MAIN CRITERIA FOR CLASSIFICATION OF THE TYPES OF INFORMATION CONFRONTATION

KRASOVSKAIA NATALIIA RUDOLFOVNA

Krasovskaia Nataliia Rudolfovna - Phd in Psychology, independent researcher, Moscow, Russia. Research interests areinformation warfare, behavioral warfare, mass consciousness manipulation, and gender studies. Author of more than 40 scientific publications. Contact details: e-mail goulina@gmail.com, +79134673984

GULYAEV ANDREY ANATOLYEVICH

Gulyaev Andrey Anatolyevich - Phd in Philosophy, Associate Professor, Lecturer at "K.G. Razumovsky Moscow State University of technologies and management" Moscow, Russia. Research interests are information warfare, behavioral warfare, mass consciousness manipulation, political and sociological research. Author of more than 20 scientific publications. Contact details: e-mail: andrey.gulyaev1966@yandex.ru, +79588154877

Received: May 2018. Acceptance: September 2019

The article discusses the grounds for the classification of the information confrontation types. A comparative analysis was used to consider psychological operations conducted in the information space. The various bases of psychological confrontations have common points that unite them into a single whole. As a result of the study, it was possible to identify the most typical grounds for the classification of information wars, determine the classification criteria and highlight their main types. The authors proposed an original approach to the classification of information wars on geographical basis. System analyses was one more method used in the study. Terms such as informational operation, informational impact, psychological warfare, behavioral warfare and cyberwarfare are the elements of a system to describe information warfare. The use of various methods in the study allowed to identify the basis for the classification of information wars.

Keywords: *information war; information operation; psychological war; behavioural war; cyberwarfare.*

Word Count: 4999

Information wars have a long history, but only recently, they have become an object of research. The article aims to examine various classifications of information warfare, also comparing the Russian and Western approaches.

Definition of the information war

An American sociologist and psychologist Harold Lasswell is one of the pioneers of the research on the issue of information wars. He considered propaganda almost the most effective weapon in the modern war, to which in his opinion the First World War belonged. "The conduct of war, conceived as a psychological problem, may be stated in terms of moral. A nation with a high moral is capable of performing the tasks laid upon it." (Lasswell 1929, p. 27) In his book "Propaganda Technique in the World War", he examines different methods of propaganda, which raises the morale of country's own population and lowers the enemy's one.

The single and universally recognized definition of the information war does not exist nowadays. Nevertheless, it is obvious that the information warfare is a very complex and multifaceted phenomenon. In our work, we examine information war only in the context of confrontation of states, societies and geopolitical systems. While formulating the definition, it is necessary to take into account all factors of that confrontation, the purpose of which is to achieve an undeniable advantage over the enemy by obtaining, processing and using different information.

Russian scientist A.V. Manoilo suggests to characterize information war as an information activity undertaken by a political entity (for example, state) to weaken and destroy another political entity; as an information battle between competing rivals; as an informational military conflict between two mass enemies, for example armies (Manoilo 2003, p.9).

According to the definition, proposed by the researcher G.G. Pochepcov: "Information warfare is a communicative technology aimed to impact the mass consciousness with short and long-term goals. The goal of the impact is to make changes in the cognitive structure in order to obtain appropriate changes in the behavioral structure"

(Pochepcov 2001, p.20). In our opinion, this definition in the best possible way reflects the psychological aspect of information wars, which can be distinguished as a separate class of information wars - "psychological warfare" (Pochepcov 2000, p.14). The term "psychological warfare" is closely related to the word "propaganda" and can be interpreted as a "propaganda warfare".

Approaches to classification of information wars

It should be acknowledged that classification of the term "information war" is quite ambiguous. In our work we deal with the problem of classifications of information wars. On what reasons and for what, types and subtypes information wars can be classified?

