The 13th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 8th-9th 2018

ESTIMATING CYBER THREATS IN THE CONTEXT OF THE CONTEMPORARY SECURITY ENVIRONMENT

Mihai Marcel NEAG*
Dănuţ MOŞTEANU**

* "Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
**"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania

Abstract:
Technological and scientific changes in all areas of activity will also bring about changes in the security environment and may create strategic surprises that we are currently unaware of and misunderstood. The rapid development and rapid implementation of information and communication technology systems, networks and applications has led to the emergence of cyber space, which generates new forms of power, generically called by international relations specialists as "cyber-power". In the current context, there is an increasing presence in cyberspace and the execution of a growing number of cyber operations by both state and non-state actors. Recent events on the international scene signal the intention of some states to boost the quantitative and qualitative development of military cyber capabilities. In this context, this communication identifies the constants, variables and transformation trends of the current security environment determined by the projection of cyber power.

Key words: cyber, threats, security, capabilities

1. Introduction

The current security environment, environment characterized as complex, ambiguous, uncertain and volatile, favors the use of cyberspace for the hostile promotion of political, economic and military interests and objectives. In the current context of an intensified global information environment, there is an increase in the presence of offensive cyber operations, performed by both state and non-state actors. Thus, offensive cyber operations appear to play an increasing role in deterrence strategies and implicitly require a reconfiguration of the operational environment and the development of military cyber capabilities.

The theoretical exploration of the trends, contexts and implications of the operational environment on military operations can contribute to the formation of a new way of thinking and a constructive approach to the training of the armed forces to cope with the uncertainty and challenges of the future, the challenges shaped and accentuated by the emergence of the operational cyber environment. Rapid changes in the geo-political, strategic, economic and technological environment, corroborated with the creativity, ingenuity and capabilities at the disposal of potential adversaries can produce strategic surprises, surprises that can have a catastrophic impact on the way of life and even the existence of democratic societies.

Although war is a politically determined act and assumed to achieve political goals, internal and external pressures as well as hesitations in strategic decision-making have always conditioned military operations and will continue to do so. Use in recent conflicts of force and violence, both by state and non-state actors, suggests that war maintains its political dimension, regardless of the nature of the trigger entity. Political calculations on

the one hand, and secular practices and ideologies on the other, combined with the impact of passionate elements and events, make it almost impossible to predict the trajectory of any potential conflict. "War does not consist of the action of a living force on an amorphous mass ... but in the collision between two living forces." [1] Therefore, in the war, any means will be used to defeat the opposing side, including cheating, misleading, misinformation, non-observance of generally accepted rules, use of any real or perceived vulnerability. A fundamental element in ensuring the premises of success is the profound understanding of the culture, history, geography, religious and ideological motivations of the enemy, with an emphasis on the ability of the forces to adapt to the changes that may occur in the operational environment.

A major challenge of the near future is the effective integration of the cyber environment and its associated capabilities, from a doctrinal, functional and action point of view, to support the efforts of the military instrument of power, security and defense. That is why it is necessary to study the typology of the 21st century war, to investigate the implications of the cyber environment on the military forces and to experiment with new forms of training of the forces and conducting the joint operations.

2. Considerations on cyber power

Although technology has revolutionized the way the war is waged, the objectives of the war have not changed. These may vary in a wide range, ranging from intimidation actions of an adverse nation, possibly to its complete destruction. The objectives can be achieved by launching a series of campaigns in all operational environments, campaigns that converge to the nation's power source.

Cyber-attacks have proven to be a powerful tool to sabotage and achieve concrete effects. Such attack tools are available and can be used by military commanders during the conflict to meet the goal of destroying or neutralizing the enemy's potential to carry out the war.

As a rule, who owns the information also has the strategic initiative, and this remains one of the fundamental characteristics of the security environment of this beginning of the century. Increasing dependence on information from any modern military organization, digital, resident, or cyber-space information requires the creation of a specialized force category, generically called cyber forces.

