Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 28-34 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

INFORMATION WAR IN UKRAINE

Volodymyr Khoroshko, National Aviation University, Doctor in Technical Sciences, Professor, Kyiv,
Volodymyr Artemov, National Aviation University, Doctor of pedagogical sciences, Professor, Kiev,
Ivan Opirskyi, Lviv Polytechnic National University, Doctor in Technical Sciences, Associate Professor,
Nikolay Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor, Kyiv, Ukraine
Ihor Ivanchenko, National Aviation University, PhD in Engineering Science, Associate Professor Kyiv, Ukraine

ABSTRACT: Today, the information war is a total phenomenon where it is impossible to determine its beginning and end. This is the existence of a struggle between states with the help of information weapons, that is, it is open and hidden targeted informational influences of states on each other in order to gain an advantage in the material sphere, where informational influences are influences by means of such means, the use of which allows you to achieve your goals. Four approaches to the definition of information war are described, containing political, legal, socio-economic, and psychological actions, involving the capture of the enemy's information space, the destruction of his communications, deprivation of means of transmitting messages, etc., as well as conceptual issues and the basics of network-centric theory control systems and the organization of military operations and cyber actions or cyber war. The implementation of the cybernetic approach strategy for organizing actions during military operations was studied to obtain the maximum effect from the impact on three areas - moral, mental, physical, and the sufficiency of such an approach to increase the mobility, accuracy and firepower of weapons was determined. Also investigated the effect on the most vulnerable objects using the system of the cybernetic approach, which allowed to assess its application in modern conditions of development of strategy and tactics of the struggle in the information field.

KEYWORDS: *informational-psychological influences, informational warfare, informational weapons, informational field, strategy, cybernetic warfare, cyber actions*.

At all stages of human civilization development, information was both the most important object and a means of fighting between people, nations, and states. Individual facts of influence on a wide audience can be revealed throughout the history of society. It is clear that in different periods, the intensity of the use of certain influence methods, as well as the perfection of its organization, are very different.

The politics of information warfare and the use of information influences emerged from the earliest times, but it should be noted that a systematic study of these phenomena only began in the twentieth century. However, the first attempts to investigate these topics took place in ancient times. Among the scholars of ancient times we should mention the works of Aristotle [1], Sun Tzu [2]. In the Renaissance, N. Machiavelli worked on this problem, publishing the book "The Prince" [1]. It is well-known fact that Princess Olga took trip from Kiev to Constantinople, but neither Byzantine nor Russian sources explain the reason and purpose of such a long journey. The realization of informational influences (concealment of information; its partial submission and others) was recorded by the chronicler in the territory of Ukraine during the times of Kievan Rus. The militant prince Svyatopolk reported in advance about his campaign, but kept the direction and forces he planned to use in secret. This was done to start the panic in the state of the enemy troops and quickly defeat him [3]. In the nineteenth century. K. von Clausewitz addressed the issue of information confrontation in the book "On War" [4]. During the XX-XXI centuries. many scientists from all over the world have been very productive in these issues and have achieved considerable success. The first documented research on the theory of information warfare is the work of Martin Libicki "What is Information Warfare?" Great contribution to the development of information warfare has been made by American scientists: Z. Brzezinski, D. Boyd, D. Warden, V. Linda, A. Sebrovski, D. Garstka, J. Stein, G. McLuyen, and also Russian: S. Rastorguev , S. Kara-Murza, A. Manojlo, I. Panyarin, S. Makarenko

and others. In addition, among Ukrainian researchers the following should be noted: G. Pohentsov, O. Litvinenko, V.V. Ostroukhova, V. Lipkanya, L.F. Kompantsev, R. Grishchuk and others.

The term “information warfare” introduced Chinese theorist Shen Wenguan [5,6]. And one of the first to write about the phenomenon of information wars publicly was M. McLuhan in 1960. Even then, it was known that the Cold War is being waged with the help of information technology, since it has been fought with the help of advanced technologies during the whole war.

It should be noted that the hybrid war was the invention of Eugene Messner, a White Guard colonel who was chief of staff at the Cornillian Division. He developed the theory of rebellion-war. In 1967, he published a book called “The Third World Theory”, in Argentina. The General Staff of the Soviet Union began to implement and develop this concept in the late 70's - early 80's of the XX century. In fact, consideration of hostilities and their organization from the standpoint of military cybernetics were formulated by M. Ogarkov during these years. Russia has adopted this concept and is now using it [6].

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

In [8] it is noted that there are now 4 approaches to the definition of information war:

- The first approach treats it as a set of political-legal, socio-economic, psychological actions that involve seizing the enemy's information space, destroying its communications, depriving the 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 war is interpreted as a form of providing and conducting military force through the most modern electronic means;
- The fourth approach identifies information wars as cyber wars.