It is important to mention the difference in the approaches of Russian and Western researchers in studying the problem of information wars. Russian scholars consider the concept of "information warfare" more broadly, as an information confrontation, including propaganda confrontation, psychological and manipulative influence, information operations (for example, information theft and disinformation), as well as cyber warfare. In doing this, Russian scholars emphasize the first aspect of the concept of "information war" - the war for the minds of people (psychological warfare), while Western scholars mainly consider the information war in a narrower militaristic dimension, as a cyber war. In the latter case, the information war or cyberwar is a military strategy aimed at creation of unfavorable situation, in particular, by disabling enemy's computers that control the vital functions of state or a separate company, intercepting and distorting information, introducing viruses, tabs and logic bombs. This understanding of information warfare is typical for American researchers Cronin and Crawford. They note the future superiority of the "digital David" over the "armored Goliath". Moreover, these researchers note the public-civilizational context of the information war, which includes "propaganda and disinformation" (Cronin and Crawford 1999, p.260). A classic example of this approach is the propaganda efforts in the American media against the regime of Saddam Hussein in 2003 and the demonstration in the United Nations of a substance in a test tube, a so-called sample of the chemical weapons that Iraq had. Thus, it is typical for the Western specialists to consider the information war, firstly, as a separate type of military operations and, secondly, as a propaganda preparation for them.

Another Western researcher Martin Libicki, who is considered as one of the first theorists of information wars, defined information wars as an informational impact, that has elements of protection, manipulation, distortion and refutation of information. M. Libicki also proposed the first classification of forms of information measures (information warfare) (Libicki 1995):

- Command and control - the impact is directed to communication channels between the command and the subordinated troops, depriving them of the opportunity to maintain control and coordination of actions;
- intelligence - the impact in which the collection and protection of information of military importance is carried out;
- electronic warfare - under this influence, electronic means of communication and computer equipment are disabled;
- psychological warfare - psychological manipulation of the population in the enemy's territory using information, the analogue of "brainwashing";
- hacker warfare - exposure through computer viruses, carried out by specialists of the appropriate field whose actions lead to communication failures;
- economic- information warfare - blocking of trade channels, information blockade;
- cyber warfare - actions similar to hacking, but for a different purpose, namely with the purpose of capturing information.

This classification given by Libicki is too cumbersome; some items can be combined, for example, electronic countermeasures and cyberwar.

D. Denning proposes to divide the information war by its nature into offensive and defensive (protective) (Denning 1999). This underpinning for the classification of information wars can be considered one of the most important.

From the perspective t of sociologists Yu. Surmin and N. Tulenkov, information wars are divided into:

- information aggression, implying the destruction of the enemy's information system and the imposition of another value system;
- information expansion, which is based on a long evolutionary impact, through its own information means in order to subordinate the enemy;
- Information and psychological civil war, which involves confrontation of various social groups within society itself.

Also Yu. Surmin and N. Tulenkov propose to distinguish the following types of information wars according to the subject of the conflict:

- the psyche of the enemy's population is the subject of psychological warfare;
- the system of information communications is the subject of the communication war;
- the struggle for acquisition of information is an information war;
- political, spiritual, ethical and other values are the subject of a value or a worldview war (Surmin and Tulenkov

2004, p.113).

The drawbacks of this classification include the confusion of the basis on which classification is made and the insufficiently persuasive division of notions, for example, “aggression” and “expansion.”

However, it should be noted that in recent years the term “information warfare” is often replaced by the term “information operation”. Many Western researchers note that in wartime information warfare is a war in the literal sense of the word, i.e. a mode of combat. In peacetime, the notion of “information operation” is more suitable for information warfare. Thus, experts call for classifying the information war into two types based on such an important basis as a “peace / war time”.

Information operations also have their own classification, proposed by V.G. Krysko:

1. Psychological operations: a planned information and psychological impact on the population of foreign countries, whose goal is to evoke the desired emotional response, to change motivation and internal goals, to make necessary adjustments in the actions of government, public and other organizations, various groups and citizens.

2. Disinformation operations: actions for deliberate misleading of decision-makers, which should induce the enemy to take steps in line with the objectives of the initiator of the operation.

3. Counterintelligence or security operations: actions to identify critical information for implementation of military, political and economic activities, as well as fields that are vulnerable to the enemy’s intelligence and his operations.

4. Electronic confrontation: –military action, in which electromagnetic radiation or other techniques are used, to control the electromagnetic range or the goal of defeating the enemy is achieved.

5. Operations in computer networks, including network attacks, protection of computer networks and assistance activities aimed at collecting and analyzing information about the enemy’s computer networks and methods of organizing network attacks (Krys’ko 1999, p.96).

