Vol. 4, No. 2, 2018

УДК 327.88

ІНФОРМАЦІЙНА ВІЙНА ТА ЇЇ ОСОБЛИВОСТІ НА СУЧАСНОМУ ЕТАПІ

Микола Бучин
Національний університет "Львівська політехніка"
buchyn@ukr.net
ORCID: 0000-0001-9087-5123

Юля Курус
Національний університет "Львівська політехніка"
ORCID: 0000-0002-3596-7073
yuliia.kurus@gmail.com

(стаття надійшла до редколегії – 19.10.2018 р., прийнята до друку – 14.11. 2018 р.)

У статті автори розкривають суть інформаційної війни, акцентують увагу на основних розумінням цього феномену. Наголошено, що в науковій літературі інформаційна війна трактується, зокрема, як: суперництво в інформаційно-психологічній сфері задля впливу і контролю над ресурсами; інформаційний вплив на прийняття політичних рішень; сучасний конфлікт, який притаманний для епохи постіндустріального суспільства; конфлікт, який передбачає використання інформаційної зброї та ін. Трактуючи інформаційну війну з позиції конфліктологічного підходу, автори з'ясовують відмінності між інформаційною війною і такими поняттями, як «психологічна війна», «збройний конфлікт», «кібервійна», «кібертероризм», «мережева війна», «хактивізм». Виокремлено суб'єктів та об'єктів інформаційної війни, виділено різноманітні форми інформаційних протистоянь. Автори характеризують основні цілі інформаційних воєн: контроль інформаційного простору; захист інформації; інформаційні атаки на суперника; підвищення ефективності збройних сил та ін.

Значну увагу звернено на аналіз інформаційної зброї. Автори виокремлюють її основні характеристики та переваги порівняно з традиційною зброєю, конкретні форми її використання. Показано відмінності між оборонною та наступальною інформаційними війнами. Виділено основні принципи ефективності інформаційних воєн, зокрема: прикладання максимуму зусиль задля розширення інформаційного простору зі збереженням контролю; здійснення інформаційного впливу на найуразливіші елементи інформаційної системи противника; здійснення протидії та контрдії інформаційному впливу ворога та зменшення сфери його поширення; застосування комплексного підходу під час формування стратегії інформаційного протиборства (поєднання методів інформаційної війни з економічними, військовими, політичними та іншими чинниками).

Ключові слова: *інформаційна війна, інформаційна зброя, конфлікт, кібервійна, інформація.*

INFORMATION WAR AND ITS PARTICULARITIES AT THE CONTEMPORARY STAGE

Mykola Buchyn
Lviv Polytechnic National University
ORCID: 0000-0001-9087-5123
buchyn@ukr.net

Yuliia Kurus
Lviv Polytechnic National University
ORCID: 0000-0002-3596-7073
yuliia.kurus@gmail.com

In the article, the authors reveal the essence of information warfare; focus on the basic understanding of this phenomenon. The article acknowledges that in the scientific literature information war is interpreted, in particular, as

rivalry in the informational and psychological sphere for the influence and control over resources; informational influence on making political decisions; a modern conflict that is inherent in the post-industrial society era; a conflict involving the use of information weapons, etc. By characterization of information warfare from the standpoint of the conflict-based approach, the authors find out the differences between the information warfare and such concepts as "psychological warfare", "armed conflict", "cyberwarfare", "cyberterrorism", "network warfare", "hacktivism". The subjects and objects of information warfare and various forms of information conflicts are distinguished. The authors describe the main goals of information wars: control of information space, information protection, informational attacks on an opponent, increasing the effectiveness of the armed forces, etc.

Considerable attention is paid to the analysis of information weapons. The authors distinguish its main characteristics and advantages compared with conventional weapons, the specific forms of its use. The differences between defensive and offensive information wars are shown. The basic principles of the effectiveness of information wars are highlighted, in particular: maximum effort is made to expand the information space with preservation of control; implementation of information influence on the most vulnerable elements of the enemy's information system; realization of counteraction to the informational influence of the enemy and reduction of its sphere of distribution; application of an integrated approach during the formation of a strategy of information confrontation (a combination of methods of information warfare with economic, military, political and other factors).