The consequences and negative impact of modern society's dependence on the cyberspace have been highlighted by events such as attacks on Estonia's cyber infrastructure since 2007, and cyberwar operations carried out during 2008 during the conflict in Georgia and 2014 the conflict in Ukraine. These events, along with countless cybercrime cases, have helped to nominate cyber space as the fifth operational environment, whereby a new type of power can be exerted.

The concept of cyber power has prompted the interest of the academic community and security and defense professionals and the awareness of its importance is reflected in the new cyber security strategies adopted by most state actors. In military terms, the promotion of cyberspace at the operational environmental level implies that the power can be projected through the execution of planned cyber operations, operations that can both defensive and offensive.

Joseph Nye defines cyberspace as "a global domain within the information environment whose unique and distinctive character is customized by the use of electronic means and electromagnetic spectrum to create, store, modify, exchange and exploit information through interdependent and interconnected networks on Information and

Communication Technology." [2] United States Department of Defense Military Terms Dictionary also includes the Internet in the definition of cyberspace.

Romania's Cyber Security Strategy defines cyberspace as "the virtual environment generated by cyber infrastructures, including information processed, stored, or transmitted, as well as user actions in it." [3] Cyber infrastructures are those "information and communication technology infrastructures, consisting of computer systems, related applications, electronic communications networks and services". [4]

Cybernetics is an artificial environment created by humans that requires continuous human effort for operation, maintenance, protection and modernization. The Internet provides global cyberspace expansion. The emergence of cyberspace has added a new dimension to the military operational environment, in addition to terrestrial, maritime, air, cosmic and electromagnetic dimensions. Cyber space has led to the expansion of the operational framework, with the potential to cause economic and political disruptions, quickly, remotely and under cover of anonymity. The specific interaction of the cyber space with the other operational environments introduces new variables in the relationship between the evolution of the international community and the tendencies towards collaboration or confrontation of the actors that make up and implicitly determine the innovative interpretations of the traditional military concepts.

Cyber power is defined as "the ability to use cyber space to create the benefits and influence the events in other operational environments and along all power tools." [5] Broadly speaking, the application of power in international relations depends on a multitude of factors within the geopolitical context. In addition to traditional power, cyber power depends on digital information channeled through cyberspace as well as its hardware and software resources.

Cyber power can be a tool used to achieve political, economic and military goals. In the current global system, characterized by increased connectivity, complex dependencies and antagonistic interests, the possibilities of applying cyber power generate security risks and pose a challenge to the international legal framework.

Cyber-attack can be classified into three categories. The first category, cyber-theft, describes criminal activity against individuals, corporations or public institutions for identity theft, unauthorized access, alteration and extraction of data and information. A second category is the attacks aimed at forbidding the access of authorized users to digital information and services. The third category includes destructive cyber-attacks aimed at unauthorized modification of information in cyberspace as well as the destruction of material assets connected and controlled through cyberspace, from personal information and informational assets to critical infrastructure management elements.

How to approach cyber-power has major implications in developing cyber security and defense policies and strategies. To address cyber challenges, in addition to managing cyber defense, states are making sustained efforts to manage cybercrime and cybercrime issues. The results achieved so far are not entirely satisfactory as the legal framework can not keep pace with technological development and cybernetic volatility.

Protection against the effects of cyber-attacks and the ability to act in the cyber environment must be a national priority. In addition to economic power and conventional military power, modern nations tend to develop cyber capabilities to protect and develop their national interests.

3. The cyber threats from a Euro-Atlantic perspective

Cyber threats to security and defense are strategic challenges that most modern nations are facing. The current North Atlantic approach to cyber security has been driven by increased geopolitical instability and the expansion of international terrorism.

Interest in cyber space has increased progressively at NATO's strategic level because of its growing complexity, cyber-attacks launched in 2007 on Estonia's cyber infrastructure, cyber operations planned and executed by the Russian forces during the war with Georgia in 2008 but also the use of cyber means and techniques by Al-Qaeda terrorist organizations and ISIS.