This classification represents a certain step forward, but it is not deprived of any shortcomings. For example, the point 4 is necessary to be removed as not conforming to this classification.

As can be seen from the above classifications, nowadays information wars are actively studied and classified from the perspective of political, military and technical sciences. However, there is not enough research in psychology, although the impact of information wars is achieved using psychological methods. It is necessary to deeply and thoroughly study the tools used by the enemy in order to create an adequate counteraction system.

In our opinion, the classification proposed by V. Ovchinsky and E. Larina is interesting, as they distinguish three main types of information wars. The first type is mental (psychological) war that actually represents wars of content, purpose of which is to change the consciousness or psyche of masses, groups and / or personality, i.e., the object of influence is values and attitudes (Ovchinskij and Larina 2015, p.25).

American scholars Lazarsfeld and Merton propose to distinguish mental (psychological warfare) into two types - conducted in the war and peacetime. So, in peacetime, the psychological war gains features of a psychological operation. When conducting a psychological operation, information flows must be controlled through formal means, the media, educational structures, social networks, etc., as well as informal means, distributed through rumors, opinions, etc. Use of the leaders’ opinion plays an important role, as it has a determining influence on the formation of opinions within the group. P. Lazarsfeld’s multistage information flow concept serves as a model in this approach (Lazarsfeld and Merton 2004).

The second type of information war by V. Ovchinsky and E. Larina is cyberwar, considered by the author of the work “Against all enemies”. : - Cyberwar – a system of actions of one state with the purpose of penetrating into the computers or networks of another state to cause damage or destruction. The famous American specialist R. Clark regards cyberwar as a separate type of the information war, essentially identical with military actions (Clark 2011, p.48).

Another Western scientist P. Cornish offers the following classification of cyberwar. Cyberwar consists of cyber attacks, cyber defense and espionage. The cyberattack is targeted at information systems supporting functioning of power, industrial, military and other facilities, as a result of the attack they fail. The cyber defense involves the possibility of repulsing the enemy’s cyberattacks. Espionage is aimed at the extraction of useful information and penetration into the enemy’s information system. It is also proposed to classify cyberwar into two types: 1. State cyberwar; 2. Private cyberwar. State cyberwar is conducted under the aegis of the state and means that the state (group of states) has declared or continues to declare war to another state (group of states). Private cyberwar may be initiated by an individual (a group of individuals) or a private non-state organization against state, economic institutions (Cornish 2010). The difficulty of the latter classification lies in the fact that, for example, a state-sponsored cyberattack can be carried out by a private structure and it is extremely difficult to establish their relationship. According to the American journalist and writer Sh. Harris, cyberwar can accept a variety of hybrid forms (Harris 2016, p.78).

The transition from a trivial information war to a cyberwar is threatening by its unpredictable consequences. Therefore, certain rules and restrictions must be developed in a collective way with the help of the international community and adopted at a conference like the Hague Conference of 1899 and 1907.

Finally, according to V. Ovchinsky and E. Larina, the third type of the information war is behaviuoral war - it is based on technologies of manipulation of behavioral algorithms, habits, stereotypes of activity imbedded into us by the society. The toolkit of behavioral wars is used to to separate the habit from the established type of the activity that shaped the situation, and use behavioral patterns to achieve other goals. Yet the theme of "behavioral" wars, their essence, content and, most importantly, practical methods of implementation are tabooed to the great extent. It is kept secret in the global information space, covered with powerful media information noise, which present this topic, either as another conspiracy scarecrow or proves the technological impossibility of conducting this type of war. But here is an example: out of 500 supercomputers in the world, 233 are in the USA. For comparison, Russia holds the ninth place with 8 supercomputers. For what purposes such powerful computing power and data storage is needed? The most plausible explanation for the emergence of such excess computing power and storage is their use to implement technologies for the formation and management of human behavior.

As M. Kaldor points out, the example of some modern Asian and African states, on whose territory civil wars do not cease for years and even decades simultaneously with the interference of other states, is not unique. In principle, the same fate can await any other state (Kaldor 2015, p.197). As Western researchers note, behavioral weapons serve as means of behavioral warfare. It is based on technology, called "nudge" (from English nudge - "pushing"). Its essence is simple - using habits and stereotypes, by creating certain situations, you can push a person or a group of people to make certain decisions and implement certain actions based on them. In fact, we are talking about a new programming technology and external management of human behavior (van Creveld 2005, p.236).

