sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVI No 1 2020

INCLUSION OF THE CYBER SPACE IN THE OPERATIONAL ENVIRONMENT OF THE MILITARY ACTIONS - A NEW PARADIGM IN THE MILITARY THINKING

Mihai Marcel NEAG

"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
mmneag@yahoo.com

Abstract: *The integration, coordination and synchronization of operations, missions and activities in the cyber space with those in the operational environment represent a significant challenge. The priority of the military operations is the accomplishment of the mission and in order for the cyber space to contribute to this purpose, a change of paradigm in the military thinking is necessary. From this perspective, the clarification of the terminological terminology is indispensable, especially in a domain that generates such different interpretations and reactions as those in the cyber field.*

Keywords: operational environment, comprehensive approach, cyber space, cyber threats, cyber operations.

1. Introduction

Knowledge related to the state of war conflict, the origin, causes, character and the regularities of war are circumscribed to military thinking which"....consist of all knowledge, concepts, trends regarding military phenomena in its dynamics, of the field and issues of military life"[1].

This knowledge also refers to the implications it has on all levels.

An important aspect that I want to highlight during this scientific approach refers to the concept of cyberspace from the perspective of military organizations, in order to allow its assimilation in the space of military operations.

The subtle form of current conflicts from the perspective of the development of modern information and communication technologies has a major impact on the social, economic, political and cultural, as well as on the military actions, marking real changes in their philosophy. Integrating, coordinating and synchronizing operations, missions and activities in cyberspace with other operational areas is a significant challenge. The priority of military operations is to accomplish the mission, and in order for the cyber space to contribute to this purpose, a change of paradigm in the military thinking is necessary.

Increased attention has been paid to ensuring cyber security and the response to cyber security challenges in cyberspace has intensified in recent years. Cyberspace is increasingly used as an environment that contributes to the systematic achievement of strategic objectives.

Against the background of the existence of hybrid risks and threats, operations in the cyber environment tend to be an integral part of all modern confrontations, contribute to maintaining the state of confusion and accentuate the uncertainty deriving from information overload, distorted representations and wrong

DOI: 10.2478/kbo-2020-0013

assumptions of planners, corroborated with the unconventional actions taken by the enemy.
Theoretical exploration of trends, contexts and implications of the operational environment on military operations can contribute to the training for a new way of thinking and a constructive approach to preparing the armed forces to face the uncertainty and challenges of the future, challenges which are modelled and accentuated by the emergence of the cybernetic operational environment.
The Warsaw Summit in 2016 marked a significant transformation at the Allied level by recognizing cyberspace as a new operational field, in which the Alliance will have to be able to defend itself as effectively as it does in the terrestrial, air and maritime fields for maintaining freedom of action and decision.

2. Promoting the cyberspace

Taking into account the evolution of the dimensions of the space of armed confrontations throughout human history, we easily find out that they have expanded continuously, depending mainly on three elements: the goals of those who triggered the conflict; the amount of forces that the belligerents could engage in the conflict, from its beginnings or during its development; the technical and technological level of the parties involved, which in turn determined and still determines the quantities and qualities of offensive and defensive military equipment. Also, in the current historical stage, the space of military confrontations tends towards cosmic dimensions and even discovers new dimensions, such as the cybernetic or virtual one, which forces the belligerents to continuous and permanent actions.
Theoretical exploration of trends, contexts and implications of the assembled operational environment on military operations can contribute to the formation of a new way of thinking and a constructive approach to preparing the armed forces to face the uncertainty and challenges of the future, challenges shaped and accentuated by the emergence of the cybernetic operational environment. The armed forces must integrate new developments in technology with an innovative way of thinking in order to develop new combat capabilities.
Meeting the requirements of information exchange and increased connectivity, characteristic of modern society, has led to the rapid and global development and implementation of systems, networks and applications based on information and communication technology.
The cyberspace has been promoted, along with the traditional environments for conducting military operations, to the rank of operational environment, an environment in which military operations can be performed on a defensive or offensive basis.
It is becoming more and more significant that cyber operations are part of a „hybrid" operational framework that seeks to implement a new model for approaching modern conflict. The Russian model promoted by the "Gerasimov doctrine" "involves the widespread use of political, economic, informational, humanitarian and other non-military measures [...] supplemented by inciting the local population and using disguised armed forces" [2], emphasizing that in the current operational context, there is an increasingly blurred line between the state of peace and the state of conflict, the armed forces no longer being the main actor to assume the role of the combatant.
During the conflict in Ukraine (2014), Russian forces used synchronized actions of cyber warfare, sabotage and electronic warfare, competing with conventional and unconventional military actions. The objectives of the Russian cyber operations were, usually, the clandestine collection of information from the cyber environment, blocking Internet communications of target