For the first time, the conceptual questions and foundations of the theory of the network-centric system of management and organization of combat and cyber-war were implemented in the US military doctrines "Joint Vision 2010", "Joint Vision 2020". The main aspects of taking a state under external control for the realization of its interests by suppressing the will of the victim population and government to resist through the use of a wide range of innovative technologies that are comprehensively applied were described in a 1989 article by William Linds “The Face of War, Changing: on the way to the fourth generation ”[9]. Major in the fourth-generation wars, according to Linda's views, is the fault of cultures, the initiation, support and nourishment from the outside, and the organization within the state of psychological and information pressure on its population and leadership, taking them under external control and management, creating the conditions for their emergence and promotion. growth in the country of socio-economic chaos and the very depletion of military, financial and other resources [9].

Targeted all-inclusive aggressive attacks on traditional cultural, historical and other values of the population, on the reputation of the most effective leaders of state and state-military administration. Creating conditions to harm education, culture, education of citizens. Starting "low intensity conflicts" with the participation of external, internal and theoretical forces on the victim territory.

The implementation and strategy of the cybernetic approach (Boyd's cybernetic cycle) to organize actions during military operations to maximize the impact on three areas (moral, mental, physical) was carried out by John Boyd during Operation Desert Storm in 1991. He considered war as a combination

of these three components: the destruction of the will of the enemy, the undermining of the common faith and common views; actions to distort and create perceptions of the enemy of reality based on misinformation and to create misconceptions about the situation; the destruction of the enemy's physical resources (weapons, manpower, infrastructure and supplies). At the same time, he proposed to consider all actions of his forces and the forces of the enemy within the cybernetic cycle, which has four processes in its structure: observation, orientation, decision, action ("Boyd's loop"), which, according to the author, reproduces itself and is self-regulating [9].

Based on the works of Boyd and his followers, the following tenets of the theory of OODA (Observe - observe, Orient - orient, Decide - decide, Act - action) [7]:

1. Counterparty military activities (combat operations) are carried out in the same cyber cycles of OODA.

2. The main elements of the OODA cycle are as follows:

- observation - gathering information from internal and external sources;
- orientation - formation of a set of possible plans (options) and evaluation of each of them according to a set of criteria;
- decision - choosing the best action plan for practical implementation;
- action - practical implementation of the chosen action plan.

3. The OODA cycle is a model of military activity of individuals and organizations for war and conflict of all levels (tactical, operational and strategic).

4. Directions for winning (gaining competitive advantage):

- reduction of the OODA cycle execution time;
- improving the quality of decisions made in the cycle.

5. Increasing the speed of all four elements of the OODA cycle is the main way to achieve victory.

Among the four stages of the OODA cycle, three are directly related to information processing and computer technology. The fourth stage (action) is generally "kinematic" and involves the movement in space, defense and defeat of the enemy on the basis of combat.

In order to maintain the timeframes of the OODA cycle of action of their forces and to provide a higher tempo of battle, it is necessary to accelerate all four stages of the cycle that are being implemented. Throughout the twentieth century, all efforts by scientists, engineers, and the military have been directed toward improving weapons and technology in the kinematic portion of the OODA loop. These efforts have resulted in increased mobility, accuracy and firepower of the weapons. However, at the present stage, the technological boundary of the kinematic part of the OODA cycle has come - more powerful weapons inflict acceptable acceptable damage, while faster and more secure weapons platforms and means of delivery deliver a striking target to the target. Due to this, there is a need to improve other stages of the OODA cycle.

Since the first three stages of the OODA cycle are directly related to the processes of gathering, distributing, comprehending, analyzing, and making decisions based on the information obtained, the faster the information is collected, distributed, analyzed, and perceived, the faster the decision is made. Speed and correctness of decision making are most important in today's real combat. This gave impetus to the development of the concept of network-centered military activity.

The issues of systematic disruption of government and the functioning of the state were proposed and implemented during the preparation of Operation Desert Storm in 1991 by Colonel US Air Force. He

developed a systematic, cybernetic approach to modern combat operations, calling it "effect-based operations" that took into account J. Boyd's developments and further developed the cybernetic concept of a network-centric organization of actions with elements of systems restriction theory. According to this concept, there are five main segments: the armed forces, the population, infrastructure, life support systems, military and political leadership - vital to any state. Each state has its unique places in them - vulnerabilities ("centers of gravity". Their correct identification and destructive impact on them leads to the effect of systemic "paralysis" of the state in certain spheres or as a whole.

The central ring of such a system is its most vulnerable object (Fig. 1). Less vulnerable objects in degree, but no less important in value are closer to the outer ring. It is worth noting that J. Warden states that each component has its centers of gravity [10].

