THE 5TH OPERATIONAL DOMAIN AND THE EVOLUTION OF NATO'S CYBER DEFENCE CONCEPT

***Mihai-Ştefan DINU, PhD*[1]**

Abstract: *The acknowledgement of the cyber domain as the fifth one – after land, sea, air and space – along with an unprecedented technological development have led to a change. A change in security culture and mentality, education and practice, change that is being shaped by the academic knowledge, trained in laboratories and practiced in organizations.*

The paper focuses on the undeniable relation between the outstanding developments of information society, along with the increasing types of threats against it, threats that tend to target every national security domain and the measures taken against those threats.

Key words: *Cyber domain, the 5th domain, information society, NATO's cyber defense concept, education*

1. Introduction

When it comes about the Cyber domain, a vast number of authors refer to William Gibson's novel *Neuromancer*. There is no doubt that modern human life of the 21st century could not be perceived in its entirety without the significant role of technology, especially information and communication technology (ICT). Indeed, ICT permitted in the last two decades a burst regarding not only the professional level of communication and information of human activities, but also to the individual intimate level of every individual. Along with these aspects of human life, research and development activities benefitted of the means provided by the

[1] Senior Researcher at the Information Systems Department of Security and Defense Faculty, „CAROL I" National Defense University

technological development. However, as researchers, educators and professionals we must mention the fact that Yoneji Masuda in his work *The Information Society as Post-Industrial* Society depicted the emergence of ICT in human society several years before the appearance of William Gibson's novel[2]. Thus, Masuda promoted information utility as the main production center of information society. In his perspective, the information utility consists in information networks and data banks[3], in other words a public infrastructure based on interconnected computers.

In the same period when Masuda's view was being promoted, another significant event was taking place: The Internet emerged public from the military testing laboratories. Initially perceived as a tool that facilitated communication, the Internet rapidly expanded its functions along with the implementation on extended geographic areas.

Today, the Internet is not only a technological tool. In 2011, the United Nations declared in a report issued by the Special Rapporteur Frank LaRue on the promotion and protection of the right to freedom, opinion, and expression that by the fact that it facilitates the realization of a range of other human rights[4], the access to internet is a fundamental right. This statement comes in the context in which, 11 years earlier, Estonia legislated[5] Internet access as a basic human right, in the year 2009 France Constitutional Council[6] declared it a fundamental right and, similarly, a 2010 decision[7] of Costa Rica Constitutional Court.

Obviously, the free access to internet did not attract only positive actions, but also criminal ones. The vast virtual cyberspace becoming populated not only with actors offering social, educational or professional

[2] Yoneji Masuda, *The Information Society as Post-Industrial Society*, World Future Society, Washington D.C., 1981

[3] *Ibidem*, pp.30-33

[4] ***, A/HRC/17/27/ - *Report of the Special Rapporteur on the promotion and protection of the right to freedom and opinion and expression, Frank LaRue*, United Nations' General Assembly, 16 May 2011, p. 7

[5] Stephen Tully, *A Human Right to Access the Internet? Problems and Prospects,* in Human Rights Law Review, vol. 14, Issue 2, Oxford University Press, pp. 175-195

[6] ***, Decision no. 2009-580 of June 10th 2009 at www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf (14.02.2017)

[7] Sala Constitutional, *La Sala en la Prensa 2010(2011) p.* 118 at www.poder-judicial.go.cr/sala-constitutional/documento/salaenpresa2010.pdf (14.02.2017)

tools but with diverse criminal actors whose actions lead to decisions taken by vast majority of nation states to legally, politically and technically protect their infrastructures against cyber-attacks.

2. Cyberspace the 5th operational domain

The existence of cyber acts in 2007 in Estonia as well as in 2008 in Georgia, led to the conclusion that cyberspace can be a battlespace. Therefore the Internet, a generally used tool after its original development in the military labs, returned to its starting activity domain, through the opportunities opened by the technological development, and got a militarized dimension. Moreover, the 2014 events in Ukraine were preceded by an orchestrated cyber- attack on communications, cell networks jamming and internet connections severing, in a Russian attempt to obtain an information blackout[8].

On this background, military organizations realized the fact that successful results of the conventional military operations are increasingly dependable on or enabled by the access to cyberspace together with the access to civil critical infrastructure within both the national borders and foreign operational theatre. In this sense most states started to develop cyber security strategies, along with the necessary doctrine to support cyber operations. Cyber Defense concepts were developing both at national and international level.

