INFORMATION WARFARE IN THE INFORMATION AGE

Sebastian SÂRBU, Ph.D.[*]

Abstract: *Information warfare represents a real non-conventional threat which in the context of the technological revolution of telecommunications and modern electronics has found its place as an instrument of prevention of classical warfare, but does not exclude conventional warfare, fought with the means of organized defense.*

The globalization of information and the needs of information protection of society at a global scale are the necessities of the moment, demanding a collective approach.

Keywords: *information age, technological revolution, globalization, information protection, NATO, electronic warfare, information operations.*

Identified and quantified at the middle of the seventh decade of the twentieth century, information warfare was considered a type of war with the potential to become as important as land, sea, air, or space warfare. In order to synthesize, it could be said that the verbs best suited to summarize its definitions are: to intercept, to transmit, to deal rapidly with a piece of information, to obstruct the adversary. The technological revolution in the field of computer science and communications has increased the importance of information, which led to the collection, processing, storage, and dissemination of information at greater distance to an ever larger number of users.

At the general level, information warfare in the strict military sense could be defined as the entire range of information operations used at tactical, operative, and strategic levels, during peace time, as well as during escalation of crises and conflicts, with the purpose of attaining some objectives or influencing certain targets. The military component of information warfare, the command and control warfare, has, in NATO's

[*] In security and defense, vice-president of the National Academy of Security and Defence Planning, Special Adviser at International Organization for Security and Intelligence

vision, the following meaning: "the integrated use of all military capabilities, including security operations, deceit, psychological operations, electronic warfare, and physical annihilation, supported by all the sources of intelligence and communication and information systems, to prevent access to information, to influence, deteriorate or destruct the capacity of command and control of an enemy, while keeping one's own military capabilities secure from similar actions".

According to some of our specialists, information warfare is defined as "the way in which a society, organization, or individual, well-adapted or not to the new information wave, tries by all means to acquire information supremacy and affect the opponents' and partners' information and information processes and systems, while undertaking actions to defend their own information processes and systems".

An interesting and surprising definition, given by the political analyst Thomas Rona, subsumes the scale and moments of information warfare, which represents the entire range of "tactical, operative and strategic level confrontations over the whole spectrum of peace, crisis, crisis escalation, conflict, war, ending of war, reconstruction, undertaken by the parties, adversaries or enemies, using informational means to attain their objectives".

We can consider information warfare as being a new concept if we consider its means, and at the same time, an old form of war if we consider its basic concepts (the Chinese philosopher Sun Tzu made reference 25 centuries ago to "cunning", the art to deceive, the necessity to prevent the opponent from correctly evaluating a certain situation).

Many definitions of information warfare, given in order to encompass the content and characteristics of this concept, insist on the fact that this form of warfare is based on defensive or offensive actions, which are part of an overall strategy, which presupposes not only a series of technical means, but also a number of operations which use the techniques and available information according to the purpose, actions which ensure the advantage of information superiority over the adversaries or even the allies.

In the military field, information warfare can be associated to the image of an iceberg whose top can be seen, but whose essential part is hidden and shrouded in secrecy.

Information warfare encompasses "any action destined to annihilate, exploit, deteriorate, or destroy the enemy's information and information functions, to ensure protection against similar actions, and to fully use one's own information capabilities".

Nowadays, information warfare has become more and more attractive from a military standpoint, given the increase in the number of targets that are vulnerable to information attacks and the increasing need for these targets to be defended. In the new circumstances, we can see that neither time nor the quantity of information can be a key factor in the political and military decision making processes. As such, during conflict situations, adversaries will have simultaneous access to enormous quantities of information, but it is the one who acquires the most precise and complete information and has an efficient system of processing and protecting it that will have the upper hand. The way events evolved during the last few years certainly proves that we are witnessing the materialization of a new type of aggression, of a new type of war, an invisible war, whose characteristics and forms of manifestation, subtle and efficient, greatly surpass the traditional, classical ones. Moreover, information warfare is relatively cheap when compared to other types of warfare, allowing developed countries, as well as the terrorist groups interested, to acquire capabilities in this field and to use them according to their purposes.

Alvin Toffler said: "if you are not interested in war, then war will be interested in you". The globalization of information, the need for information protection, not only of institutions, but society in its entirety, transforms information in a strategic weapon in the competition over open spaces between global centers of power in all fields of activity.

The particularly complex nature of information war is defined by the following factors: the impossibility of exact identification of opponents; the multitude of targets; the lack of spatial limitations; the lack of fast methods of fixing dysfunctional aspects; the lack of political limitations; the use of relatively simple, relatively cheap, and accessible technology; the increasing need for information; the lack of geographical limitations; the impossibility of establishing clear and precise responsibility.