US military experts are introducing another type of the information war - network-centric wars. The US military theorists A. Cebrowski and J. Garstka developed the concept of «network-centric warfare» in the late 90s of the last century. At the heart of the network-centric war lies an increase in the total combat power of military formations by combining them into a single network. This network has two main features: speed of control and self-synchronization. The speed control is achieved through information superiority by the introduction of new control systems, tracking, intelligence, control, computer modeling. As a result, the enemy is deprived of the opportunity to conduct effective operations, because all its actions will be delayed. Self-synchronization refers to the ability of the organizational structure of military formations, the forms and methods of accomplishing combat missions, to be modified at its discretion, but in accordance with the needs of the higher command. As a result, military actions take the form of continuous high-speed actions (operations, campaigns) with ambitious goals. Thus, the network allows geographically dispersed forces (related to different types and kinds of troops) to be combined in a single design of the operation and at the expense of information superiority. It aims to use these forces with greater efficiency by ensuring the unity of views of the leaders (commanders) of the various troops (forces) and the place of interaction in the operation, as well as by self-synchronization of their actions in the interests of achieving the overall goal of the operation (Cebrowski and Garstka 1998).

This description emphasizes the properties of network-centric warfare as manifestations of cyberwar. Therefore, we cannot distinguish the network-centric war as a separate type of information war and consider it a kind of cyberwar.

We propose to supplement a given classification of information wars by introducing a territorial feature. It is very important to determine the territories on which the information war is conducted relative to the source of information impact, since the goals and objectives of information wars being conducted on its own population as an object of influence and the population of the enemy's country as the object of influence will differ fundamentally. Using this base of classification, it is first necessary to distinguish types of territories:

- external in relation to the source. In this case, the population of the enemy country or population of neutral countries will be the target of impact.

- internal territories. In this case, the population of the country to which the source belongs will be targeted.

Let us consider objectives of the psychological impact according to this division of information wars on territorial basis. When the population of the enemy's country is affected, the following types of mental wars can lead to a gradual weakening of the enemy's country:

1. Psychological / propaganda war. The goal is to change the picture of the world and the attitudes of the target object, that is, the population of the enemy's country. In this case, information is broadcasted in the territory of the enemy's accessible communication channels and as a result, the necessary public opinion desired by the initiator of operation is created. Public opinion, in turn, can impact the adoption of political decisions by the elite of the state. It also influences the behavior of the population, both its active forms (protest peace actions or, for example, actions to prepare for emigration), and passive forms (apathy, inaction, lack of planning for the future and actions to achieve previously set life goals), which, of course, leads to further weakening of the enemy's country.

The psychological warfare of some media on Russian territory can be used as an example. In the 1990s, a lot of media in Russia belonged to oligarchs. Instead of a healthy pluralism of opinions and discussions, based on norms of civilized society, patriotism acts as a natural feeling and conviction of the citizens, the oligarchic and clannish media conducted a rampant denigration of Russian reality. It resulted in citizens' melancholy and depression, lack of self-confidence and shame for their own Homeland. Over the past 15 years in Russia individual organizations and individuals adopted similar function of discrediting the whole of Russia. Often the sources of such communication are popular media persons, bloggers, etc.

The manifestation of a psychological war is a value-based (ideological) war. There is a term "consciental war", but, in our opinion, it is not precise enough. The consciental war assumes that the impact is on the mind of a person, changing it. In our opinion, the impact is three-level in this type of the war:

- distortion and destruction of the value system;
- destruction of identity;
- formation of a new identity.

The changes in consciousness are secondary to these processes.

An example of the destruction of the old and the imposition of a new identity are the events taking place on the territory of Eastern and Central Ukraine during 2014 - 2018. The glorification of Nazi collaborators of S. Bandera and his accomplices, tolerance and acceptance by a part of society of the far-right radical nationalism of West-Ukrainian origin led to large-scale changes in mass consciousness in Ukraine. These changes form a new "Banderite" identity that is completely incompatible with the traditional identity of Eastern Ukrainians.

