WAR AND DEFENSE IN VIRTUAL SPACE

Colonel (Ret.) Professor Gheorghe BOARU, PhD [*]

Abstract: *In the information society, information - as a weapon, target and strategic raw material is at the root of all decisions.*

Information warfare has become an area of exceptional research and development, for which increased attention is paid, but also the resources needed for research and implementation, due to the rapid advances in information technology in recent decades.

The conflict in cyberspace or cyber-war has become a phenomenon at the confluence of several forms of confrontation between these actors, such as imagistic warfare, psychological warfare, information / counter-information warfare, cyber-terrorism, network-based warfare, electronic war, cybercrime, etc.

Cyberspace has become the fifth dimension of the military confrontation so that in the information warfare, we can define, depending on the states of peace, crisis, conflict (war) or the post-conflict period, some specific phases of cyber confrontation.

The common feature in the cyber-space confrontations is the continual antagonistic ratio established between cyber-threatening threats (terrorism, espionage, sabotage, subversion and organized crime) and information security.

NATO has developed policies and strategies and set up bodies and institutions in the field of cyber defense. Romania has acted in accordance with European and NATO measures by developing similar documents and creating specific national cyber security structures.

Keywords: *information warfare, cyber war, virtual space, cyber security, cyber terrorism, electronic warfare, information security.*

[*] Corresponding Member of Academy of Romanian Scientists, Member of the Academy of National Security Sciences, *e-mail: boarugheorghe@yahoo.com*

In the informational age, the war no longer exclusively concerns the military domain. In the information competition, which is as old as the human conflict, states, institutions and individuals are trying to increase and protect their own information base, while trying to limit the opponent's. In the information society, information - as a weapon, target and strategic raw material is the basis for all decisions.

Moreover, it is obvious that, in the information age, information has become an integral part of human competition. The actor who possesses better abilities to compile, understand, control and use information will hold superiority and ultimately gain substantial advantages over other competitors.

Modern military actions represent a dynamic process with two components that are mutually conditioned: the energy component and the information component. The action of the energy component aims at destroying or neutralizing an adverse physical system.

The information component aims at procuring, processing and transmitting information in order to ensure the effectiveness of energy action.

Compared to the destructive one, the informational component is characterized by a much lower energy consumption. Therefore, it is considered that information is a real weapon of combat, a fourth weapon.

In the literature, information is approached both as *"a strong weapon as well as a preferred target"*[1], or it is stated that *"information may be the most feared weapon in technological developments in the battle space…"*[2].

The Information assurance in the military environment is strictly dependent on information and communication technology, and modern communications and information components have become the primary support of military systems, especially the specific information systems for command and control (C4I, C4I2, C4ISR, C4ISTAR etc.).

The information revolution has led to the emergence of a new type of war in which neither the size of the forces nor their mobility can determine

[1] *Cornerstones of Information Warfare*, Department of the Air Force, Washington DC, 1995, p. 2.
[2] Peter Grier, „Information Warfare", *Air Force Magazine*, No. 3, March 1995, p. 23.

the outcome. This is primarily due to the new technologies, the way of collecting, storing, processing, transmitting and presenting information, and secondly, how organizations are prepared to take advantage of the huge amount of information available in information and communication systems.

Information and communication technology (ICT), especially the Internet, has been an increasingly important aspect of political and economic social life for two decades worldwide and is the backbone of the global information society today.

Their evolution and development have brought many benefits to individuals, as well as to a number of public and private institutions and actors, but at the same time allowed us to witness the positive impact of social networks in the Arab Spring riots in 2011, or to increased use of e-commerce among business people and individuals.

However, ICT has also brought serious threats of cyber attacks, demonstrated in recent years through cyber spying and cybercrime in virtual networks within the ecosystem in which we live.

The vulnerabilities of ICT-based systems depend on several factors among which I consider that the number and quality of users (security culture) are very important. In this respect, I analyzed some statistical data that would allow me to draw some conclusions as follows:

- on 31 December 2017 out of 7,515,560,214 inhabitants of the globe[3] there were 4,156,932,140 Internet users[4], meaning over 55% of the world's population;

- The distribution of internet users across the globe shows that all continents (geographic areas) use this service in different percentages[5], as follows: Asia: 48.7%; Europe: 17.0%; Africa: 10.9%; Latin America: 10.5%; North America: 8.3%; Middle East: 3.9%; Oceania / Argentina: 0.7%.

