# NATO'S CYBER SECURITY AND DEFENSE. BEFORE AND AFTER 2014 WALES SUMMIT

**Iulian F. POPA**
**Ph.D. candidate**
**Babeş-Bolyai University, Cluj-Napoca**
**ifp2@georgetown.edu**

**ABSTRACT**
*UNTIL RECENTLY, CYBER THREATS WERE CONSIDERED A QUASI-LIMITED SECURITY RISK. HOWEVER, THE WIDESPREAD OF ICT IN THE LAST DECADE CAUSES A SIGNIFICANT INCREASE IN CYBER RISKS, VULNERABILITIES, AND THREATS TO BOTH NATIONAL AND INTERNATIONAL SECURITY. UNDOUBTEDLY, NOWADAYS, CYBERSPACE IS A STRATEGIC ENVIRONMENT AS VALUABLE AS THE LAND, AIR, SEA OR SPACE DOMAIN. IN ESSENCE, THIS PAPER HIGHLIGHTS THAT CYBER SECURITY AND GOOD GOVERNANCE SHOULD NOT BE NEGLECTED IN ANY WAY BY ANY STATE OR NON-STATE COMPETITIVE ACTORS. IN PARTICULAR, THIS PAPER SELECTIVELY EXAMINES THE PATHWAYS FOLLOWED BY NATO, THROUGH CONTINUOUS REFORM, MODERNIZATION, AND TRANSFORMATION, TO ADAPT ITSELF AND EFFECTIVELY RESPOND TO INFORMATION AGE CHALLENGES WITHIN CYBERSPACE. NOT THE LEAST, THIS PAPER SELECTIVELY DISCUSSES THE USE OF (ARMED?) FORCE, IF ANY, WITHIN CYBERSPACE AND CYBER OPERATIONS, USING A CONSTRUCTIVE AND THEORETICAL APPROACH.*

***KEYWORDS**: CYBER SECURITY, CYBER DEFENSE, NATO, CYBER DEFENSE.*

## Introduction

There is no serious doubt that the achievement of both security and insecurity, along with the producing and dissemination of information or knowledge are factors largely available to almost anyone due to the Information Age [1].

More precisely, we currently witness various and profound transformations that take place inside a world driven by constant uncertainties, poorly predictable, where the large-scale digital/cyber phenomena – besides undeniable positive contributions, set the foundations of a new "reality", not that peaceful as may have been expected years ago.

Besides this, however, cyberspace still offers countless highly valuable opportunities for rapid information and knowledge dissemination into timely decisions and operational flexibility, far beyond those offered by the tangible reality. In this regard, once for all, it should remembered that cyber security – hereinafter referred as CYBERSEC – the seventh conceptual dimension of security, is above all the most valuable liaison factor between military, economic, social, societal, human, and, more recently, environmental security dimensions; even though the current expansion of cybercrime, cyber terrorism, and cyberwarfare (read as cyber conflict) have extensively transformed the cyberspace into a "battlefield" characterized by a myriad of unpredictable and asymmetrical challenges.

However, compared to tangible reality which we live in, the "cyber arena" is by no means different: it's dynamic, relatively quiet, expansive, and difficult to shape in accordance to (very often) divergent security interests of various global cyber actors.

Therefore, although it has become a truism so far, the deep and profound understanding of cyberspace dynamics is crucial not only for main international actors such as NATO, but also for any competitive, both public and private, transatlantic organization which places cyber security at its heart, as long as cyber threats lead, at least in theory, to significant changes in the physiognomy of both (contemporary) security and defense concepts. Perhaps now more than ever, CYBERSEC, good governance, and CYBERDEF should be of great interest for the entire spectrum of global decision makers, as the use of commercial airliners to initiate and launch terrorist attacks has proven us that *almost anything may become a valuable weapon [2]*.

### *1. Cyber security and defense within NATO. Preliminary remarks*

NATO was among the first international organizations which have expressed firmly their concerns over the security, good governance, and defense within cyberspace.

In fact, one may appreciate the specific issues regarding the security and the stability of cyberspace came into NATO’s sight even since the `90s, when the conflict in the former Yugoslavia has acquired a clear “cyber warfare” dimension. Years later, the unprecedented cyber-attacks over Estonia (2007) – resulting in serious damage to critical cyber infrastructures brought once again to the forefront the NATO's concerns the decision-making and operational hurdles posed by the security threats within cyberspace. As a consequence, upon the 20th NATO Summit (Bucharest, 2008) the Alliance has officially approved its own "cyber defense policy" (officially known as the *NATO Policy on Cyber Defense*), in order to sanction *de jure* CYBERSEC and CYBERDEF as a top priority. Withal, starting 2008, following the initiative of Estonia, Germany, Hungary, Italy, Lithuania, Latvia, Netherlands, Poland, Slovakia, Spain, and US, the *Cooperative Cyber Defence Centre of Excellence* (CCD COE, Tallinn) was established. The CCD COE’s mission *is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.* Also the *Centre is a research and training facility which tries to take a broad look on cyber defence, mixing and matching different areas of research under the cyber umbrella [3]*.