Thus, at the NATO summit in Bucharest in 2008, the concept of cyber defense was debated in response to the identified cyber threat. Under the auspices of the "Comprehensive Approach" concept, following an evolutionary process of research and review of the international strategic context, the NATO leadership has endorsed Member States with a new cyber defense policy. The evolution of the concept and the increasing importance given to cyber threats materialized in the recognition of cyberspace as an "operational domain" during the NATO summit in Warsaw in 2016. The inclusion of cyber space in the operational media category suggests a collective defense space, the invocation of Article 5 of the Washington Treaty by any NATO member state for an allied response to high-magnitude cyber-attacks.

In the Allied context, it is difficult to launch, by invoking Article 5 of the North Atlantic Treaty, a military response to large-scale cyber-attacks, like those suffered by Estonia in 2007. Building on this premise, the apparent option of NATO members states remains the reinforcement of cyber infrastructures, so that future similar attacks do not have significant effects on society. Under a volatile, uncertain and predictable security environment, it is necessary to understand the nature and implications of the new challenges to the Alliance's defense before making strategic decisions and hiring resources for their implementation.

In the context of the proliferation of cyber capabilities, solving the challenges of the virtual environment does not resolve in a solution that favors a strictly military approach. Cyber conflict must be analyzed in several ways, and new methods of fighting cyber action should be developed and implemented along with increased international legal efforts to regulate it.

Fundamental changes in the physiognomy of modern conflicts by the recrudescence of terrorism and geopolitical status quo motions impose the need for formal recognition of the cyber operational environment within national security and defense strategies. The current security environment is influenced by the evolution of hybrid threats, which are ways used by certain state and non-state actors to meet geopolitical goals, which use the combination of military and non-military assets on a large scale. NATO Secretary General, Mr. Stoltenberg, categorized the cyber threat as one of the utmost importance, similar to other serious threats defying territorial borders, such as terrorism and proliferation of nuclear weapons. From this perspective, this posture may lead NATO to either a firm policy of cyber-deterrence or a policy of tacitly encouraging the development of offensive cybernetic capabilities.

An alternative approach to cyber-deterrent policy suggests that states and political-military alliances need to consider the consequences of a paradigm shift, through strategic reorientation, from discouragement policies to successfully deal with the accelerated evolution of cyber threats to policies focused on preventing attacks and cyber resilience. From a military point of view, this reorientation involves changes in doctrines, operational procedures and hiring rules, along with the development of new cyber capabilities and the training needed to operate and maintain them. The analysis suggests that, although enhanced cyber-prevention and cyber-resilience measures will not reduce cyber threats, implementing such defense policies is preferable in the current geo-political context.

4. Spectrum of cyber attacks

The phenomenon of cyber-attacks is by nature a global one given the current dependence of society on information technology and the fact that the interconnection of elements of today's society transcends the frontiers of nations. Cyber-attacks have become a phenomenon, primarily because of their possible effects on the normal functioning of society, with potentially damaging consequences in most areas of activity.

The cyber war is made up of a system of actions aimed particularly at disrupting, by all means, the opponents' information networks, the protection of their own, the disinformation of the opponent and its information intoxication. Cyberwar is not an extremely informational war. Cyberwar aims to apply cyber power through specific methods, in a new operational environment, which influences significantly all other media, including the informational environment.

The types of actions that can be encountered in the cyber environment are: cyber-attack (which has the role of producing effects on a computer system); cybercrime (which includes all the actions, long publicized, theft of credit cards, deception, identity theft, etc.); cyber spying (obtaining classified information through cyber-space actions); subversion (by breaking into some computer platforms and placing subversive information, or by creating sites dedicated to subversive messaging); cyber terrorism (cyber-action involving physical violence and fear induction).

Generally, cyber-attack is the exploitation action or attempted unauthorized exploitation of a vulnerability within a computer system. From a modest effect to a deeply destructive one, the wide spectrum of cyber-attacks can include intrusion, surveillance, data copying, spying, intellectual property theft, data manipulation, data destruction, device and system control, kinetic effects by device control, destruction of devices and property, destruction of critical infrastructure, individual fatalities, and operations with national impact. Cyber-attack may take the form of a passive attack that attempts to copy or delete data from the target computer, or may take the form of an active attack, which may involve altering the data stored on a computer system, modifying the software by altering its entry data.