The latest International Telecommunication Union (ITU) report shows that of the over four billion people using the Internet in the world, eight of the top ten countries in the top-most states are European.

[3] *Statisticile lumii în timp real*, [http://www.worldometers.info/ro/].
[4] *Internet World Stats*, [http://www.internetworldstats.com/stats.htm].
[5] *Ibidem*.

According to the ITU ranking, Denmark is the most "connected" country in the world, ranking in Top 10 being completed by South Korea, Sweden, Iceland, UK, Norway, Holland, Finland, Hong Kong and Luxembourg.

As a European country, Romania has been experiencing an exponential evolution in ICT since 1989. Now in Europe, among the top countries with most Internet users, Romania is in the top 60. It is worth mentioning that Romania ranks 58th in the top Worldwide, which includes 166 states, because although the speed of connections is among the best, we are "depressed" at the penetration rate[6], Romania ranks sixth out of 20 countries in a quarterly ranking by the American company Akamai Technologies on Internet connection speed, managing to surpass the US and UK in this area. The ranking drafted for the July-September 2013 period was achieved based on the maximum connection speed in traffic through in the company's global network[7].

The United States was only 13th, one of the reasons being the country's large surface, making it difficult to install optic-fiber cables all over the country.

Romania was outrun by Hong Kong, South Korea, Japan, Singapore and Israel. The seventh is Latvia.

Akamai Technologies explained that small countries are succeeding in installing faster technology needed for the high-speed Internet.

Bulgaria ranks 12th, with a connection speed of 37 megabits per second, more than twice the global average and the United Kingdom ranks 16th at a speed of 35.7 megabits per second, 3.9% lower than in the previous quarter, but 27% faster than a year ago.

Almost 70% of people aged 16 to 74 in Romania, equivalent to 10.6 million users, used the Internet in 2016, up 1.2 percentage points from the previous year, while 65% of households in the country had access to the home network, according to data from the National Institute of Statistics (INS)[8].

[6] hotnews.ro.
[7] https://www.bloomberg.com/.
[8] http://www.insse.ro/cms/sites/default/files/com_presa/com_pdf/tic_r2016.pdf.

The explanation of these Romanian performances is that due to the fact that in Romania the Internet was adopted much later than in some economically developed countries, it allowed skipping the early technologies that were slower and the best performing technologies were adopted directly.

The number of Internet users and their proportion in the global population has risen at an unimaginable rate, which entitles us to say that we are in the informational era.

The security of virtual space has become one of the most pressing security challenges of the 21st century, given its importance for everyday life, government, national security, business and citizens alike. The cyber world and associated technologies created, on the one hand, more social, cultural, economic and political opportunities for all and on the other hand its borderless nature has brought with it threats in the form of cyber-attacks and Informatics criminality[9].

*The **cyber-conflict*** is strictly determined by the informational and the network-based one and is a concrete form, customized for the crisis and war periods. It must not be mistaken for hacker actions or accidental infection of computer networks with computer viruses. It consists of a system of actions aimed in particular at disrupting or "blinding" by all means the adverse informational networks, the protection of their own, the misinformation of the opponent and his information intoxication.

If we admit that cyberspace is a space in which a complex confrontation with important state or non-state actors can take place, such as international terrorism or cross-border crime, then cyber conflict or cyber war is a phenomenon at confluence of several forms of confrontation between these actors, such as: imagistic war (media); psychological warfare; information / counter-information warfare; cyber terrorism; network-based war; command and control war; electronic warfare; cybercrime, etc.

The study of the means and methods of computer attack, as well as the identification of the purposes of these offensive actions, allows us to analyze and characterize threats from cyberspace, starting from the TESSO classical threats of the cyberspace.

[9] Col. (r.) prof. univ. dr. Gheorghe BOARU, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Ştiinţe ale Securităţii Naţionale nr.2/2017, p.65.

With the onset of cyber war, in response to computer aggressions, the specialists sought to define new cyber defense solutions that materialized in a complex set of offensive and defensive actions. In this framework, defensive actions to respond to IT security incidents, developed by specialized structures known as the ***C**omputer **E**mergency **R**esponse **T**eam* (***CERT***), have been developed and implemented at both civilian and military level.

At European level, there are key EU agencies, including the European Defense Agency (EDA), which work to develop the EU's cyber defense.

Moreover, it is essential for the EU to achieve the objectives it set in the Digital Agenda for Europe (2010), and equally significant, the driving force of such an agenda - the Europe 2020 strategy.