Keywords*: information warfare, information weapon, conflict, cyberwarfare, information.*

Conflicts are an integral part of the functioning of human civilization. However, if in the previous epoch the concept of conflict was associated with armed confrontation and human casualties, in the era of the development of post-industrial society, which a priori is information society, a theoretical rethinking of the essence, place, and role of conflict in human relations is taking place. In particular, it refers to the concept of «information war», which has not yet received the proper theoretical justification but has become an attribute of modern international relations. Moreover, the understanding of the aforementioned concept is complicated by the absence of not only a single interpretation of the phenomenon, but also by the use of such concepts as "network war", "cyberwar", "cyberterrorism", "hybrid war" etc. This requires not only a conceptual study of these concepts but also a clear differentiation of them.

For Ukraine, the selected issues are extremely relevant, because our state is in a status of undeclared war with Russia, which is largely an informational confrontation in its essence. Therefore, the research of the problem of information war will enable not only to more clearly define the features of this phenomenon but also to develop effective mechanisms for counteracting Russian aggression against Ukraine.

The problems of the information war were engaged by such foreign scholars as V. Belonozhkin, I. Vasylchenko, A. Gor, D. Denning, A. Edelstein, R. Clarke, V. Korovin, A. Manuilo, S. Rostorhuiev, E. Toffler, M. Trebin, M. Troitskyi, V. Tsyhanov and others. Among the domestic researchers, it should be noted such scholars as I. Valiushko, I. Denysenko, E. Mahda, O. Merezhko, G. Pocheptsov, G. Sasyn, T. Chukhlib, P. Shpyha, and others. They explored the essence and features of the information war, the goals, and principles of its implementation. At the same time, the lack of a unified interpretation of the concept of "information war", its newest and dynamic nature requires a more detailed understanding of this phenomenon, ascertaining its role in modern international relations.

The aim of the article is to carry out a political analysis of information warfare at the present stage.

The phenomenon of information influence, as well as information threats and confrontations in the socio-human sciences, is the subject of research by many scholars. It is also worth noting that the concept of "information warfare", as well as the derivatives of it definitions ("informal confrontation", "informal and psychological warfare», "informal influence", "information and psychological operation" etc.), appears to be rather unspecified in the theoretical terms and not fully developed and worked out in relation to its functional purpose.

As is well known, the term "information war" first appeared during the Cold War – the confrontation between the Soviet Union and the countries of Western Europe and the USA in the 1970s. It is worth drawing attention to the work of the former US Vice President, Nobel Laureate, Albert Arnold Gore Jr., who called the information war as an attack on the mind. In his work "Attack on the Mind" emphasizes the role of information influence on the adoption of political decisions, as well as the peculiarities of behavior and reaction of individuals to the «information boom» from the side of interested parties [Гор 2008].

It is clear that during the interpretation of information warfare as one of a variety of conflicts, this concept should be considered, first of all, through the conflictological paradigm. In this context, it should be noted that the change in social formations also changed the classification of wars. In particular, one of the authors of the concept of "information civilization", American

sociologist Elvin Toffler, divided the development of society into "three waves", namely:

► wave 1 – agrarian society. This wave was characterized by the concept of "power".

► wave 2 – an industrial society. This wave was characterized by the concept of "wealth";

► wave 3 – post-industrial society. This wave was characterized by the concept of "knowledge".

Based on the theory of the scientist, during the agrarian society, those who showed their strength came to power, in the industrial society – those who owned the material property, and already in the post-industrial society – those who owned knowledge, intelligence, and the main thing – information [Тоффлер 2003].

So, in the modern third wave of post-industrial society, the wars acquired completely different characteristics and forms. Key properties of such wars: information becomes a weapon in the conduct of war; space is increasingly being mastered; computerization of management takes place [Денисенко 2008: 214].

History gives a lot of examples of wars that are significantly different among themselves by means, methods, objects, and subjects. Information warfare also has many differences from other forms of wars. That is why, in our opinion, it is worthwhile to consider the difference between information warfare and other types of wars.