Impact on such centers causes changes in the management processes of the objects of influence and consequently affects the whole system. Typical of such a theory is that the degree of influence of the center of gravity on the whole system depends on the degree of its closeness to the central ring. According to J. Warden's theory, the objects of influence are the connections between the rings and the connections within the rings themselves. Thus, the differentiation of subjects or objects of influence on the rings allows them to identify those that are related to the critical cybernetic infrastructure. It is this differentiation that allows them to be perceived as a coherent whole. This ensures that objects (entities) with critical cyber infrastructure are first exposed and then broken. And the tools or means of influence are political, informational, economic and military, which affect objects or centers of gravity.

At the heart of J. Warden's model is the state's military and political leadership, national leaders, which are a critical component of the national security architecture and surrounded and protected by four other rings. The second ring is the system of life support, production, factories, banks, which during the war are vital for the functioning of the military-industrial complex. State infrastructure - roads, railways, power lines - create a third ring. The fourth ring is the society (population), and the last, fifth outer ring is the armed forces [7, 10].

This model is implemented as the scheme "war from the middle to the outside." However, the US scheme works well in conflict zones where the armed forces are viewed by the local population as an external aggressor.

In contrast to this model, Russia has for a long time received support from the local population in the Crimea and significant military formations of the Black Sea Fleet, which were never perceived as an enemy (Fig. 2).

Russia has exerted a long-lasting and consistent influence on the population of the ARC in order to perceive Russian servicemen as defenders of the population and to correct a "historical mistake" regarding Crimea's belonging to Ukraine. Then began to exert influence on the leadership of the Autonomous Republic of Crimea and the city of Sevastopol, and after that - mass information and psychological influence on the personnel of the Armed Forces of Ukraine. The main objects of the transport infrastructure and the life support system were taken under control. The efforts of the Russian Federation to launch a campaign for the introduction of the Armed Forces into the Crimea were accompanied by actions that had all the characteristics of an information and psychological operation prepared and thought out for the purpose, measures and consequences of an information and psychological operation aimed primarily at a Russian audience and, on the other hand, Ukrainian and Western audiences [6]. , 11, 12].

The "hybrid war" tactics applied by Russia in the Crimea were also extended to the southeastern regions of Ukraine (Fig. 3).

The main impact was focused on populated regions. The next influences were government infrastructure and life support systems, respectively. The fourth and fifth circles of influence were the Armed Forces and the military-political leadership of Ukraine [11, 13].

The peculiarity of conducting information-psychological operations in Russia in the south-east of Ukraine is the constant search and use of up-to-date information drives capable of forming the necessary civic opinion. Recently, there has been a tendency to expand its influence on areas previously uncharacteristic of information confrontation, namely the revision of the history of statehood of Ukraine and Russia and interconfession relations.

It should be noted that the information war against Ukraine is aimed not only at loosening the situation inside the country, but also at creating a negative image of Ukraine in the world. This process started in 2005 during the first gas war. At the time, Ukraine was successfully portrayed as a dishonest, and at least dubious, gas transporter, despite the fact that for decades Ukraine had never allowed the disruption of natural gas supplies to Europe. Significantly, at the same time as these accusations, Russia emphasized the need to build gas pipelines alternative to the Ukrainian system. In addition, Ukraine's allegations of gas theft were not substantiated by specific facts [14].

It should be noted that in recent years Ukraine has become the target of powerful information attacks from Russia. Among the most striking examples of such a war is the imposition of the idea of federalization, giving the Russian language the status of a second state language. At different times the list of leading topics, such as the problems of the Black Sea Fleet, the problems of the fuel and energy complex, the problems of the Crimea, as well as the activities of political organizations such as the Right Sector, UNA-UNSO, changed.

For the first time, Ukraine was defeated in this war by spreading and misrepresenting that Ukraine was incapable of holding and servicing nuclear weapons, resulting in Ukraine voluntarily losing its nuclear status, losing its influence in the international arena.

And then there were the cluster scandal, gas wars between Ukraine and Russia, allegations of selling Kolchug to Iraq, and weapons in the Russian-Georgian war. It should be noted that in the years of independence, Ukraine has never worked ahead, took an active position, and always defended itself against information and psychological attacks.

It should be noted that what has been done by Russian media technologists on the territory of Ukraine in recent years has often not been considered as a threat to national security, and the demand of the Ukrainian population for Russian television programs has not caused fears of the Ukrainian authorities that their review will eventually lead to destructive and destabilizing influence on the consciousness of citizens, and through their consciousness - to change the attitude towards Ukraine itself.

And it is really clear that Russia does not spare the finances for the information war, provides information that the state is falling apart, that Ukraine is run by radicals, fascists, “Banderas”, Nazis, junta, who are committing mass riots, vandalism, and the most terrible - they are killing people on the streets, burning Communist houses , "Regionals" and Russian-speaking citizens.