The EU Cyber Security Strategy (EUCSS) recognizes that "*it is primarily the responsibility of Member States to deal with security challenges in the virtual space"*[10], but also that the EU must play a key role as an actor in its own right within this „game".

In the same spirit of approach (EUCSS) states that *"Cyber-security can only be solid and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union ..."*[11].

To this end, it is clear that the EU can be a mediator to provide a platform or even a bridge between the different cyber security domains, to create the necessary conditions for an effective implementation of a cyber security culture within the Member States.

At national level, in February 2015, the National Strategy on the Digital Agenda for Romania 2020 was approved, in full agreement with the European actions, which defines four domains of action, of which only the first domain is mentioned: e-Governance, Interoperability, Cyber Security, Cloud Computing and Social Media.

This document has taken on and adapted to the specifics of our country the elements of the Digital Agenda for Europe. The Digital Agenda

[10] *Cybersecurity Strategy of the European Union*, Brussels, 7.2.2013, JOIN (2013) 1 final, p.4, [http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf], accessed on 10.03.2018.

[11] *Cybersecurity Strategy of the European Union, op. cit.*

thus defines the major role that the use of ICT must play in achieving the Europe 2020 objectives.

In Romania, the general framework of cooperation that brings together those authorities and public institutions with responsibilities and competences in the field of cyber security is represented by the National Cyber Security System (SNSC). SNSC's activity is coordinated at strategic level by the Supreme Council of National Defense.

The unitary coordination of SNSC elements is ensured by the Cyber Security Operational Council (COSC). Depending on the specific competencies in the field of national security and defense, each of the institutions represented in the COSC cooperates with the international bodies of the EU, NATO, OSCE, etc.

The Government of Romania, through the National Cyber Security Response Center - CERT-RO[12] - ensures, according to its competence, the elaboration and the promulgation of the public policies for prevention and counteraction of the incidents within the national cyber infrastructures.

As a national-specific element, in the sense of Cyber Security Strategy of Romania, ***cyber defense*** is defined as *"cybernetic actions in a timely manner against threats to cyber-specific infrastructures specific to national defense"* [13] .

It is worth highlighting that, in this area of cyber security, the Romanian approaches are in full agreement with the European ones but also with the NATO requirements.

The following aspects are considered in the formulation of cyber defense strategies:

- the multi-disciplinarity of the INFOSEC domain: it addresses issues related to staff, physical and document security, IT security and industrial security;

- the ability to react is responsive to the most diverse and unpredictable forms of cyber aggression;

---

[12] *Government Decision no. 494/2011* regarding setting up the National Response Center to Cyber Security Incidents - CERT-RO.

[13] *HG nr. 271/2013* for endorsing the *Romanian Cyber Security Strategy* and the National Action Plan regarding the Implementation of National Cyber Security, Annex no.1 at *Romanian Cyber Security Strategy*.

- cyber defense is also a complementary form of cooperation between people, organizations, alliances and states to combat *cyber crime*.

Defense against cyber-attacks is particularly complex and involves much more than simply using simple procedures or a single protection system. As an immediate response to computer aggression, the specialists sought to define new cyber defense solutions that materialized in a complex set of offensive and defensive actions.

If offensive actions are more of a military nature, it is recognized that defensive measures are the result of an effective collaboration of civil society with military organizations.

Thus, at present, it can be said that the defensive actions to respond to IT security incidents have best developed and implemented at both civilian and military level.

At present, NATO and Member States are at risk of cyber-attacks that may affect their physical or information assets, their international actions or their public image. Such attacks can be carried out for the purpose of misinformation, electronic espionage to obtain global competitive advantage, clandestine change of sensitive data within theaters of operations, or to alter or interrupt the operation of national critical infrastructures such as energy, water, fuel, communications, banking or transport, which are essential to the functioning of society and the economy.

At military level, they may target sabotage, subversion, espionage or terrorism, and are materialized in the exploitation / challenge of leakage of information, preventing missions, causing anomalies in the course of operations, etc.

As a rule, such acts may be motivated by gaining illicit gains or political advantages, and may be committed by persons, organizations or states that are capable of executing, inciting, transporting, transmitting or sustaining a threat by conducting actions and using automated processes to support / develop this capability. Depending on the actors involved and their motivation, cyber-attacks can be categorized as cybercrime, cyber terrorism or cyber-war.