state institutions, exploiting vulnerabilities in critical infrastructures, disrupting critical services for the population, attacking and disrupting military and civilian communications and the command and control systems, the dissemination of one's own ideology, the manipulation of internal and external public opinion, the creation of a state of confusion, and last but not least, the modelling of the combat space in support of conventional military operations.
The consequences and the negative impact of modern society's dependence on the cyber environment have been highlighted by events such as the attacks on Estonia's cyber infrastructure in 2007 as well as by cyber combat operations carried out in 2008 during the conflict in Georgia and in 2014 during the conflict in Ukraine. These events together with the countless cases of cybercrime recorded have contributed to the nomination of cyberspace as the fifth operational environment, an environment through which a new type of power can be exercised.
In military terms, promoting the cyberspace to the rank of the operational environment implies that within it, the power can be projected by executing planned cyber operations, operations that can be both defensive and offensive.
Joseph Nye defined the cyberspace as "a global field within the informational environment whose unique and distinct character is customized by the use of electronic means and electromagnetic spectrum for the creation, storage, modification, exchange and exploitation of information, through interdependent and interconnected networks based on information and communication technology"[3].
The emergence of cyberspace has added a new dimension to the military operational environment, beside the terrestrial, maritime, air, cosmic and electromagnetic dimensions.
The use of cyberspace offers considerable advantages for cooperation but creates simultaneous dependence and vulnerabilities.

3. Characteristics of the cyber operational environment

Cyberspace is a man-made artificial environment, a system of systems animated by the connection between its hardware components (computers, controllers, interfaces, network nodes, physical or wireless connections) and software components (operating systems, programs, applications). Due to its anthropic character, the existence and development of cyberspace requires continuous human effort, for operation, maintenance, protection and modernization. The Internet ensures the global expansion of cyberspace, facilitating human interaction and an unprecedented exploitation of the information resources [4].
The specific characteristics of the cyber environment differentiate it from the natural environments.
The characteristics of the cyber environment (relatively easy and cheap access, anonymity, global reach, very high speed, specific time rhythm and asymmetry of vulnerabilities) make it possible to apply cyber power not only by state actors but also by non-state actors and even by to individuals with appropriate resources and skills.
The use of the force in cyberspace must, however, be done within a legal framework, in accordance with the principles enshrined in international law, principles such as discrimination and proportionality.
Cyberspace is characterized by the tendency to strict control. This control is manifested internally by censorship, by limiting the population's access to information and by limiting its possibility of disseminating information, and externally, by using its own cyber capabilities or partners against other state actors, usually under the protection of cyber anonymity and below the threshold of incrimination established by international law.

The development of cyberspace has accelerated the process of globalization by creating complex interdependencies between the political, social, economic and financial spheres, interdependencies that in the absence of adequate international cooperation lead to increased risks to security and defense.

The specific nature of cyberspace, ease of access and relatively inexpensive tools available on the market, create the premises for ensuring an important role of non-state actors in the conduct of cyber warfare actions. Non-state actors can take various forms (ordinary citizens, patriotic hackers, cybercriminals, cyber terrorists and cyber militias), under which they can operate in the anonymity provided by cyberspace.

The response to the challenges of cyber aggression is addressed on at least two organizational levels, decision-making and action. The first level is, as a rule, located at the central level of the executive power, being coordinated by state institutions defined and established by law. This level is responsible for the policy development and ensures the guidance, coordination and supervision of the performing of specific activities by national organizations with responsibilities in the field of cyber security and defense.

The second level is represented by operational units that are responsible for the implementation of policies established at the central level, through concrete activities in the cyber environment, activities aimed at the operation, maintenance, protection and defense of national cyber infrastructures. Some of these operational units, based on the decision taken at the central level, can plan and execute offensive cyber operations.

The artificial, volatile, unpredictable and anonymous nature of cyberspace ensures the possibility of cybersecurity being projected with relative ease and by a wide range of actors. Therefore, cyberspace is ideal for conducting asymmetric combat operations.

