.
4. Інформаційна війна. URL: uk.wikipedia.org/wiki/

5. Карпенко В. Інформаційний простір як чинник національної безпеки України. *Українознавство*. 2005. № 3. С. 182–192.
6. Курбан О. В. Сучасні інформаційні війни в мережевому онлайн просторі : навчальний посібник. К, 2016. 286 с.
7. Лисичкин В. А. Третья мировая (информационно-психологическая) война. URL: <http://malchish.org/lib/politics/infwar.htm>
8. Малик Я. Інформаційна війна і Україна. URL: http://lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf
9. Манойло А. В. Государственная информационная политика в особых условиях. М, 2013. 320 с.
10. Маруненко О. Зовнішні і внутрішні інформаційні війни у медійному просторі України. *Освіта регіону. Політологія, психологія, комунікації*. 2011. № 4. С. 92–96.
11. Михальченко И. А. Информационные войны на рубеже XXI века. *Безопасность информационных технологий*. 1998. № 3. С. 14–15.
12. Панарин И. Н. Информационная война и третий Рим. М., 2001. 244 с.
13. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: <http://www.justinian.com.ua/article.php>.
14. Почепцов Г. Г. Інформаційна політика : навчальний посібник. 2008. 66 с.
15. Проноза І. І. Інформаційна безпека держави: сутність та основні визначення. *Гілея : науковий вісник. Збірник наукових праць*. 2017. № 127(12). С. 345–349.
16. Проноза І. І. Інформаційна війна: сутність та особливості прояву. *Актуальні проблеми політики. Збірник наукових праць*. 2018. № 81. С. 79–84.
17. Расторгуев С. П. Философия информационной войны. М, 2003. 496 с.
18. Чистоклетов Л. Г. Інформаційно-психологічні впливи як невід’ємна складова парадигми інформаційної. *Науковий вісник Львівського державного університету внутрішніх справ*. 2012. №2(1). С. 183–193.
19. Шпига П. С. Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*. 2014. № 8. С. 326–339.

20. Der Derian J. Virtuous War / Virtual Theory. *International Affairs*. 2000. № 4 (76). P. 771–788.

21. Szafranski R. Theory of Information Warfare: Preparing For 2020. Official Site of “Airpower Journal”. URL: http://www.airpower.au.af.mil/airchronicles/apj/apj95/spr95_files/szfran.htm

Information about the author:

Pronoza I. I.

Candidate of Political Sciences,
Senior Lecturer at the Department of Political Sciences and Law,
South Ukrainian National Pedagogical University
named after K. D. Ushynsky
26, Starofrankivska str., Odessa, 65000, Ukraine