Briefly speaking, our digital infrastructures have become national strategic assets and are now exposed to major security risks. The expeditionary nature of modern army missions, the deployment of operations based on the *Network Enabled Capability* (*NEC*), to allow

interoperability of coalitions, brings a new era of threats and challenges to the security of military operations.

The cyber war also determines the development of new strategies and new doctrines of organizing and conducting actions, able to answer new questions such as: what types of forces are needed, where and how they unfold, how they can hit the enemy, where and when computer and communications systems are positioned, what kind of computers, sensors, networks and databases are being used.

As the innovation of the war, cyber war became for the twenty-first century what "*lightning war*" (*blitzkrieg*) was for the twentieth century. Simplifying it to a minimum, cyber war is an extension of the importance of past actions to obtain information in the war: possession of superiority through command and control systems and realization of the opponent's surprise by discovering, locating, and misleading it.

The common feature of cyber-space confrontations is the continual antagonistic ratio established between cyber-threats - *terrorism, espionage, sabotage, subversion and organized crime, on the one hand, and information security* on the other. These threats manifest themselves in a very broad environment, offered by the information warfare, in an intense conceptual and action interference between *electronic warfare,* that of *hacker*, *psychological*, *economic* and a complex typology of *computer attacks*.

Given that it is a Defense Alliance, NATO identified and recognized, even at the beginning of the past decade, the gravity of cyber threats and the importance of protecting information networks.

Cyber defense appeared on NATO agenda at the Prague Summit in 2002 and was subsequently confirmed as a priority at the Riga Summit in 2006. A policy in this field was agreed on for the first time by the Heads of states and governments at the Bucharest Summit in April 2008.

The rapid evolution of the attacks and their sophisticated character determined the placement of the theme at the center of NATO's security agenda. Thus, the Lisbon Summit (2010) adopted a **Strategic Concept** that mentions cyber threats, pointing out that *"they can directly target the security of vital national infrastructures and reach levels that could*

jeopardize «prosperity, security and national and Euro-Atlantic stability»"[14].

Accordingly, this type of challenge requires that the Alliance develop its capacity to prevent, detect and defend against them, to recover from their emergence, ***to strengthen and coordinate national cyber defense capabilities.***

Analyzing the essence of the Lisbon Summit, we find that while the Strategic Concept set the NATO Strategy for the next decade, the Summit Declaration provided for an in-depth review of the current allied policy aimed at ***adapting it to the security environment.***

The next step was at the Wales Summit (2014), where NATO Heads of State and Government confirmed, empowered and endorsed the new Enhanced Cyber Defense Policy that underlines the fact that ***cyber defense*** *is part of NATO's basic* ***collective defense***.

I believe that particularly important for the field dealt with in this article, is the **NATO Summit in Warsaw** (8-9 July 2016) to which the Heads of State and Government participating in the North Atlantic Council meeting drew up a joint statement with 139 points, of which some (points 5, 47, 70) refer even to the types of threats that I have mentioned in this article, from state and non-state actors - from military forces, but also from the side of terrorist, cyber-attacks or hybrids.

The importance attached to this issue at NATO level is also demonstrated by the fact that at the **Warsaw** Summit some issues discussed at the Summits in **Bucharest** (2008), **Lisbon** (2010), **Chicago** (2012) and **Wales** (2014).

Cyber -attacks can directly affect information flows flowing in the military command and control systems, and in Warsaw it was said that *"It is increasingly important to develop our ability to understand, pursue and, at the same time, anticipate the actions of potential adversaries, through Information, Recognition and Surveillance (IRS) capabilities, and comprehensive information exchange agreements. These are essential to enabling timely and informed political and military decisions. We have set*

[14] NATO, *Apărarea cibernetică*, [https://nato.mae.ro/node/435].

the appropriate capabilities to ensure the speed of response to our forces with the highest degree of promptness"[15].

NATO officials believe that cyber-attacks pose a clear challenge to Alliance security and could be as damaging to modern societies as conventional attacks. It was reminded on this occasion that NATO has a *defensive mandate* and that *"cyber-space is considered as a field of operations in which NATO must defend itself as effectively as in the air, on the ground or at sea"* [16].

In the same context, the participants at this summit, who, in my opinion, were most relevant to the field of cyber defense, voiced their support for NATO's widespread deterrence and defense actions in which cyber defense will continue to be integrated into the planning operational and Alliance operations and missions, and that they will work together to contribute to their success.