On a microscale, an example of a value-identity war is recruiting conducted by ISIL (banned in Russia).

On a society-wide scale, such a war nearly ended with the defeat of Russia after the collapse of the Soviet Union. And the dramatically increased mortality, was caused among other factors by the fact that part of the population could not go through to the third stage, losing their values and identity. People simply perished by launching self-destructive processes, passive (psychosomatic) or active (self-destructive behavior).

2. V. Ovchinsky and E. Larina distinguish the behavioral war separately. It is also conducted, first of all, on the territory of the enemy. By collecting and analyzing large data, patterns of behavior and trigger processes are identified. By using the "stimulus-response" connection, appropriate stimuli are selected that cause the revealed reactions in other conditions that are not similar to the original ones, which makes it possible for the source to gain an advantage. At present, this type of information impact on indirect data available in open sources is being actively developed in the United Kingdom and the United States. To a certain extent, this kind of warfare can be attributed to "color revolutions", when disinformation and provocative actions lead to the active-aggressive reaction of the masses and trigger the process of confrontation with the power structures. It results either in overthrow of the existing power or bloody suppression of unrest. In any case, it sharply weakens the position of the enemy's country in relation to the source of information impact. Information, reinforced by the impact of strong emotions, is spread and used at the local level in a variety of ways to increase the degree of "mobilization outrage". Distribution of such information in social networks is carried out by means of SMS, local blogs, images and video films, for which cameras are used on mobile phones, for example.

3. The goal of external mental wars, the targeted object of which is the population of neutral countries, is to strengthen the influence of the country-initiator of the attack on the population, including the political elite of a neutral country, whereby the enemy's country is weakened in the future. The objective of such war is to destroy contacts of the country whose population is affected, with the country-opponent of the source of information impact at all possible levels, from the political to the everyday.

In this situation, the war is primarily conducted through information attacks in the media, using Internet channels and personal impact with the transfer of information (international events, forums, conferences), which result in the formation of negative public opinion and leads to a reduction of contacts. Reducing contacts is the basis for minimizing the flow of objective information, creating barriers to the use of soft power tools, increasing economic isolation, etc. It creates opportunities for strengthening the influence of the source of information impact on the society of the country. An example of such a war is the actions of the collective West in the territory of the countries of the former USSR on the formation of a negative image of Russia.

Another vivid example of the effect of reducing the number of contacts with representatives of a country that is an adversary in the information war through information impact was a creation of a negative image of Russia in order to minimize Russia's visit to European countries. "FIFA and the organizing committee reported that 700,000 FanID (special document, without which it is impossible to get to the stadium during the match) is given to foreign fans. China (60,000) is the leader in the list of states that delegated, followed by the United States (49,000), Mexico (43,000), Argentina (35,900), Brazil (32.000), Colombia (29,000) and Peru (26,000). Of all the European countries, only Germany (28.6 thousand fans) managed to squeeze into this list. But, for a correct comparison, it is worth remembering that about a million foreign tourists arrived in South Africa in 2010 for the World Cup. Four years ago, 1,015,035 foreigners arrived in Brazil. Of course, most of them in 2014 were residents of neighboring countries with Brazil and the United States, but after all, most of the football tourists came to Russia from there. On closer examination, it turns out that 700 thousand is not a miracle and not a record, but rather an ordinary indicator. A call for a boycott and terrible stories in the media played its role - European teams were half of the tournament participants, European fans in terms of income are not inferior to Latin American. Much more Poles, Belgians, Swedes, Spaniards and Englishmen were supposed to come to Russia but preferred to stay home.

Contrary to the established opinion, to manipulate an educated person proficiently is more easy. The manipulator in this case will more accurately achieve the goal, since an educated person will be a more effective tool in the hands of the manipulator. This requires non-standard, creative approaches in the formation of such information and the ways of its distribution in order to penetrate into the consciousness of the manipulated educated person and push him/her to the desired behavior. Often a method of comparison is used - "they" (usually in the West) are compared to "us". Such comparisons usually do not withstand any criticism, since they are extremely incorrect.

With the advent of modern media, social networks and other Internet platforms, the opportunities for information wars have grown many times. Fake news, thousands of reposts of unverified information, provocative videos in YouTube, etc. can blow up stability and consolidation in society. Modern "color revolutions" have been already largely the offspring of Internet platforms.

