DOI: 10.46340/eppd.2020.7.3.6

Kateryna Sylantieva-Papp
ORCID ID: https://orcid.org/0000-0002-2815-4429
Uzhhorod National University, Ukraine

THE FOURTH-GENERATION WARFARE ORIGIN

This research analyzes the development of the fourth-generation wars. The creation and the basic tendencies of the functioning of information and network-centric wars are revealed in detail. Armed prosecution of war tended to pale into significance in today's society; the primary tool now is hybrid warfare, which combines psychological, ethical, moral and information factors. Elements of hybrid aggression include certain strategic communications, misinformation, economic blockade, illegal cyber-sphere operations. New technologies and methods of hybrid warfare have become a challenge to international security. Information and network-centric wars are referred to as the most significant part of a hybrid war.

Keywords: hybrid warfare, network-centric warfare, information wars, aggression.

The whole history of humanity is mainly the history of wars and armed conflicts. According to scientists over the last 5.5 thousand years, there were about 14.5 thousand of major and small wars. In addition to that, the wars were different, and accordingly, the theories of wars were also different. The war has a long evolution. Today there are four generations of such evolution. In the first-generation wars, the linear tactics of warfare were used with the usage of smoothbore firearms. The example of which is the war of the XVI – the first half of the XIX century.

The second-generation wars used methods and forms of positional warfare with the mass usage of rifles and human power. Machine guns were used, massive shelling was carried out, and the first models of weapons of mass destruction were developed and used. Despite the predominantly positional, trenchant nature of the war, the railway usage is widely spread, enabling the high mobility of troops to essential areas of the front. Examples of the-second-generations war are the Civil War in the United States (1861-1865) and the First World War (1914-1918).

The third-generation wars used armoured vehicles and aircraft, which made it possible to manoeuvre warfare at the tactical and operational levels. Besides, weapons of mass destruction (chemical, bacteriological, and nuclear) became widespread. The first attempts to use climate and seismic weapons took place that days. Examples of this generation wars are the Second World War (1939-1945), as well as some armed conflicts during the Cold War (1946-1989). Immediately after the Second World War, the doctrine of nuclear war was adopted in the United States that was subsequently reflected in all official US and NATO strategic concepts. The military doctrine of the USSR also emphasized the decisive role of missile and nuclear weapons in the war. The first stage considered the possibility of a general nuclear war, characterized by unlimited, massive and concentrated use of all nuclear weapons for military and civilian purposes. However, it was probable that the resolution of such a war would lead to the death of human civilization, so in the second half of the 1950s, the concept of limited nuclear war was put forward by the United States. Later, such a conflict came to be seen as an armed struggle with the usage of various weapons, including tactical and operational-tactical nuclear weapons, the application of which was limited in scope, area and types of nuclear weapons. Nuclear weapons, in this case, are used to defeat the most critical military and military-economic objects of the enemy.

In 1961, as the USSR increased its nuclear capabilities and formed a roughly equal balance of forces, the US leadership switched to a flexible response strategy – the admissibility of using nuclear weapons not only in total but also in limited military conflict. Furthermore, in 1971, the United States proclaimed a strategy of realistic deterrence (realistic intimidation) retained the basic principles of the former strategy but gave it high activity and flexibility in building up and using the US military and its allies.

However, we are interested in the of the fourth-generation warfare. These modern conflicts actively use neoteric high-precision weapon systems and information technologies. Now the battlefield extends to the information space (including the cybersphere). Combat operations are conducted mainly by small,

technologically equipped military units, and special operations forces widely used. Technological superiority of the enemy is crucial. Nuclear weapons play the role of a deterrent tool. The possibility of using seismic and climatic weapons is increasing. Hybrid and network-centric warfares are an example of such conflicts.

After the end of the Cold War, the dangers of the First World War diminished. In the modern war, the predominance of the moral and psychological factor thesis over the physical destruction of the enemy has become increasingly common. Modern war is an information war, and it could be won by those whose information systems developed better. The term "information warfare" was introduced in the mid-1980s in connection to the new tasks of the US Armed Forces after the end of the Cold War, and was formally enshrined in the US MOD Directive of December 21, 1992. Moreover, in October 1998, the United States Armed Forces introduced the "Unified Doctrine of Information Operations", which is a concentrated statement of the views of the US military leadership on the nature and organization of influence on the enemy's information resources and protection of their information resources from similar influences. The doctrine preface states, the ability of the US Armed Forces to "prevent or anticipate crises and conflicts in peacetime, as well as to win in wartime, depends crucially on the effectiveness of information operations at all levels of war and across the spectrum of armed hostilities."