The statements made by participants highlight this: *"We are continuing to implement NATO's cyber defense policy and to strengthen NATO's capabilities in cyber defense benefiting from state-of-the-art technologies. We reaffirm our commitment to acting in accordance with international law, including the UN Charter, international humanitarian law and human rights legislation, as the case may be"*[17].

The NATO Defense Ministers meeting held in Brussels on 14 February 2018 also aimed at implementing the decisions previously made at the Warsaw and Wales Summits on defense and deterrence, discussions on the size the design of stability and the fight against terrorism as well as NATO-EU cooperation.

Military analysts believe that the outcome of the talks will help shape the framework for addressing this issue at the NATO Summit in Brussels in July 2018.

During the talks, the Romanian President welcomed the progress made in the implementation of the Forward Presence, stressing the need for *"by decisions to be adopted at the Brussels Summit this year to ensure unity,*

[15] *WARSAW SUMMIT DECLARATION*, adopted by the chiefs of state and government participating in the Reunion of North Atlantic Council in Warsaw (8-9 July 2016), line 47, [https://www.mae.ro/node/36635].
[16] *WARSAW SUMMIT DECLARATION, op. cit.,* pct. 70.
[17] *WARSAW SUMMIT DECLARATION, op. cit.*

consistency and consolidation of allied measures on the Eastern Flank as part of NATO's deterrence and defense posture"[18].

I consider and hope that the political-military activities that have taken place and which will follow at NATO, EU and national level will contribute to the development of international / national norms and / or regulations that raise the level of responsible behavior of states and measures to increase confidence in cyberspace.

Conclusions

I believe that the specific threats to cyber security, which have become increasingly serious in recent years, are also due to the fact that they are not limited by borders and that they are constantly increasing in frequency and degree of sophistication, but also in their universal membership of the cyber space. The security risks which involves cyber-attacks and the global nature of their effects call for joint international cooperation efforts to ensure the security of the information systems of the Alliance's member states.

Documents drawn up by NATO member states reaffirm the principles of Allied security indivisibility as well as prevention, detection, resilience, recovery and defense. They remind that NATO's fundamental responsibility in the field of cyber defense is to defend its own networks and that Alliance assistance must be addressed in accordance with the spirit of solidarity, underlining the Allies' responsibility to develop relevant capabilities in to protect their own national networks.

BIBLIOGRAPHY

*** *Cornerstones of Information Warfare*, Department of the Air Force, Washington DC, 1995.

*** *Cybersecurity Strategy of the European Union*, Brussels, 7.2.2013, JOIN (2013) 1 final, http://eeas.europa.eu/ archives/docs/-policies/eu-cyber-security/cybsec_comm_en.pdf.

[18] http://www.amosnews.ro/iohannis-s-intalnit-cu-ministrii-apararii-ai-cele-noua-state-membre-nato-din-flancul.

*** *Declaraţia Summit-Ului din Varşovia,* Adoptată de şefii de stat şi de guvern participanţi la reuniunea consiliului nord atlantic din varşovia (8-9 Iulie 2016), pct. 47, https://www.mae.ro/-node/36635.

*** *HG nr. 271/2013* pentru aprobarea *Strategiei de securitate cibernetică a României* şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, Anexa nr.1 la Strategia de securitate cibernetică a României.

*** *Hotărârea de Guvern nr. 245/7 aprilie 2015* prin care se aprobă *Strategia Națională privind Agenda Digitală pentru România 2020.*

*** *Hotărârea de Guvern nr. 494/2011* privind înfiinţarea *Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO.*

*** *Internet World Stats*, [http://www.internetworldstats.com/stats.htm].

*** NATO, *Apărarea cibernetică* , [https://nato.mae.ro/node/435].

*** *Statisticile lumii în timp real*, [http://www.worldometers.info/ro/].

BOARU G., *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Ştiinţe ale Securităţii Naţionale nr.2/2017.

GRIER P., *Information Warfare, Air Force Magazine*, No. 3, March 1995.

PETRESCU S., *Informaţiile a patra armă*, Editura Militară, Bucureşti, 1999.

http://www.amosnews.ro/iohannis-s-intalnit-cu-ministrii-apararii-ai-cele-noua-state-membre-nato-din-flancul.

http://www.insse.ro/cms/sites/default/files/com_presa/com_pdf/tic_r2016.pdf.

hotnews.ro.

https://www.bloomberg.com/.