In the same time, since the revision of its Strategic Concept in 2010, NATO formally recognizes cyber threats as a very serious set of challenges to its prosperity, security, and stability. Since that time, but not necessarily as a direct consequence, the Alliance along with MS pay at least formally a greater attention on protecting ICT systems and critical infrastructures, by enhanced monitoring and cyber awareness, along with improved incident response cooperation and resilience. In fact, to properly achieve these goals, it is worth mentioning NATO has adopted its own "cyber defense policy" (namely *NATO Policy on Cyber Defence* – revised version) and its own action plan in cyberspace (*NATO Cyber Defence Action Plan*) [4] – to be extensively discussed later on.

### *2. Cyberspace and the use of (armed?) force. An everlasting dilemma?*

Years ago cyber threats were not as pervasive as compared to nowadays. Consequently, NATO is greatly concerned about the security challenges within cyberspace, along with preventing or mitigating nuclear proliferation, global terrorism, and cross-border crime by means of collective defense, crisis management, and cooperative security [5].

In particular, concerning operations within cyber domain it is worth mentioning that some experts are still reluctant [6] about resorting to collective defense under the famous Article No. 5 in case of cyber incidents/attacks/threats which involve directly or indirectly the use of (armed?) force – if any. In this respect, no less true is that a gradual separation among different or various „use of force” levels is theoretically almost impossible to define at the moment in the absence of any precisely quantifiable kinetic impact. As such, it may be considered that cyber-attacks which imminently and significantly cause damage to national security, critical goods or casualties among human beings constitute undoubtedly, even if generically, “use of force”. Therefore, one may appreciate that cyber-attacks which threat the human beings integrity or cause significant material disruption or destruction, within and/or outside cyberspace, qualify undoubtedly as acts of use of force under the auspices of UN Charter. In fact, in this respect it is worth remembering that *cyber war differs from the traditional idea of war in that it does not necessarily make use of physical violence, although it may have indirect violent consequences. Physical violence thus marks a basic difference, at least in the premise, if not in the consequences, of kinetic and cyber-attacks[7].*

That said, any use of cyber force without any complementary conventional use of force is unlikely to fall under the auspices of Art. No. 51 of the UN Charter and Art. No. 5 of the North Atlantic Treaty [8]. Therefore, it should be broadly admitted that any military response to cyber incidents/threats/attacks, even in self-defense (!), accomplished using any conventional and non-cyber means may seriously breach the international law.

### *3. Governance instruments in support to security and defense within NATO*

Table no. 1, Institutions and departments within NATO holding cyber-related responsibilities (cf. Atlantic Council [9])

| **Institution / Department** | **Role** |
|---|---|
| ESCD - (NATO Emerging Security Challenges Division) | *The Division deals with a growing range of non-traditional risks and challenges in the field of terrorism, WMD proliferation, cyber defence, and energy security. It brings together various strands of expertise already existent in different parts of NATO Headquarters to provide NATO with a Strategic Analysis Capability and therefore to monitor and anticipate international developments that could affect Allied security [10].* |
| NATO Communications and Information Agency (NCIA) | *The Agency was established on 1 July 2012, under the Charter of the NCIO as a result of the merger of the former NATO Consultation, Command and Control Agency (NC3A), the former NATO Air Command and Control System Management Agency (NACMA), the former NATO Communication and Information Systems Services Agency (NCSA [except Deployable CIS]), the former Active Layered Theatre Ballistic Missile Defence (ALTBMD) Programme Office and NATO HQ Information Communication, Technology Management (ICTM) and constitutes an integral part of the NATO.*<br>*As part of its missions and as NATO’s principal CIS service provider, the NCI Agency will in particular have to be capable of ensuring continuous CIS support to all on-going operations in which NATO is engaged, responding in particular to SACEUR’s needs and taking his* |