Defining the specifics of the information war, US government security expert R. Clark introduces the term "cyberwar". By its definition, "cyberwar is the action of one nation-state to penetrate the computers or networks of another nation-state in order to achieve the objectives of causing damage or destruction"[1]. Also, the term information war is not used in the professional sphere; it is more publicists and replaced by the term information operations. The first works on studying the information war appeared in the 90s of the XX century. Thus, one of the first works was the work of US Air Force Colonel R. Szafranski.

R. Szafranski stated that the purpose of information warfare was the epistemology of the enemy. It is the knowledge that an opponent views as true or real. "At the strategic level, the goal of an 'ideal' information warfare campaign is to assert influence to the enemy's choice and, consequently, to his behaviour, without the understanding his acts came under by someone"[2].

R. Szafranski clearly formulates the critical issues of the information campaign:

– the information campaign correlation to the goals of the whole military campaign,
– the desired epistemological result (in what everybody should believe by the end of the campaign),
– definition of information campaign tools used to achieve the set goals.

The information war is about the process of how people think and how they make decisions. The term information war is related to the writings of T. Ron, who was a scientific adviser to the Department of Defense and the White House. Rhone defined information warfare as a battle of decision-making systems. Furthermore, this accent on the decision-making process remains topical to this day[3].

In 1994-1995, many works conceptually defining this subject came out. M. Libicki criticized T. Ron's approach for being too broad and including all kinds of informational influences to achieving the goal[4]. R. Szafranski saw the purposes of war as compelling the enemy to obey our will[5]. He is interested in controlling and shaping the enemy's behaviour by influencing his thinking and perception of the world. In 1995, Stein published a paper entitled "Information Warfare", where stated that "the meaning of information warfare is the human mind, especially one that creates vital decisions on war and peace, and one that performs crucial judgments about where, when and how to use the potential and capabilities of the strategic structures"[6].

---

[1] Szafranski, R. (1997). *Neocortical warfare? The acme of skill. In Athena's camp. Preparing for conflict in the information age.* Santa Monica.

[2] Szafranski, R.A theory of information warfare. Preparing for 2020. *Airpower Journal* <www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/szfran.htm> (2020, February, 12).

[3] Dearth, D.H. Rethinking the application of power in the 21st century. *Military Intelligence.* <www.fas.org/irp/agency/army/mipb/1997-1/dearth.htm> (2020, February, 25).

[4] Libicki, M. What is information warfare? *Information Warfare Site.* <www.iwar.org.uk/iwar/resources/ndu/infowar/a003ch01.html> (2020, March, 25).

[5] Libicki, M. What is information warfare? *Information Warfare Site.* <www.iwar.org.uk/iwar/resources/ndu/infowar/a003ch01.html> (2020, March, 12).

[6] Szafranski, R.(1997). *Neocortical warfare? The acme of skill.* Santa Monica.

The war in the Gulf of 1991 considered being the first information war, which had been described in P. Taylor's work[1]. There are also numerous works by J. Arquilla on the subject of information war[2]. J. Arquilla was the first to conceptualize all significant areas of information warfare. It includes the information strategy of the United States as a whole, cyberattacks, network wars and the fundamental understanding of information. The author influenced the whole US information sphere with his works.

Contemporaneously, E. Toffler affected the military and civilian "chiefs" by his works on the third wave. According to him, there are three stages of human development (three waves): agrarian, industrial and information. Hence, special attention is paid to the Third Wave Wars. He believed the commander using the strategy of the next stage wins. For example, Alexander of Macedon used an industrial-type strategy while fighting in the agrarian civilization.

M. Libicki, as a respectful scientist, was one of the very first researchers on this topic, and he is continuing to focus on this issue today. Except for special attention to the fake message placing in adversary decision-making systems, he offers to divide information into three categories[3]:

– crucial information that may be known by some (such as scout identity),
– crucial information known by significant number of people (such as war plans);
– non-crucial information (such as pizza orders).