Cyber-spying is the use of cyber space by specialized services to fraudulently get classified information. This type of action originates in the early period of the accelerated development of computer networks in general and of the Internet in particular. Certainly, this type of espionage is considered essential, not only in peacetime, but also in crisis or wartime, to multiply the effort to obtain informational supremacy, with effects in all areas of activity of society as a whole: economic, financial, social, political and military.

Cyber terrorism is defined as "a premeditated, politically motivated act committed by non-state or clandestine clans against computer systems, computer programs and data that involve physical violence and which is intended to induce fear in non-combatant targets." [6] The essential difficulty is generated by the fact that, while operating with this concept of cyber terrorism, the casuistry is very rare. Terrorism is based on inducing fear in the non-combatant population, this fear having the role of facilitating the fulfillment of terrorist goals. The essential differences between cyber-attack and cyber terrorism consist not in the methods and means used, but rather in the authors of the action, their motivations and the objectives pursued.

In this context, the "counter-reaction" to computer aggression appears as a necessity for all levels of society, starting from an individual, organization, state or alliance. With the emergence of cyber-attack methods, as an immediate response to computer aggression, the specialists tried to identify cyber defense solutions. Cyber Defense is a form of reaction that constitutes a complex set of defensive measures and actions, designed to prevent and ensure an effective and prompt response to offensive cyber-action.

5. Conclusions

Transforming the contemporary security environment is influenced by complex threats, diversified vulnerabilities and globalized risks. In the context of the development of new technologies as well as the uncertainty caused by possible social disturbances, which can include violent manifestations within states, it creates new challenges and threats to security.

Evolutionary trends in the expansion of the number of devices connected to the Internet, the numerous possibilities to exploit their vulnerabilities, the ease with which these activities can be performed, and the limited detection capabilities of the attackers lead us to the idea that classical security tools must be supplemented with new elements that help limit the possibilities of being subjected to a cyber-attack.

The dependence of modern, knowledge-based societies on an increased volume of information transmitted at extremely high speeds implicitly determines their dependence on cyberspace. As new technologies are adapted for military use, new dimensions are added to the operational environment that transforms and generates new opportunities and risks for the armed forces.

The specificity of the cyber dimension lies in the fact that, alongside the electromagnetic dimension, it crosses and influences all other operational dimensions. The cyber environment has evolved in a way that can affect the balance at the geostrategic level, as well as the fact that the virtual presence in the cyber space of state actors and their armed forces is vital for maintaining physical presence in all other operational environments.

From the military point of view, cyber power directly supports ground power, maritime power and air power. By extrapolating the observations, we concluded that because of its ubiquity and trans-domain nature, cyberspace has become a key element for the projection of any kind of power, and therefore it is a mandatory element to consider in any national security and defense strategy.

Using cyberspace can create advantages and influence events in other operational areas. The influence of events in cyberspace is reflected in physical reality, and therefore, the actor possessing and using developed cyber capabilities possesses in fact a new type of power, cybernetic power.

Cyber security is a dimension of national security. The challenges embodied in this concept relate to managing risks, threats and vulnerabilities by developing comprehensive security strategies and concrete implementation plans.

References:

[1] Translation after Carl von Clausewitz, On War, Edited and Translated by Michael Howard and Peter Paret, Princeton University Press, 1976, p. 97.
[2] Translation after Joseph S. Nye Jr., The future of power, New York: Public Affairs, 2011, p. 2.
[3] Romanian Government, Decision no. 271/2013 to approve The Cyber Security Strategy of Romania and the National Action Plan on the Implementation of the National Cyber Security System, published in the Official Gazette, Part I, no. 296 of 23.05.2013.
[4] Ibidem
[5] Joseph S. Nye Jr., op.cit., p. 5.
[6] Andrew Colarik, Cyber-Terrorism, Political and Economic Implications, Idea Group Publishing, 2006, pp. 48.