| | |
|---|---|
| | *stated priorities into account. Overall, the structures of the new Agency will bring along economies of scale, through co-location and partial centralisation of functions, an integrated life-cycle approach, the sharing of best practices, increased commonalities and standardisation, a strong cooperation with relevant stakeholders and more effective governance. Additionally, the proposed establishment should ensure improved coherence of the Agencies' missions through more transparency, accountability and better coordinated strategic direction[11].* |
| NATO Cyber Defense Management Board (CDMB)<br>- CDMA - | *Out of the Bucharest Summit, the Alliance leadership established two major cyber defense institutions: the Cyber Defense Management Authority (CDMA) and the Cooperative Cyber Defense Center of Excellence (CCDCOE). The CDMA – under the governance of the Cyber Defense Management Board (the main NATO governance body for cyber defense) – became fully operational in April 2008 to initiate and coordinate cyber defenses, review capabilities and conduct appropriate security risk management. CDMA also helps member states to improve their own national CYBERDEF capabilities. CDMB comprises both NATO political and military leaders, along with operational and technical staffs holding responsibilities for CYBEREF. CDMB coordinates CYBERDEF activities throughout NATO HQ and associated commands and agencies. The Board operates under auspices of HQ NATO ESCD[12].* |
| NCIRC Coordination Centre | *The Alliance's "first responders" to prevent, detect, and respond to cyber incidents. Handling and reporting incidents and disseminating important incident-related information to system/security management and users[13].*<br>NCIRC works under CDMB and North Atlantic Council. |
| ACT - Allied Command Transformation | *ACT is NATO's leading agent for change, driving, facilitating, and advocating continuous improvement of Alliance capabilities to maintain and enhance the military relevance and effectiveness of the Alliance[14].* |
| NATO Communications and Information Systems School (NCISS) | Provides specialized advanced training and assistance, for both NATO and Non-NATO countries, to military and civilian personnel involved in the field of communications and information systems [15]. |
| NATO School (Oberammergau) | Conducts highly developed cyber training and education. |
| NATO CCD COE - Cooperative Cyber Defense Center of Excellence | *Its mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation [16].* |

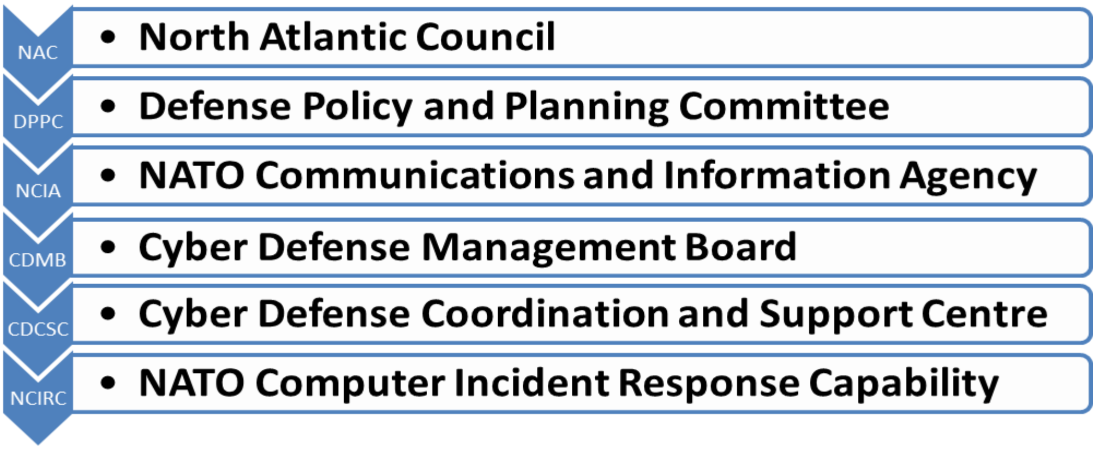
NAC
• North Atlantic Council
DPPC
• Defense Policy and Planning Committee
NCIA
• NATO Communications and Information Agency
CDMB
• Cyber Defense Management Board
CDCSC
• Cyber Defense Coordination and Support Centre
NCIRC
• NATO Computer Incident Response Capability

Fig. no. 1, NATO Cyberspace Governance – Schematic Institutional Chain Diagram (Source: Security Affairs [17])

### *Concluding remarks*

As well as for any other similar political or military organization throughout the world, the next five years will be critical for NATO in terms of decision-making and operational or tactical strategies concerning security, good governance, and defense in cyberspace.

As we have seen, speaking in terms of policies, strategies, best practices, and standards for cyber security and defense, the developments which took place in recent years within the Alliance were indeed important steps forward, but yet not enough to fully and effectively ensure the collective cyber defense of the Alliance and its members.

However, it is worth mentioning NATO stands out nowadays as one of the most proactive international organizations which fights against cyber threats, as it is seriously and continuously engaged in improving its capabilities and resilience within cyber domain using even approaches that proved their efficiency over time in other strategic domains like land, sea, air or space. In this respect, are extremely welcomed the past years initiatives of the Alliance regarding the establishment and development of new and fully operational early warning and rapid response systems to cyber incidents, despite defense budgeting issues or internal challenges regarding inter-coordination, continuous training, and cooperation within cyber domain among the members of the Alliance.