The development of information technology will have different implications for these types of information.

M. Libicki has been working at the National Defense University for twelve years[4]. His main specialization is cybersecurity. He is one of the authors of the book "Internet Freedom and Political Space", which came to light in 2013. This research, commissioned by the US State Department, was focused on the problem of how the freedom of the Internet affects the relationship between civil society and government: if the governments become more open to the public as a result. The fascinating question is: how does online freedom affect offline political space? China and Russia's analysis show that online political mobilization is growing out of the non-political usage of the Internet. Another conclusion is that online information can trigger an information cascade. Non-democratic regimes do not know the level of their real support because citizens are afraid to show their disapproval. The Internet facilitates social protests by anonymously expressing opinions and coordinating collective action that can lead to a domino effect.

The work "Cyber deterrence and Cyberwar" by M. Libicki begins with the idea that cyberspace is an extraordinary type of space. Here the attack is carried out not by the generation of force but by the exploitation of the enemy's vulnerability. It is impossible to repeat the same attack because this type of login will be closed[5]. Herewith, he gives the following definition of strategic cyber warfare: "the cyberattacks campaign launched against the state and its society, first and foremost, but not only, targeting to influence on the behaviour of the chosen state." Libicki has repeatedly emphasized that cyberspace made by the human. As opposed to the city that is also created by the human, the cyberspace is easily changeable. This difference is essential. He also believes that emphasizing protection issues we put the cart (information protection) before the horse (task completion).

Another concept of the future armed struggle based on the use of information technology is the concept of network-centric war. Network Warfare is an emerging theory of war developed by the Office of Force Transformation, under the authority of Vice-Admiral Arthur K. Cebrowski and adopted by military leadership. Rethinking military strategy in the postmodern era led to the emergence of the concept of post-industrial or network wars in the United States. Arthur K. Cebrowski summarized the systematic presentation of the network war foundations. The ideological inspirer and influential advocate of this classic military strategy modernization line was Donald Rumsfeld, the US Secretary of Defense under George W. Bush, Jr.

---

[1] Taylor, P.M. (1995). *Munitions of the mind. A history of propaganda from the ancient world to the present day.* Manchester – New York: Moorcraft P.L.

[2] Arquilla, J., Ronfeldt, D. (1999). *The emergence of noopolitik. Toward an American information strategy.* Santa Monica; Arquilla, J., Ronfeldt, D. (1997). *Cyberwar is coming.* Santa Monica; Arquilla, J., Ronfeldt, D. (2001). *The advent of netwar.* Santa Monica; Arquilla, J., Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Santa Monica.

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

[4] Libicki, M. (1995). *What is information warfare?* Washington.

[5] Libicki, M. (2009). *Cyberdeterrence and cyberwar*. Santa Monica.

The theory of network warfare based on the fundamental division of the human history cycles into three phases: the agrarian, industrial and information epochs, each of which corresponds to specific models of strategy arising from sociological concepts: premodern, modern and postmodern. The information age is a postmodern period (today) when the developed societies of the West (first of all, the USA) are moving to a qualitatively new phase.

The new theory has been implemented actively in US warfare and has been already put into practice in Iraq, Afghanistan, and other countries successfully. Its technological approaches are tested on training and simulators. The developers of this theory convinced that if it does not replace the traditional theory of war soon, it will significantly and irreversibly change its quality.

The meaning of military reform under the information age "new theory of war" consists in the creation of a powerful and inclusive network that conceptually replaces former models and concepts of military strategy and integrates them into a single system. War becomes a network phenomenon, and military action transforms into a kind of network process. At the technological level, it is accompanied by the re-equipment of the army with high-precision weapons and weapons based on new physical principles situated not only on land or sea but also in space; with the protection of their infrastructure from enemy`s similar weapons. The regular army, all kinds of intelligence, technical discoveries and high technology, journalism and diplomacy, economic processes and social transformations, civilians and military personnel, regular units and some poorly designed groups these all integrate into a single network through which information circulates. Creating such a network is at the heart of US military reform.

Network wars are virtual wars. The one who wins virtually wins in general. Because the purpose of any war, in any sphere, is to establish control over the enemy's territory. Nevertheless, if the territory of the enemy is no longer real and not sacral but virtual, then the victory in this virtual space by virtual means over the virtual opponent through a virtual act is the result of victory in the virtual war. Here, the reality is not subordinate to virtuality but replaced by it.