Cyber operations can aim at gathering information, modelling the cyber operational environment, creating military advantage at the strategic, operational or tactical level, supporting kinetic operations and asymmetric combat methods and finally achieving some politico-military objectives.

Documentary analysis and observations of the operational environment indicate that cyber technologies are evolving faster than cyber policies. This gap usually causes functional fractures between the strategic level, responsible for developing security and defense strategies, policies and doctrines, and the operational-tactical level, responsible for the carrying out of the cyber operations.

Cyberspace is a dynamic and complex environment. Recent events suggest that the presence and the capacity of action in the cyberspace play an increasingly important part in future conflicts, with cyberspace control becoming the mode of criticism and control of traditional operational environments. From this perspective, the military forces must have the doctrine, equipment and specialized personnel to act in the cyberspace by carrying out cyber operations of offensive or defensive character. These, even if they have no visible kinetic effects, if applied calibrated and at the right time, can act as a force multiplier. During war, cyber attacks are a tool at the disposal of military commanders similar to other weapon systems used in war, through which valuable targets can be hit, targets that help support the enemy's military effort.

From a technological point of view, in cyberspace there is a constant race between attacker and defender. The attacker designs new methods and applications for gathering information and launching cyber attacks and the defender reacts by blocking ports, updating software and developing more efficient mechanisms for defending its own network. In such a scenario, the attacker must constantly improve his attack skills

while the defender must constantly update his own technology.

4. Risks and threats caused by cyber operations

We note that, given the existence of hybrid risks and threats, operations in the cyber environment tend to be an integral part of all modern confrontations. The Russian strategy used in the Ukrainian campaign was successful, with cyber operations acting as a force multiplier or sometimes, through the effects produced, as a substitute for conventional military operations.

Cyberspace triggered the expansion of the operational framework, with the potential of causing economic and political disruption, quickly, at a distance and under the guise of anonymity. The specific interaction of cyberspace with other operational environments introduces new variables in the relationship between the evolution of the international community and the trends of collaboration or confrontation of actors that make it up and, at the same time, determines innovative interpretations of traditional military concepts.

Cyber attacks launched by an entity against a state and its population, for the primary purpose but not exclusively, of affecting the behaviour of that state actor, fall into the category of strategic cyber operations. This form of conducting combat actions in the cyber environment can be used at any time, without the two state entities involved being at war. Even when hostilities between two states seem imminent, they can carry out cyber attacks long before conventional military action begins.

Cyber attacks mainly target critical infrastructures and government warning, communications and information systems, with asymmetric consequences and effects on the population. The consequences of cyber attacks can affect the supply of goods and services of strict necessity to the population (water, food, electricity, heat) and seriously disrupt the capacity of the population as well as the state institutions to communicate and coordinate actions, to combat threats and restore the state of normalcy. All this leads to a state of chaos that supports the conditions for launching a conventional attack.

Offensive cyber action can result in a cyber attack that seeks to degrade, disrupt, destroy, or prohibit the operation or access to the computer system and existing information within it. Offensive cyber action can also materialize in exploitation, an attack technique that aims to steal confidential information. It can be seen that both attack and exploitation use the same pathways to opportunistically use the same vulnerabilities.

Cyber warfare is a particular form through which the information warfare is displayed; it is a continuous war, carried out in the spectrum of information and communication technology, a network war, which aims at domination and manipulation of information. Although the interception and manipulation of information has always been carried out in a military conflict, what is new in this type of war refers to the predominance of information, the ability to monitor and influence the flows that transit the cyber environment.

Cyber warfare aims to apply cyber power through specific methods to a new operational environment, an environment that significantly influences all other environments, including information. Perhaps one definition may be that "cyber warfare is the art and science of fighting without a fight, of defeating an opponent without shedding his blood."[5].

Cyber threats generally consist of actions that could be set in specific circumstances against target entities, by various actors in the cyber environment, in order to cause direct or indirect damage, which may affect the accomplishment of the mission in the joint operations. The main properties of threats in the operational cyber environment are:

- overcoming any physical, geographical boundaries;

- asymmetric effect;
- anonymity of actors;
- versatility - given by the ability of cyber actors to adapt quickly to the new characteristics of the social, political, military and, especially cybernetic environment, depending on the interests pursued;
- time - highlighted in the extremely fast dynamics of the development of actions specific to cyberspace.