In fact, in the long run, NATO is expected to pay greater attention on (good) cyber governance, better early warning, deterrence, and efficient cooperation and resilience within cyber domain. In particular, as stated above, I believe NATO holds currently optimal legal and operational instruments to tackle most of the cyber threats and engage lawfully in cyber operations that might fall under the public international law (see the discussion above on Article 5 and cyber domain) [18].

Finally, despite the "collective fatigue" of its MS [19], I appreciate that future efforts of NATO should start or continue to focus mainly on three main directions, namely:

a. implementing of a "phased adaptive approach" within cyber domain, (e.g. CDPA - Phased Adaptive Approach Cyber Defense), similar to ABM defense;

b. supporting both state and non-state actors within the Alliance to continuously improve or develop new cooperative cyber incident response systems for better resilience and intelligence sharing;

c. continuously supporting research and development in the areas related to CYBERSEC and CYBERDEF by adequate budgeting [20].

*[This work was possible due to financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number POSDRU/159/1.5/S/140863, with the title Competitive Researchers in Europe in the Field of Humanities and Socio-Economic Sciences. A Multi-regional Research Network.]*

## REFERENCES

[1]. George Cristian Maior, „Analistul şi beneficiarul de informaţii: rolul analistului în cunoaşterea strategică", în George Cristian Maior, Ionel Niţu (coord.), Ars Analytica: Provocări şi tendinţe în analiza de intelligence, Bucureşti, Editura RAO, 2013, p. 35.

*[2]. Ibidem.*

[3]. (NATO) CCD COE, Our Work, available at https://www.ccdcoe.org/our-work.html, accessed on August 3, 2014.

[4]. *, NATO and Cyber Defence, 2013, available at http://www.nato.int/cps/ro/natolive/topics_78170.htm, accessed on August 2, 2014.

[5]. *Strategic Concept – Active Engagement, Modern Defence,* 19-20 noiembrie, 2010, available at http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, accessed on August 4, 2014.

[6]. Emine Akcadag, „NATO and the fight against the cyber-threat", in *Atlantic Voices / The Growing Cyber-Threat – What role for the Transatlantic Alliance?,* vol. 2, no. 5, 2012, pp. 4-10.

[7]. Masimo Durante, „Violence, Just Cyber War and Information", în *Proceedings of 1st Workshop on Ethics of Cyber Conflict,* Ludovica Glorioso, Anna-Maria Osula (ed.), Tallinn, NATO CCD COE, 2014, pp. 61-64.

[8]. Michael N. Schmitt (ed.), *Tallinn Manual on The International Law Applicable To Cyber Warfare,* New York, Cambridge University Press, 2013, pp. 49-52.

[9]. *, "Transforming Towards a Smarter Alliance: NATO's Role in Cyber Security", in *Atlantic Councul Issue Brief,* february, 2012, pp. 2-4, available at http://www.atlanticcouncil.org/publications/issue-briefs/natos-cyber-capabilities-yesterday-today-and-tomorrow, accessed on August 3, 2014

[10]. *, *New NATO division to deal with Emerging Security Challenges,* August 4, 2010, available at http://www.nato.int/cps/en/natolive/news_65107.htm, accessed on August 3, 2014.

[11]. *, *NATO Communications and Information Agency – Interim Customer Catalogue 2014 of C4ISR Services,* December, 2013, p. 5, available at https://www.ncia.nato.int/, accessed on August 4, 2014.

[12]. Jason Healey, Leendert van Bochoven, "Transforming Towards a Smarter Alliance: NATO's Role in Cyber Security", in *Atlantic Council Issue Brief,* February, 2012, pp. 2-4, available at http://www.atlanticcouncil.org/publications/issue-briefs/natos-cyber-capabilities-yesterday-today-and-tomorrow.

*[13]. Ibidem.*

*[14].* *, *NATO's Allied Command Transformation (ACT),* available at http://www.act.nato.int/mission, accessed on August 4, 2014.

[15]. NCISS, *About Us,* available at https://www.nciss.nato.int/mission.php, accessed August 5, 2014.

*[16].* (NATO) CCD COE, *History,* available at http://www.ccdcoe.org/history.html, accessed on August 4, 2014.

*[17].* Pierluigi Paganini, *NATO has constituted Cyber Response Teams*, December 24, 2013, available at http://securityaffairs.co/wordpress/20705/cyber-warfare-2/nato-attack-response-teams.html, accessed on August 3, 2014.

*[18].* [Following the summit held in Wales, NATO formally extended the Joint Defense Concept on CYBERDEF, meaning that a major cyber attack on the Alliance could trigger collective military action according to the famous Article 5.

*[19]*. Elise Labott, "NATO's post-Afghanistan future unclear", May 18, 2012, available at http://security.blogs.cnn.com/2012/05/18/natos-post-afghanistan-future-unclear/, accessed August 3, 2014.

*[20]*. Jason Healey, Leendert van Bochoven, *op. cit.*, p. 7.