Each type of war is directed at a certain type of space. For the traditional type of war (armed confrontation) the main objective is the physical space. If this is psychological war than the main objective is the cognitive space. For the information war, the main objective is an informational space. The difference between these types of wars is also the time values. Physical space, which is the purpose of the traditional war, needs an instant reaction. The information war requires, in turn, a daily plan of action. At that time, psychological warfare requires planning of action for decades [Поцепцов 2013].

The main difference between the *psychological warfare* and information is that the psychological warfare is primarily a whole range of means and methods that are aimed at influencing a person and his consciousness in order to change his views, thoughts, value orientations, stereotypes, norms, established stereotypes, mass sentiment and public consciousness in general. Information influence is directed not only on the public consciousness but also on the image of the state, its computer systems, decision-making systems, systems for the dissemination and use of information resources etc. [Чухліб 2004].

The differences between the *armed conflict* and the information war are not only the target space, methods, means, but also the presence of defeat: the defeat in information warfare, compared with armed confrontation, is almost impossible.

Regarding this issue, a lot of discussions arose in political science, but if it is logical to proceed from the fact that both the traditional and the information confrontation are wars, then the defeat, as in any confrontation, should be on one side. The information war has only one difference from the traditional war – a type of weapon. So, if the type of weapon used in these types of wars is different, then the signs of defeat should be the same.

If we take into account the traditional war, the signs of defeat in such a confrontation may be such effects as the reduction of armed forces, the loss of part of the territory, political dependence on the winner, the removal of technology-intensive technology, the death or emigration of a part of the population, the destruction of industry and payment of indemnity etc. [Расторгуев 2003: 155].

As for the defeat in the information warfare, one can distinguish the following features:

• Injury of the information system, change or loss of its elements and substructure units. Such transformations and simplifications in the system make it safe for the enemy.

• Performance of tasks in the area of interests of the winner. The system processes only the data that it receives from the winner.

• The defeated system takes over the algorithm of the winner system's operation. The system is directly absorbed by its structural units and elements, that is, the structure in general [Расторгуев, 2003: 155-156].

As we see, in general, for the losing party, it does not play an important role in which war it has lost – in the traditional form of the war, or in the information. The distinction between these two types of wars is the culmination. If we are talking about information warfare, then there is no definite end. If we are talking about the traditional form of war, then the culmination, in this case, is most likely to be in the form of signing a peace agreement. In addition, the winning party will not refuse to control the information system of the defeated party both through material and security benefits.

If we are talking about such concepts as cyberwarfare, cyberterrorism, network warfare, hacktivism, so for each of these activities there are its distinct characteristics from information.

Network wars differ in the fact that they are not conducted by armed or other means, but by network organizations. That is participants in the network warfare use network organizations, doctrines, strategies, and technologies that are typical of the present-day information era. Network warfare can also be seen as the organization

and conduct of hacker attacks, as well as the spread of computer viruses in the information and communication systems and enemy databases [Коровин 2009].

Today, the most dangerous kind of crime is *cyberwarfare*. Many scholars give a variety of definitions to this notion. Some of them identify the cyberwar with computer confrontation on the Internet. Ukrainian scientist O. Merezhko defines cyberwarfare as technological and informational tools and methods that are carried out through the Internet to cause damage not only to the enemy's information security, but also to the military, economic, technological, and political [Мережко 2009].

The well-known magazine The Economist, in turn, characterizes cyberwarfare as the so-called fifth wave of forms of war [Cyberwar 2010]. Alan Richard Clark, a well-known American politician, and anti-terrorism expert describes this concept as penetration into computer systems and networks of an opponent of one of the participants in the confrontation, namely the state, in order to damage or destroy them directly [Clarke 2010].

Ukrainian scientist V. Topchiy under *cyberterrorism* understands a deliberate, motivated attack on computer systems, networks that contain and process information for certain political purposes.

Hacktivism is the use of computers and computer networks to achieve certain political goals. Hacktivism is a fairly controversial term with many definitions. In general, the word meant direct electronic actions aimed at social change by combining program skills and critical thinking. However, hacking is now defined as a crime that is destructive, harmful, dangerous and undermining Internet security as a technical, economic and political platform [Denning 1999].

