AARMS Vol. 12, No. 1 (2013) 83–91. **10.32565/aarms.2013.1.10**

The NATO Policy on Cyber Defence: The Road so Far

SZENTGÁLI Gergely[1]

In recent years news about cyber attacks targeting states, corporations and individuals have been steadily increasing. There is no doubt that more and more emphasis is being placed on the threats emerging from cyberspace. Security experts agree that the question of cyber security has become one of the most important challenges of the new millennium. The aim of this paper is to examine the issue from NATO's perspective by analyzing the accomplishments to date - the road so far.

Introduction

NATO faced cyber warfare for the first time during the 1999 air campaign in Kosovo. The military intervention, called operation *Allied Force*, started on 24 March1999 against the forces of Slo- bodan Milošević. The campaign in itself was questionable since the UN Security Council did not give permission to begin the assault, despite this, military operations began. Shortly after, Serbian hackers attacked several NATO websites.

Due to the continuous distributed denial of service (DDoS) attacks, NATO websites became repeatedly unavailable for long periods. The Serbian hacker group, called *Black Hand*, who was re- sponsible for these cyber assaults, 'defaced' several governmental websites and tried to break into the NATO command servers. The act was a failure, because they could only manage to get access to the computer networks of the air force, but could not recover any confidential information. Due to the impact of bombing the Chinese embassy in Belgrade, Chinese and russian hackers joined the cyber attacks against NATO. They also used DDoS and deface attacks on the Alliance and the websites of the uS embassy. A russian hacker group, called *From Russia With Love*, operated as the flagship of these attacks. According to statistics they hacked at least 14 military and govern- mental websites, working together with Serbian hackers during the 1999 Balkan War.[2]

Decision-makers were quick to realize the importance of cyber defence in the wake of these events. As a result the Alliance decided to launch its cyber defence program during the Prague Summit in 2002, which included the establishment of the NATO Computer Incident response Capability (NCIrC).[3] The Technical Centre, which operates as the background of NCIrC is ca- pable of detecting intrusions into the NATO networks. It is important to note that the protection of computer systems and the networks of the member states is still the task of the state.[4]

With these developments, the preparation for the key security challenge of the 21th century has begun.

1 Corvinus university of Budapest, Hungary
2 SeBőK (2007) p. 102.
3 *NATO Computer Incident Response Capability.* http://www.ncirc.nato.int/index.htm (17.12.2012.)
4 KLIMBurG (2012) p. 181.

First steps

It is indisputable that the biggest impact on the cyber defence policy of NATO was the cyber at- tacks against Estonia in 2007.[5] This cyber assault was the first example that showed what cyberwar might look like in reality, and it forced several political and military leaders to think about the im- portance of cyber security. The Russian-Georgian conflict, which took place one year after, again highlighted information operations and cyber warfare. The demand for the unification of cyber security efforts of the member states formulated at the meeting of defence ministers took place on 14 June 2007. As a result in January 2008 the Alliance accepted the Cyber Defence Policy, with the objective of synchronising this process. The leaders stood for the strengthening of cyber security processes at the Bucharest Summit on 2–4 April, 2008. Beyond the realization of new threats, the decision-makers also declared their intention to fortifying the computer systems of NATO and the future cooperation of states. In the history of NATO, it was the first example of an official frame- work for the subject of cyber security:

NATO remains committed to strengthening key Alliance information systems against cyber at- tacks. We have recently adopted a Policy on Cyber Defence, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasises the need for NATO and na- tions to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities.[6]

Corresponding to the previous steps the NATO Cooperative Cyber Defence Centre of Excel- lence (CCD COE)was established. It is indicative that the Centre was set up in Tallinn, Estonia. Beyond this organisation there are 15 further centres of excellence operating, they belong to the Allied Command Transformation (ACT), with the same task to support the experts of the given areas and to develop the capabilities of member states. Nevertheless the Centre is not a part of the command structure of NATO, it is only a part of the military structure. Therefore it is not the Alli- ance who finances it, but the sponsor nations who do.[7]

The Centre was established with the cooperation of the following countries: Estonia, Germany, Italy, Lithuania, Latvia, Slovakia, and Spain. Hungary joined the effort in 2010 and in November 2011 uSA and Poland became supporting members as well.