For the war on internal territories (the second type) the impact is on the population of its own country, the key goal is to create the basis for political decision-making - the formation of public opinion and the creation of conditions so that this public opinion is not subject to correction with the reciprocal influence of the enemy.

An example of the creation of the negative public opinion in the conduct of psychological warfare on its own territory is the war against the Taliban movement on the territory of Afghanistan. To prepare for a decision on the invasion of Afghanistan, the US population was actively processed by the leading media.

Conclusions

Information wars exist for long time and became comprehensive in the era of the distribution of media (newspapers, magazines, radio, television) and general literacy. But the comprehensive research on such wars is just developing. The article examined how modern scholars conceptualize and classify various types of information wars.

Most classifications in the modern literature dwell on the political and technological platforms. We note that it is very important to account for a psychological aspect of the information warfare.

Psychological war has three directions: in relation to its own population, neutral population, the population of the country - the enemy.

Each kind of information warfare has its own types. The psychological war involves a mental war and a behavioural war. Both kinds can act in two qualities - attacks and defenses.

Information wars have actually become an integral part of our lives. The sophistication of the methods of influence will only increase, which makes the research of this problem highly relevant and necessary to be studied further from various angles, including from the point of view of psychology. It should be identified what tools are used in this field, methods of suggestion and manipulation. It is needed to develop adequate countermeasures.

References

1. Cebrowski, A. and Garstka J. (1998) «Network-Centric Warfare: Its Origins and Future», Naval Institute Proceedings, January, USA.

2. Cronin, B. and Crawford, H. (1999), «Information Warfare: It's Application in Military and Civilian Contexts», The Information Society, 15 (4), October, pp.257-263.

3. Denning, D. (1999), Information warfare and security, Boston, USA.

4. Harris, S. (2016), Cyberwar: fifth theatre of war. Trans. from Engl. [Kibervojn: pyatyj teatr voennyh dejstvij. Per. s angl.], Al'pina non-fikshn, Moscow, 392 p.

5. Kaldor, M. (2015), New and old wars: organized violence in a global era. Trans. from Engl. [Novye i starye vojny: organizovannoe nasilie v global'nuyu ehpohu. Per. s angl.], Izd-vo Instituta Gajdara, Moscow, 416 p.

6. Clark, R. (2011), Third world war. What it will be Trans. from Engl. [Tret'ya mirovaya vojna. Kakoj ona budet. Per. s angl.], Piter, SPb, 336 p.

7. Kornish P. (2010), On Cyber Warfare, The Royal Institute of International Affairs, London, UK.

8. Krys'ko, V.G. (1999), Sekrety psihologicheskoj vojny [The secrets of psychological warfare], Harvest, Minsk, 208 p.

9. Lasswell, H.D. (1929), Propaganda technique in the World War Trans. from Engl. [Tekhnika propagandy v mirovoj vojne. Per. s angl.], Gosudarstvennoe izdatel'stvo: otdel voennoj literatury, Moscow, 200 p.

10. Lazarsfeld, P. and Merton, R. (2004), Mass Communication, Popular Taste, and Organized Social Action, New York, USA.

11. Libicki, M. (1995), What is information warfare?, Washington, USA

12. Manoilo, A.V. (2003), Gosudarstvennaya informacionnaya politika v osobyh usloviyah [State information policy in special conditions], MIFI, Moscow, 388 p.

13. Ovchinskij, V. and Larina, E. (2015), Mirovojna. Vojna vsekh protiv vsekh [World. The war of all against all], Knizhnyj mir, Moscow, 83 p.

14. Pochepcov, G.G. (2001), Informacionnye vojny [Information war], Refl-buk, Moscow, 576 p.

15. Pochepcov, G.G. (2000), Psihologicheskie vojny [Psychological warfare], Refl-buk, Moscow, 528 p.

16. Surmin, YU.P. and Tulenkov, N.V. (2004), Teoriya social'nyh tekhnologij [Theory of social technologies], MAUP, Kiev, 608 p.

17. van Creveld, M. (2005) The Transformation of War. Trans. from Engl. [Transformaciya vojny. Per. s angl.], IRISEHN, Moscow, 344 p.