In general, information warfare differs from other activities by the fact that it exercises its influence on the consciousness of people; on information and technical systems of different scale and purpose; on systems of formation of public consciousness; on decision making systems; on systems of formation and functioning of public opinion. While other types of activities direct their influence on a certain category: psychological warfare affects people's consciousness, cyberwarfare – on computer networks through the Internet, network wars – on information and communication systems, cyberterrorism – on computer systems and networks, hacktivism – on information systems through computers, computer networks, and the Internet [Цыганов 2007: 65].

Information warfare is a deliberate action to achieve information advantage by causing damage and detriment to information, information processes and information systems of the enemy. Hence it turns out that the purpose of the information war is to inflict an attack to protect itself or defeat the enemy [Белоножкин 2009].

The main component of the information war is information weapons. It is difficult not to agree with those authors who consider information weapons more dangerous than nuclear ones because these types of weapons have different goals of harming. More importantly, the information weapon has a distinct offensive character, because the effect of the information strike has a preventive nature. Offensive nature of information weapons largely determines the subject of information warfare and immediately allows declassifying an aggressor. Offensive information weapons can in some way measure the potential of aggressiveness if you determine the amount of information that is broadcast from one participant of the information confrontation to another.

Information weapons are defined as information that serves as the main weapon for victory and damage to the enemy. One of the advantages over other types of weapons is its intangible value. One American president, namely Richard Nixon, once said that one dollar spent on propaganda is more important and will give more than ten dollars that were invested in weapons. Since this one dollar will be used and put into action immediately, those ten dollars will still be waiting [Edelstein 1997].

Another advantage of information weapons is its latent character. In the information theory, there is the principle of secret and invisible use of this weapon, which is explained by the fact that the subjects of the information war can hurt the enemy hidden and invisible, which complicates the nature of interactions in information wars [Василенко 2010]. This implies that information warfare can be carried out independently, that is, without the use of traditional means and methods of armed struggle, and in combination with other types of hostilities.

The quality of information possessed by the parties to the confrontation directly affects their combat readiness. For the readiness of the enemy, the influence is exercised, for example, by destroying the infrastructure, living power and technology, violating the processes of information exchange, infusing the information systems of the enemy of their information.

From this point of view, the task of information warfare – the impact on the enemy's information in order to undermine his combat readiness, as well as protecting own information from the enemy’s influence at the same time. The information can act as an object of influence, and as a weapon in information warfare.

An important point regarding information wars is that such confrontations are generally perceived only as an offensive and attack on an opponent. However, information warfare can be both offensive and defensive.

The Defensive Information War is characterized by actions aimed at protecting its own information

systems and combat communication means from hostile attacks and attempted damage.

The offensive information warfare deals with the degradation of information on the enemy's battlefield. That is, those are the actions, means, methods, and principles that are considered to be the definition of the concept of information confrontation.

In addition to tools and methods, there are also certain principles that guide participants in information wars during their conduct or training. In general, we can highlight the following principles of the effectiveness of information wars:

• Maximizing efforts to expand the information space while maintaining control.

• Influence on the most vulnerable elements of the enemy's information system.

• Counteraction to the informational influence of the enemy and reduce the scope of its spread.

• Application of an integrated approach during the formation of an information confrontation strategy. This means the combination of methods of information warfare with economic, military, political, etc. [Шпига 2014].

However, as scientists point out, the main principle of conducting an information war is the aggressor's desire to continuously expand the controlled information space, despite acceptable moral standards and rules, deliberately violating all social restrictions and moral principles [Василенко 2010].

With regard to the latest principle of conducting information warfare, namely, the formation of a strategy, it should be noted that the strategy is a certain action plan, which is followed by participants in information wars for the effective completion of the confrontation. The development of the strategy includes not only the identification of vulnerable structural units of the enemy's information system but also the outline of the main means, methods, and principles of protecting the information space in order to ensure the security of its own information structure.