The responsibility of the Centre includes:

- endorsing the development of the cyber capabilities of member states;
- assisting in elaborating doctrines, concepts and strategies of member states;
- organizing education and other training sessions pertaining to information security;
- analyzing the legal dimension of cyber warfare, taking the necessary steps for drawing the international legal framework.

Therefore the organisation does not represent the offensive cyber warfare capabilities of NATO, rather it wishes to operate as a research and educational centre. One of the priorities is to con- duct the aforementioned cyber defence exercises. Such exercises were: *Baltic Cyber Shield 2010*, *Locked Shields 2012* and *Cyber Coalition 2012*.[8] The latter based on the attacks against Estonia in 2007. Hungary also participated in this exercise; according to the scenario the attacks targeted the banking system and air traffic control.

Besides the Centre, NATO established the Cyber Defence Management Authority (CDMA) which is subordinated to the Cyber Defence Management Board (CDMB).[9] The organisation is headquartered in Brussels and it is tasked with directing the centralized Alliance-wide cyber de- fence; responding to attacks against NATO and its member states and supporting national cyber defence on a member state level. Furthermore, subordinated to the NATO Computer Incident re- sponse Capability Technical Centre (NCIrC TC), a so-called rapid reaction Team (rrT) was formed, which provides assistance against cyber attacks on a national level, by deploying in the particular country. The decision making body of the organisation is the CDMB, only this board can authorize these deployments. The core of rrT is constituted of a group of experts whom can be supported by further NATO professionals if the given case requires it. By the end of 2012, the rrT capability became operational.

Besides the CDMA, the Computer Emergency response Team (CErT) was established on a national level. Following the Bucharest Summit, defence ministers agreed that every member state should establish its own CErT, thereby reinforcing and increasing the effectiveness of NATO cyber defence.

Responses to changing challenges

The next step took place on 19–20 November, 2010, when member states adopted NATO's new Strategic Concept in the course of the Lisbon Summit. Besides dealing with the topics of NA- TO-russian relations, the operations in Afghanistan, and the missile defence system, attacks com- ing from cyberspace were discussed as well. As NATO continuously keeps pace with new types of challenges, the issue of cyber security was included in the new Strategic Concept:

Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transporta- tion and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence ser- vices, organised criminals, terrorist and/or extremist groups can each be the source of such attacks.[10]

According to this, member states must be prepared for attacks which could be linked to both state and non-state actors. In line with these steps the so-called Global Commons project was launched, supervised by the Allied Command Transformation. The project is concerned with geographical and virtual dimensions which cannot be associated with any specific country; however, they play a cru- cial role in NATO's security. Such dimensions include airspace, outer space, oceans and seas, and cyberspace itself.[11] Out of these domains cyberspace is the most complex, given that it is basically composed of virtual elements, however, the possession of tangible, physical assets is required to implement information operations. This is the complexity which gives vulnerability to cyberspace.[12]

5 HuNKEr (2010) p. 9., HAIG (2009) p. 335.

6 *Bucharest Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008.* Item 47.

7 CSÁNyI, Benedek: *A NATO Kibervédelmi Kiválósági Központja.* http://www.biztonsagpolitika.hu/?id=16&aid=1148&title=A_NATO_Kiberv%C3%A9delmi_Kiv%C3%A1l%C3%B3s%C3%A1gi_K%C3%B6zpontja (10.01.2013.)

8 Not all these exercises were necessarily conduct by the Centre.
9 *Nato sets up Cyber Defence Management Authority in Brussels.* http://www.computerweekly.com/news/2240085580/Nato-sets-up-Cyber-Defence-Management-Authority-in-Brussels (11.01.2013.)
10 *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon, 2010.* Item 12.
11 *Assured Access to the Global Commons.* http://www.act.nato.int/globalcommons (28.01.2013.)
12 BABOS (2011) p. 42.