Today the Russian-Ukrainian information war is open. However, Russia also conducts information attacks and actions against other states.

Yes, advocacy companies were previously seen as an ideological tool for promoting concepts. For the first time, Russia's propaganda campaign was also viewed as promoting the idea of a Russian peace. The new quality is that it is not only an advance of ideology, but also a tool of war. In addition, it was not clear until recently what Russian propaganda was. Now the picture has cleared up, it is a multifunctional tool with the highest level of expertise, which involves not only trolls operating in Europe, the US and most in Russia, but also a large group of experts who perform in-depth analysis of

urgent situations and respond very quickly to them. And it is an analysis of both psychological, political and military.

Only now have the European Union countries begun to wake up. They began to realize that in 1981 they had practically completed their activities to counteract the Soviet Union on the information front.

The House of Lords of the British Parliament noted that intelligence and foreign policy analytics of the West had lost the war to Russia, underestimating the directions of its development, and only events in the Crimea and the Donbass made it possible to understand that nothing had changed. Russia has inherited the entire system of the Soviet Union and very well uses information as an element of state power, while the West has actually disarmed itself.

In addition, it appears that the influence on the Western media and institutions is actually exercised by Russia. It also bribes tens of millions of dollars from journalists and European politicians. And this is without taking into account projects that have been converted into propaganda tools - television, radio, newspapers, online publications, as well as a large number of institutes operating in the USA, Europe and other places. In addition, individual arrangements and agreements with lobbyists.

Therefore, the SERA project was created in the European Union to identify information-psychological attacks and impacts, control, collect, analyze and repel or to bring Russian propagandists to the clean water in Europe. The program brings together leading journalists, activists and media analysts from European countries who use their expertise to develop an analytical tool to effectively address Russian misinformation at the strategic, conceptual and institutional levels [15].

Thus, an incredibly powerful information war is being waged on Ukraine. Therefore, it is necessary to develop a strategy and tactics for fighting in the information field.

In addition, it should be borne in mind that in modern conditions the nature of the armed struggle has changed significantly - it has become a "hybrid war".

The emphasis of the armed struggle is shifting towards the practical implementation of information technology. At the same time, information and psychological operations, attacks, actions and actions are becoming increasingly important in achieving political and military goals.

Underestimation of the capabilities of information and psychological weapons, counteracting influences and features of a particular territory can be fatal in the further aggravation of the military and political situation around Ukraine.

REFERENCES

1. Korolko, VG. 2000. “Fundamentals of Public Relations” - M. - K .: Refsl-beech - Wackler. - 528 p.

2. Sun Tzu. 2002. *Treatises on military art.* - M: LLC ATS Publishing House, St. Petersburg: Tezza fantastica. - 260 p.

3. Guz, A.M. *History of information protection in Ukraine and leading countries of the world*. 2007 - K: CST. - 864 p.

4. K. von Clausewitz. 2007 *On war* - M: Exmo. - 260 p.

5. Belska, T.V. 2014. “Information-psychological war as a way of influencing civil society and public policy” / TV Belska // *Technologies and mechanisms of public administration,* no. 3.: 49-56.

6. Zelinsky, S.A. 2008. *Information-psychological impact on the mass consciousness*. - St. Petersburg: Scythia. - 403 p.

7. Pirtskhalava, L.G. 2019. “Information confrontation in modern conditions: a monograph” / LG. Pirtskhalava, V.A. Khoroshko, Yu.E. Khokhlacheva, M.E. Shelest - To: Comprint CPU, - 226 p.

8. Spyga, P.S. 2014 “Fundamentals, technologies and patterns of information war” / PS Spiga, R.M. Rudnik // Problems of International Relations, vol. 8, - p. 326-339.

9. Danik, Yu.G. 2018. “High-tech aspects of national security and defense” // Communications and Networks. Telecom, October - p. 58-69.

10. Grischuk, R.V. 2010. *Fundamentals of Cyber Security* - Zhytomyr: ZhNAEU. - 636 p.

11. Pevtsov, G.V. 2015. “Information-psychological operations of the Russian Federation in Ukraine: models of influence and directions of counteraction” *// Science and Defense*, no. 2: 28-32.

12. Tolubko, V.B 2004. *Information security of the state in the context of combating information wars*. - K: NAOU,. - 176 p.

13. Gorbulin, V.P. 2017. World Hybrid War: The Ukrainian Front / For the General. - K: NISD,. - 496 p.

14. Magda, E. 2014. “Challenges of hybrid warfare: information impact” // *Scientific Notes of the Institute of Legislation of the Verkhovna Rada of Ukraine*, No.5: 138-142.

15. SERA. n.d. “Information and psychological confrontation in Ukraine” Accessed on January 21, 2019
http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/14459