So we can conclude that the information has become a new weapon, due to which it is possible to gain victory in the war. Information warfare is not a new phenomenon and its origins date back to the last century. In the scientific environment, there is no clear definition of information warfare. Due to the rapid development of technologies, the modification of the means and methods of information confrontation has begun, contributing to the constant modification of the features and assertions regarding this concept. Information warfare is a systematic information impact on the entire information-communicative system of the enemy and neutral states in order to create a supportive global information environment for conducting any political and geopolitical operations that provide maximum control over space.

Taking into account the fact that Ukraine became the object of Russian military aggression, which also includes an information component, the issue of Russia's information war against Ukraine is forward-looking for further research.

СПИСОК ЛІТЕРАТУРИ

Белоножкин, В., Остапенко, Г. (2009). Информационные аспекты противодействия терроризму. Москва: Горячая линия-Телеком.

Валюшко, І. (2015). Еволюція інформаційних війн: історія і сучасність. *Історико-політичні студії. Серія: Політичні науки, № 2*, 127–134.

Василенко, И. (2010). Политическая философия. Москва: Инфра-М.

Гор, А. (2008). Атака на разум. Москва: Амфора.

Денисенко, І. (2008). Сучасні війни: нові підходи та інтерпретації. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: «Питання політології»*, Вип. 12, № 810, 212–218.

Коровин, В. (2009). Главная военная тайна США. Сетевые войны. Москва: Яуза, Эскмо.

Магда, Є. (2014). Виклики гібридної війни: інформаційний вимір. *Наукові записки Інституту законодавства Верховної Ради України*, № 5, 138–142.

Мануйло, А., Петренко, А., Фролов, Д. (2004). Государственная информационная политика в условиях информационно-психологических конфликтов высокой интенсивности и социальной опасности: Учебное пособие. Москва: МИФИ.

Мережко, О. (2009). Проблеми кібервійни та кібербезпеки в міжнародному праві. *ЮСТІНІАН*. Отримано з: http://www.justinian.com.ua/article.php?id=3233.

Соловьёв, А. (2004). Политические коммуникации: учебное пособие для студентов вузов. Москва: Аспект Пресс.

Почепцов, Г. (2013). Смислові та інформаційні війни: пошук відмінностей. *MediaSapiens*. Отримано з http://osvita.mediasapiens.ua/
ethics/manipulation/smislovi_ta_informats
iyni_viyni_poshuk_vidminnostey/

Расторгуев, С. (2003). Философия информационной войны. Москва: Московский психолого-социальный институт.

Сасин, Г. (2015). Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). *Грані*, № 3, 18–23. Отримано з http://nbuv.gov.ua/j-pdf/Grani_2015_3_5.pdf.

Тоффлер, Е. (2003). Нова парадигма влади. Знання, багатство й сила. Харків: Акта.

Требин, М. (2005). Войны XXI века. Москва: АСТ; Минск: Харвест.

Требін, М. (2013). Феномен інформаційної війни у світі, що глобалізується. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія*. Право, № 2 (16), 188–198.

Троицкий, М. (2002). Концепция «программирующего лидерства» в евроатлантической стратегии США. *Pro et Contra*, № 4, 86–103.

Цыганов, В. (2007). Информационные войны в политике. Москва: Академический проект.

Чухліб, Т. (2004). Батько «психологічних війн». *Газета "День"*. Отримано з http://day.kyiv.ua/uk/article/ukrayina-incognita/batko-psihologichnih-viyn.

Шпига, П., Рудник, Р. (2014). Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*, № 8, 326–339.

Clarke, A., Knake, R. (2010). Cyber War. New York: Harper Collins Publishers.

Cyberwar (2010). The Economist. Отримано з http: //www. economist.com/node/16481504?story_id=16481504 &source= features_box1

Denning, D. (1999). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *Nautilus Institute for security and sustainability*. Отримано з http://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

Edelstein, A. (1997). Total propaganda. From mass culture to popular culture. New York: Lawrence Erlbaum Associates.

REFERENCES

Belonozhkin, V., Ostapenko, H. (2009). Informational Aspects of Countering Terrorism. [In Russian]. Moscow: Goryachaya liniya-Telekom.