The defence ministers of the member states amended the Cyber Defence Policy in line with the new Strategic Concept during their meeting on the 8–9 June, 2011 in Brussels. Besides the new Policy they also adopted the Action Plan, which essentially put theory into practice. While the newly adopted Policy itself is not public, certain points were disclosed in the press:

- the leaders of the member states recognized that cyber defence is indispensable for collective defence and crisis management;
- prevention, resilience and the protection of IT equipment is of utmost importance for NATO and the member states;
- the goal is to develop cyber capabilities and to protect NATO's own network through central- ized security;
- to help the member states to reach a minimal level of cyber defence, reducing the vulnerability of national critical infrastructure;
- cooperation with other partners, international organisations, the private sector and aca- demia.[13]

The organisational reform within NATO has changed the composition of cyber defence bod- ies as well. The most important decision-making and executive bodies in the current structure of NATO are the following:

- Naturally, the main policy making body remained – as in all other matters, including cyber defence – the North Atlantic Council.
- The majority of the tasks pertaining to incident management and prevention provided by NATO Communication and Information Agency (NCIA) became the main body on one hand for the technical and implementation aspects of cyber defence, and on the other hand for the technical support for any missions undertaken by the member states of NATO itself. The agen- cy, which was created early July 2012, functions as the successor to NATO Consultation, Command and Control Agency (NC3A). Its priority objective is to bring NATO bodies under centralized protection. Its functions is related to cyber defence are managed through NATO Computer Incident response Capability Technical Centre.
- The Defence Planning Committee is continuously submitting proposals to the Council, funda- mentally pertaining to defence-related issues, thus the ideas and plans developed by them have a great significance in the field of cyber defence as well.

It is also important to emphasize that cyber defence has become an integral part of the de- fence planning process of NATO.[14] In March 2012 the decision-makers voted for a €58 million to upgrade the network security of NATO, and to modernise its existing infrastructure; all executed involving the private sector, coordinated by the NATO Communication and Information Agency (back then known as NATO Consultation, Command and Control Agency).[15] The investment project was also intended to allow the aforementioned Computer Incident response Capability to reach full operational capability by the end of 2012. Furthermore, a Cyber Threat Awareness Cell was set up, which is tasked with pooling intelligence and to facilitate the counteractions to such attacks.[16]

13 *Defending the networks. The NATO Policy on Cyber Defence.* www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (28.01.2013.)
14 *The Secretary General's Annual Report 2011.* http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120125_Annual_report_2011_en.pdf. p. 10. (28.01.2013.)
15 *NATO signs contract for Cyber Defence.* http://www.nato.int/cps/en/SID-CA2E493B-54BE65CB/natolive/news_85034.htm (28.01.2013.)
16 KOVÁCS (2012) p. 308.

The Alliance held its 25th summit in Chicago, on 20–21 May, 2012. The main themes of the summit included the review of defence and deterrent capabilities, how the Smart Defence concept could be improved, the question of withdrawal from Afghanistan, and the evaluation of the military operation in Libya. Naturally, the issue of cyber defence was also raised, and after the summit the stance on this question was published:

Cyber attacks continue to increase significantly in number and evolve in sophistication and complexity. We reaffirm the cyberdefence commitments made at the Lisbon Summit. Following Lisbon, last year we adopted a Cyber Defence Concept, Policy, and Action Plan, which are now being implemented. Building on NATO's existing capabilities, the critical elements of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC), including protection of most sites and users, will be in place by the end of 2012. We have com- mitted to provide the resources and complete the necessary reforms to bring all NATO bodies under centralised cyber protection, to ensure that enhanced cyber defence capabilities protect our collective investment in NATO. We will further integrate cyber defence measures into Alli- ance structures and procedures and, as individual nations, we remain committed to identifying and delivering national cyber defence capabilities that strengthen Alliance collaboration and interoperability, including