A very illustrative example is the evolution of NATO Cyber Defense Policy.

3. Evolution of NATO Cyber Defense Concept

As a political-military alliance NATO has always focused on its communication and information systems, so when an Alliance Web server had been shot, down back in 1999, by a series of attack DDoS type, military leaders understood that bombs could also be logical, as the investigations they performed revealed traces leading to Serbian military[9]. As a result,

[8] Shane Harris, *Hack attack*, Foreign policy, 3 March 2014 at http://foreignpolicy.com/2014/03/03/hack-attack/.

[9] Ellen Messmer, *Serb supporters sock it to NATO, US web sites*, CNN, 6 April 1999, at http://edition.cnn.com/TECH/computing/9904/06/serbnato.idg/index.html

starting with the 2002 NATO Summit held in Prague, the Alliance has been developing NATO Cyber Defense Concept.

We can consider that so far, the development of afore mentioned concept has had five successive stages, as follows (table no. 1).

STAGE	YEAR	SUMMIT	MILESTONES FOR CONCEPT DEVELOPMENT
1ST - Recognition	2002	Prague	NCIRC establishment
2nd – Foundation	2008	Bucharest	NCD Policy 1.0
3rd - Centralization	2010	Lisbon	•Capability targets in NATO Defense Plan Process •Information Sharing •NCD Policy 2.0 •Investments
4th – Enhancement	2014	Wales	•NCD 3.0 •Legal issues •Creation of Cyber Range •Fostering Partnerships
5th - Adaptation	2016	Warsaw	•Cyber Defense Pledge •Cyberspace as the 5th operational domain •Partnerships at national and international level with industry and academia

Table no. 1. Evolution Stages of NATO Cyber Defense Concept

The main characteristics of each stage will be further discussed.

The first stage, RECOGNITION, constituted a purely technological approach, with exclusive focus on protection of key NATO systems as a result of recognition of cyber threats to NATO networks. It is the creation stage of NCIRC (IOC)[10]

The second stage, FOUNDATION, at Bucharest Summit, represents in fact the first step in policy approach by:

•Issuing NCD Policy 1.0

[10] NATO Computer Incident Response Capability

- Adopting 1st Policy following 2007 cyber-attacks in Estonia
- Establishing objectives and principles (NATO and allies' responsibilities)
- Organization of CDMA[11] structure, later CDMB[12]

The third stage, CENTRALIZATION, represents the moment when:

- NCD Policy 2.0 was issued
- Lisbon Strategic Concept was launched
- 2nd policy was adopted (June 2011)
- Protection was centralized through NCIRC (FOC) with 80 million euro invested
- Cyber defense capability targets were agreed upon in the framework of NATO Defense Planning Process
- Information Sharing Mandate was issued

In the fourth stage, ENHANCEMENT represents moment when cyber defense was directly linked to NATO's core task of collective defense and, additionally, the following aspects were settled:

- The applicability of international law in cyberspace was recognized
- The focus on training, education and exercises was enhanced
- The creation of cyber range was decided upon
- The Enhancing Information Sharing process was initiated, including MISP
- Calls for partnership were launched, including industry

The current stage, ADAPTATION, shows a focus on:

- Strengthening and enhancing national cyber defense capabilities as a matter of priority by issuing Cyber Defense Pledge
- Recognition of cyberspace as a domain of operation in which NATO must defend itself as effectively as in the air, on land, at sea and in space.
- Starting new and enhancing existing partnership with countries, international organizations, industry and academia.

[11] Cyber Defense Management Authority
[12] Cyber Defense Management Board

4. Implications of the NATO Cyber Defense Concept on CAROL I NDU educational process

"Carol I" National Defense University as a military educational, research, and cultural flagship, shared NATO's assumed mission to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in the field of cyber defense through education, research and development, lessons learned in order to accumulate, create and disseminate knowledge by its many degree programs at several levels and forms of university education: doctoral programs, masters, undergraduate programs, open education distance majors, and other training courses.

Consequently, in the framework of "Carol I" NDU the Military Information Systems and Defense Information Department (MISDID) was developed, whose specialized programs cover research and educational aspects regarding the cyber defense field. Moreover, the Information Systems Department manages graduation and post-graduation programs for officers and for the civilian students. Thus, Information Systems graduation program is open to any civilian student who might want to attend it, following an exam, as the positions are limited to a number of 25 each year. Subsequent to the admission to the graduation program, the students will benefit from training with the NDU professors and internships in different organizations in the field. Considering the fact that during the three years' study program the disciplines are gradually developed toward cyber security leadership essentials, many classes are destined to cover hands-on activities in the Cyber Defense Laboratory. In the lab, students have the opportunity to practice their theoretical knowledge and develop their skills participating in practical exercises on network vulnerabilities, cyber threat detection, active defense and incident response or red team-blue team type of exercises. The main objective of theoretical knowledge and laboratory training is not only to learn about security, but also to learn about *managing* security.