Chukhlib, T. (2004). The Father of "Psychological Wars". [In Ukrainian]. *Newspaper "Day"*. Retrieved from http://day.kyiv.ua/uk/article/ukrayina-incognita/batko-psihologichnih-viyn

Clarke, A., Knake, R. (2010). Cyber War. New York: Harper Collins Publishers.

Cyberwar (2010). *The Economist.* Retrieved from http://www. economist.com/node/16481504?story_id= 16481504&source=features_box1.

Gor, A. (2008). Attack on the Mind. [In Russian]. Moscow: Amfora.

Denning, D. (1999). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *Nautilus Institute for security and sustainability*. Retrieved from http://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

Denysenko, I. (2008). Modern Warfare: New Approaches and Interpretations. [In Ukrainian]. *Visnyk of V. N. Karazin Kharkiv National University. Series: "Questions of political science"*, Issue 12, № 810, 212–218.

Edelstein, A. (1997). Total Propaganda. From Mass Culture to Popular Culture. New York: Lawrence Erlbaum Associates.

Korovin, V. (2009). The Main Military Secret of the United States. Network Wars. [In Russian]. Moscow: Yauza: Eskmo.

Mahda, E. (2014). Challenges of the Hybrid War: Information Dimension. [In Ukrainian]. *Scientific notes of the Institute of Legislation of the Verkhovna Rada of Ukraine*, No. 5, 138–142.

Manuylo, A., Petrenko, A., Frolov, D. (2004). State Information Policy in the Conditions of Information-Psychological Conflicts of High Intensity and Social Danger: Tutorial. [In Russian]. Moscow: MIFI.

Merezhko, O. (2009). Problems of cyberwarfare and cyber security in international law. [In Ukranian]. *YUSTINIAN*. Retrieved from http://www.justinian.com.ua/article. php?id=3233.

Pocheptsov, H. (2013). Semantic and Information Wars: Finding Differences. *MediaSapiens*. [In Ukrainian]. Retrieved from http://osvita.mediasapiens.ua/ ethics / manipulation / smislovi_ta_informats iyni_viyni_poshuk_vidminnostey/.

Rastorguyev, S. (2003). The Philosophy of the Information War. [In Russian]. Moscow: Moscow Psychological and Social Institute.

Sasyn, H. (2015). Information War: the Essence, Means of Realization, Results and Possibilities of Counteraction (on the Example of Russian Expansion into Ukrainian Space). [In Ukrainian]. *Hrani*, No. 3, 18–23. Retrieved from http://nbuv.gov.ua/j-pdf/Grani_2015_3_5.pdf

Shpyha, P., Rudnyk, R. (2014). The Main Technologies and Patterns of Information Warfare. [In Ukrainian]. *Problems of international relations*, №. 8, 326–339.

Solov'yva, A. (ed.). (2004). Political Communications: Textbook for University Students. [In Russian]. Moscow: Aspect Press.

Toffler, E. (2003). New Power Paradigm. Knowledge, wealth and power. [In Ukrainian]. Kharkiv: Akta.

Trebin, M. (2005). Wars of the XXI century. [In Russian]. Moscow: AST; Minsk: Harvest.

Trebin, M. (2013). The Phenomenon of Information Warfare in a Globalizing World. [In Ukrainian]. *Visnyk of Yaroslav Mudryi National Law University. Series: Philosophy, Philosophy of Law, Political Science, Sociology*. Law, No. 2 (16), 188–198.

Troitskiy, M. (2002). The Concept of "Programming Leadership" in the US Euro-Atlantic Strategy. [In Russian]. *Pro et Contra*, no. 4, 86–103.

Tsyganov, V. (2007). Information Wars in Politics. [In Russian]. Moscow: Academic project.

Valiushko, I. (2015). Evolution of Information Warfare: History and Modernity. [In Ukrainian]. *Historical and political studios. Series: Political Sciences*, № 2, 127–134.

Vasilenko, I. (2010). Political Philosophy. [In Russian]. Moscow: Infra-M.