Information warfare is accompanied by new means of action/influence which elude conventional military power and national borders. Many of these means act upon the direction, the level of command

and control, of will, of information, as well as upon essential elements of national infrastructure.

The essential element of information warfare is represented by the avoidance of conventional warfare, of human life loss, and material damages, by using these new means situated at the borderline between the conventional state of war and the conventional state of peace. It tries to influence the way systems work instead of destroying them, and it represents an evolution from the state of organized violence to the state of hostile influence.

Nonetheless, information warfare must not be mistaken for image war or classical propaganda.

It is necessary to implement the concept and laws regarding the control of technology and information, as well as the concept of information security, by developing convergent social mechanisms which would generate "close protection society" expertise.

Information operations.

The operations triggered by information warfare belong to the following categories: computer hacking; human spies; spy satellites; interceptions; video surveillance cameras; electronic warfare; physical destruction of communication components or energy systems; document forgery; perception management; psychological operations; viruses, worms, Trojans, fake viruses; theft of commercial secrets; interception of personal data; counterfeit emails; as well as many others.

By their simple enumeration, we can conclude that they can be used during real wars (such as Yugoslavia, Afghanistan, Iraq) or so-called "cold wars". Depending on the circumstances, some of them are treated as crimes, others are legal but ethically condemnable. Some parties or governments consider them normal practices. In the military field they are assimilated to conflicts. In any event, all they have is common is the purpose of exploiting the informational resources in the advantage of the attacker and the disadvantage of the other party, the attacked or the defender. We can thus conclude that the information operations that are specific to this type of war are both defensive and offensive.

The defensive ones integrate and coordinate policies, procedures, actions, personnel, and technology, in order to protect and defend

information and information systems. They focus on protecting one's own information, information-based processes, command and control systems, and communications and information systems. The protection has to be suited for any type of friend or foe and any situation (peace, crisis, conflict) and has four components: the protection of the information infrastructure; the discovery of attacks; the restoration of vital functions; and the reaction to attacks. The integration of all these components is essential.

The offensive information operations involve the integrated use of designated capabilities and activities, supported by information activity (intelligence), for the purpose of adapting to friendly or enemy decision making factors and promoting specific objectives. The basic purpose of this type of operations is to influence the knowledge and beliefs of decision making factors, to reduce their will and ability to decide and thus disrupt the decision making process. The offensive capabilities of information operations focus on information, on the processes which are based on information, on the systems of command and control, and on the communications and information systems. It is for this purpose that it is necessary to design them at the technological level that is specific to the entities involved in and particular characteristics of the conflict.

These two components are complementary and ensure the accomplishment of the purpose of information warfare: the information-based domination of the enemy. In the near future, these will likely be more than complementary, by the means of integration of one into the other. In these circumstances, the efficiency of the security of information systems will depend upon intelligence, and the efficiency of intelligence upon the security of information systems. Combat actions after the operation "Desert Storm" – at that time considered a basic example of future warfare, in strategy, operational art, and tactics – became a lot more decentralized, independent, direct, mobile, fluid, and efficient. They rely enormously upon the information system, the highly technical character of the available means, the existence of great power and precision intelligent weapons, the possibility of carrying out simultaneous, fast actions across the entire field of operations. Moreover, the most recent wide armed confrontations have shown that, regarding the way of planning, executing, and leading military operations, using information as a weapon confers it the primary role in

decision making and ensuring success, while leading to essential changes in the way military operations are being carried out.

As such, the fundamental principle according to which "the information war is a permanent war" has to be implemented as a security doctrine. It is necessary to build "electronic defense walls", on several complementary levels, in order to protect national structures.

It can thus be said that the new concepts and military technologies are being developed and experimented upon in a continuous manner, allowing developed countries to enter in the 21st century, in the Information Age, and ensuring technological and doctrinal advantages hard to equal by the other countries.

The technologies of the Information Age will completely revolutionize the manner in which military actions are being carried out and will change the face of conflicts/wars. The most significant advantages in the means of carrying out wars will arise from the quantity, quality, as well as the high degree of processing and using information. Leading technologies and information, accompanied by adequate military strategies and doctrinal concepts, competent military leaders, professional personnel, high level instruction and efficiency of armed forces, they will all lead to real power. The price of progress will be huge, but once paid, it will offer extraordinary advantages, possibilities and gains to those brave enough to pursue it.

BIBLIOGRAPHY

SUN Tzu, "Arta războiului", Editura Antet, 2012;
TOFFLER, Alvin & Heidi, "Război şi antirăzboi", Editura Antet, 1995;
RONA, P. Thomas, "Weapon Systems and Warfare: Report on Informational War", 1976.