The basis of all network wars is operations and basic effects. They are defined as a set of actions aimed at forming a model of behavior of friends, neutral forces and enemies in a situation of peace, crisis and war. In other words, it's such a qualitative environmental impact that nothing is directly imposed on participants, but they do what the networkers want. This means explicitly establishing full and absolute control over all participants of current or possible hostilities and total manipulation of them in all situations – both when the war is in progress, when it is ripening, and when peace is ruling. This is the whole essence of network warfare – it has no beginning and end, it is ongoing, and its purpose – to provide those who lead it, the ability to comprehensively control all the forces of humanity. This means that the implementation of the network is a deprivation of countries, peoples, armies and governments of the world, whatever their independence, sovereignty and subjectivity, their transformation into rigidly managed, programmed mechanisms. The purpose of such an "operation" is to formulate a pattern of behavior not only friends but also neutral forces and enemies, that is, all, consciously obeying the imposed scenario, act not on their own volition, but on the will of those who carry out the network war.

Therefore, having analysed the abovementioned, we can draw the following conclusions. Today we can state there is an academic tradition that is weakly moving forward the theory of information wars. Moreover, it is possible to say that the development of this theory has even slowed down to some extent. In our opinion, its origins could be expressed in the following:

– it is practitioners, not theorists, who study this field thoroughly (so, they have little interest in writing theories);

– the first group of researchers has passed away, and nobody came to replace them;

– in the case of Americans various agencies see this field differently, relying on diverse terminology (such as the Department of Defense or the State Department), that results in a lack of a unified approach;

– this field is in secrecy mode, so a particular stream of texts does not reach the general public;

– insufficient development of social science tools.

It becomes clear that the network warfare strategies development only begins, as for conducting military operations (US Army in Iraq, Afghanistan), so for the creation of "starting conditions" of the conflict before it begins.

The goal of network wars is to have absolute control over all international relations participants worldwide. There is no need to use the direct occupation, to introduce the troops massively or to capture the territories, to conduct unnecessary hostilities or spend vast military duties. The Network is a more flexible

weapon, it manipulates violence and military force only in an extreme case, and its main results achieved in contextual impact on a wide range of factors.

The goals of the transition to network military models are:

- to ensure the existence of permanent allied forces;
- to inculcate the idea of one's military potential superiority;
- to prevent threats and aggression;
- to guarantee a quick and decisive victory in the case of fighting.

These must be achieved through the specific advantages of the network approach, which include: better synchronisation of the combat units' operations directly on the battlefield; quick military commands transfer; increasing the enemy's number of victims proportionally to the reduction of own losses.

References:

1. Arquilla, J., Ronfeldt, D. (1997). *Cyberwar is coming*. Santa Monica. [in English].
2. Arquilla, J., Ronfeldt, D. (1999). The emergence of noopolitik. Toward an American information *strategy.* Santa Monica. [in English].
3. Arquilla, J., Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Santa Monica. [in English].
4. Arquilla, J., Ronfeldt, D. (2001). *The advent of netwar*. Santa Monica. [in English].
5. Dearth, D.H. Rethinking the application of power in the 21st century. *Military Intelligence.* <www.fas.org/irp/agency/army/mipb/1997-1/dearth.htm> (2020, February, 25). [in English].
6. Libicki, M. (1995). *What is information warfare?* Washington. [in English].
7. Libicki, M. (2007). *Conquest in cyberspace. National security and information warfare.* Cambridge. [in English].
8. Libicki, M. (2009). *Cyberdeterrence and cyberwar.* Santa Monica. [in English].
9. Libicki, M. What is information warfare? *Information Warfare Site*. <www.iwar.org.uk/iwar/resources/ndu/infowar/a003ch01.html> (2020, March, 25). [in English].
10. Szafranski, R.(1997). *Neocortical warfare? The acme of skill.* Santa Monica. [in English].
11. Szafranski, R.A theory of information warfare. Preparing for 2020. *Airpower Journal* <www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/szfran.htm> (2020, February, 12). [in English].
12. Taylor, P.M. (1995). *Munitions of the mind. A history of propaganda from the ancient world to the present day.* Manchester – New York: Moorcraft P.L. [in English].