Along with afore mentioned program, MISDID manages a number of 13 post-graduation programs in the department fields of study and an MA program in the field of communications, IT and cyber defense.

During their study program, students have the opportunity to enroll in third party specialized courses: Juniper, Mikrotik, CISCO etc.

At the same time, professors and some selected students take part in an annual project targeted at the development of cyber security culture named *Cyber-security for the jeans generation.* The project consists in activities that take place in high schools, mainly workshops led by MISDID professors/researchers and students in which high school students and teachers are invited to participate actively.

The initial start of the project was grounded on several issues that emerged due to the large use of modern ITC devices:

- Protection of privacy
- Personal data protection[13]
- Cyber bullying
- Cyber harassment
- Increased frequency of cyber-attacks targeting single individuals

Therefore, this project is based on the idea that creating and developing a cyber security culture will lead in fact to the creation and development of a certain behaviour, namely the security behaviour of the users who interact with different types of information and communication technology in the large framework of ideas and values developed in the cyber security field.

A solid research dimension grounds all previous educational programs, activities and projects. Inspired by the guidelines projected in the "Carol I" NDU Research Strategy, research is conducted in MISDID by the heads of chair in the field of information systems, communications, intelligence and cyber defense, in the collaboration with the department researchers in the framework of department board.

Outside NDU, the research dimension is developing mainly on four main cooperation efforts:

- Centre of Excellence for Advanced Technologies in Cyber Security (coordinated by the Military Technical Academy) – training courses and exercises, research and innovation to address cyber security challenges, developing best practices and guidelines to identified cyber security solutions, solutions for protecting communication and information system,

[13] Mihai-Ştefan DINU, *Emergence of a discipline: Information Law*, in Annals Series on Military Sciences, Volume 9, Number 1, 2016, pp. 52-59.

developing collaboration and information sharing between academia and industry;

- Research Center for Navy – theoretical ground for identification of risk factors in littoral areas, cyber security management policies and procedures etc.
- Private companies which main activity lies in cyber security domain – internships, documentary stages, scientific event, research project competitions
- Independent think-tanks focused on cyber domain – creating and developing knowledge hubs, fostering dialogue between decision makers and academia, leadership and policy projections etc.

5. Conclusions

In the cyber defense domain NATO focuses formally and de facto on the doctrine, which proves to be a defensive one, as NATO does not approach the use of offensive cyber operations. The complex and very dynamic nature of challenges rising in cyberspace leads NATO towards establishing a solid direction in education, training and exercises. In this respect, "CAROL I" NDU education and research programs are evolving at the same time with NATO Cyber Defense Concept, nowadays professors and researchers grounding the standards for legal evaluation of cyberspace acts, meantime developing a cyber defense culture not only at military organization level, but also for the civilian segment.

BIBLIOGRAPHY

*** A/HRC/17/27/ - *Report of the Special Rapporteur on the promotion and protection of the right to freedom and opinion and expression, Frank LaRue*, United Nations' General Assembly, 16 May 2011;

*** Decision no. 2009-580 of June 10th 2009 at www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/-2009_580dc.pdf (14.02.2017);

DINU M.Şt., *Emergence of a discipline: Information Law*, in Annals Series on Military Sciences, Volume 9, Issue 1, 2016;

HARRIS S., *Hack attack*, Foreign policy, 3 March 2014 at http://foreignpolicy.com/2014/03/03/hack-attack/;

MASUDA Y., *The Information Society as Post-Industrial Society*, World Future Society, Washington D.C., 1981;

MESSMER E., *Serb supporters sock it to NATO, US web sites*, CNN, 6 April 1999, at http://edition.cnn.com/TECH/computing/9904/-06/serbnato.idg/index.html;

Sala Constitutional, *La Sala en la Prensa 2010(2011)* at www.poder-judicial.go.cr/sala-constitutional/documento/salaenpresa2010.pdf (14.02.2017);

TULLY S., *A Human Right to Access the Internet? Problems and Prospects*, in Human Rights Law Review, vol. 14, Issue 2, Oxford University Press.