The main types of cyber threats are:

- Computer Network Attack (CNA);
- unauthorized operation of computer networks (Computer Network Exploitation / CNE);
- kinetic attacks on the physical level of the cyber environment infrastructure;
- electronic attack on the physical level of the cyber environment infrastructure;
- the use of undercover agents or inside personnel to cause damage to the system or to gain physical and logical access to it;
- control of mission-critical infrastructure, with the help of a third party (e.g. through local telecommunications and Internet service operators).

The cyber threat, often implemented in a hybrid confrontation framework, proved difficult to counteract because, apparently, the state actor directed and used the services of non-state actors such as cybercrime organizations, "patriotic hackers", thus taking advantage and exploiting the operational advantages given by the problem of attributing cyber attacks. This is what happened in the Russian-Ukrainian conflict that started in 2014. With the annexation of the Crimean peninsula, the conditions were created for a hybrid framework of confrontation between two state actors. This framework has favoured the implementation of the cyber threat, in the broader context of the hybrid war through which the Russian government is trying to promote its geopolitical interests.

Cyber threats have a deep asymmetric character, because, with relatively limited resources, an individual or a group of individuals, affiliated or not with governmental structures, can generate significant destructive effects with a destabilizing impact at the level of a state. Such actions can remain in an area of "plausible denial" in the way they have been planned and carried out, making it very difficult to attribute such attacks or take decisions on possible countermeasures. "It will be more difficult to make a decision for a military response, be it purely cyber, even in the context of a cyber attack with devastating impact. It is also one of the reasons why cyber campaigns have been and will continue to be used more and more in the context of hybrid actions "[6].

5. Conclusions

The analysis of the operational environment must be directed by examining the development trends of new technologies and the effects of their implementation.

Cyberspace appears as a new type of human interaction environment, an environment built for practical reasons, to meet the requirement of modern societies to provide the new type of fundamental resource, namely information.

The cyber environment has evolved in a way that can affect geostrategic balance, as well as the fact that the virtual presence in cyberspace of state actors and their armed forces is vital for maintaining the physical presence in all other operational environments. From a military point of view, cyber power directly supports land power, maritime power and air power.

I consider that, in the near future, the sophistication of cyber attacks will increase in the sense of expanding the ability to secretly attack computer networks, gathering information from the cyber environment, causing damage and destruction of critical cyber infrastructures. Information societies and modern economies must prevent, protect, deter and, where it is applicable, respond firmly to asymmetric threats. Otherwise, information,

the fundamental resource of the progress and prosperity of modern society, will become the tool negatively exploited by potential adversaries.

Cyber threats have distinct characteristics from conventional ones. The effects of cyber attacks can be either visible in physical space or "invisible", with effects only in virtual space. The effects can be instantaneous or time-lapse, activated at moments of opportunity and identifiable only using specialized cyber defense capabilities. Cyber attacks are difficult to attribute, often involving the use of civilian communications infrastructure, and it is difficult to determine when a cyber attack requires a military response and what are the limitations and constraints of such a response if cyber action is needed outside the military cyberspace.

The operationalization of cyberspace will represent a challenge for the future, for imposing the integration of military cyber forces and capabilities in planning process, in operations and missions, developing relevant capabilities in the context of hybrid conflicts, as well as for the whole spectrum of evolution of the conflicts from peace to crisis and armed conflict. Information support, in this context, will be vital for knowing the threats and identifying the risks that affect our systems, and also for knowing the vulnerabilities of enemies systems and networks.

References

[1] Col.dr. Soare Corneliu, *Istoria gândirii militare româneşti*, Editura Militară, Bucureşti, 1974, pag. 9.

[2] Ana Stan, *Rusia a ridicat războiul la rang de artă*, 02.09.2014, http://adevarul.ro/international/rusia/razboiulhibrid-putin-inceput-timp-urma-rusia-ridicat-stacheta-dus-razboiul-rang-arta1_5405b3c30d133766a8cb23aa/index.html

[3] Traducere după Joseph S. Nye Jr., The future of power, New York: Public Affairs, 2011, p. 2.

[4] FM 3-38, Cyber electromagnetic activities, Department of the Army HQs, Washington DC, 2014.

[5] Jeffrey Carr, Inside Cyber Warfare, O'Reilly Media Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2012, p. 2.

[6] Bogdan Dumitrescu, *Operaționalizarea spațiului cibernetic – de la securitate cibernetică la succesul operational,* Gândirea militară românească, nr.1, București, 2019, pag. 58.