through NATO defence planning processes. We will develop further our ability to prevent, detect, defend against, and recover from cyber attacks. To address the cyber security threats and to improve our common security, we are committed to engage with relevant partner nations on a case-by-case basis and with international organisations, inter alia the EU, as agreed, the Council of Europe, the UN and the OSCE, in order to increase concrete cooperation. We will also take full advantage of the expertise offered by the Cooperative Cyber Defence Centre of Excellence in Estonia."[17]

In addition to the resolution at the summit, a document relating to defence capabilities was released, in which cyber capability were displayed as a vital military capability.[18]

Cyber attacks and Article 5

It is undeniable that the relationship between international law, law of armed conflicts, Article 5 and attack coming from cyberspace are vague at best. The evaluation and construction of the legal framework of cyber crimes and cyber attacks are pending issues. According to the new Policy, an occurring cyber attack constitutes a political attack, and therefore it does not fall under the provi- sion of Article 5; under this policy the response has to be political in nature as well. After such an attack, decisions lie with the leader of NATO and the member states, not with the commanders of the reaction forces. In other words, NATO retains a degree of resilience in how to manage a crisis which includes a cyber component.[19]

A major result is the *Tallinn Manual*,[20] written by the Cooperative Cyber Defence Centre of Ex- cellence, which is the first attempt to agree on the international legal framework of cyber warfare. The manual itself is the result of three year long research; it does not qualify as an official NATO doctrine, but rather wishes to be an advisory, guiding text. The document tries to cover all fields

17 *Chicago Summit Declaration.Issued by the Heads of State and Governments participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012.* Item 49.

18 *Summit Declaration on Defence Capabilities: Toward NATO Forces 2020.* http://www.nato.int/cps/en/natolive/official_texts_87594.htm (26.01.2013.)

19 JOuBErT (2012) p. 5.

20 T*he Tallinn Manual.* http://www.ccdcoe.org/249.html (28.01.2013.)

of international law, with an emphasis on the relationship between the right to wage war (*jus ad bellum*), the applied law in war (*jus in bello*) and cyber warfare.

experts confirm and experience also shows that there is no need to create an automatic mecha- nism to resolve such issues; each one should be examined on a case-by-case basis, and the nations concerned would decide whether they classify the particular cyber-attack as an armed attack.[21]

Recommendations

Taking into account the information aforesaid, I formulated the following conclusions and recom- mendations in relation to NATO's cyber warfare aspirations:

- ***Up-to-date knowledge, up-to-date systems.*** It continues to be crucial that the necessary fi- nancial resources be in place for the maintenance and development of the IT infrastructure. Only the most recent technology and the latest systems can be competitive nowadays. Besides maintaining the various systems, it is also important that professionals themselves should have up-to-date knowledge as well; therefore forums where experts can share their latest experienc- es are of critical importance. For this reason, the flow of information should continue to be a priority.
- ***Offensive capabilities and deterrence.*** The new Policy puts the emphasis on defensive. However, it should be worthwhile and timely to map the feasibility of any counter strikes, and to establish a significant offensive capability. The US strategies already treat cyberspace as an existing dimension of war, and for that reason they consider the training of relevant forces important; in other words, the demand for a strike force emerged.[22] Officially NATO does not have offensive cyber capabilities – this is exactly why it came as a surprise that several military leaders supported a pre-emptive strike through cyberspace during the Libyan intervention.[23] Although it is likely that this plan (which was later rejected) would have been implemented by uS forces, it would have also been a great oppor- tunity for NATO to test itself in this field. Relevant forces need to be trained to successfully carry out operations in cyberspace even during an enemy attack.[24] Moreover, there are some researchers who believe that the development of such high level offensive capabilities could serve as a similar deterrent as did nuclear weapons in the Cold War and even today.[25]
- ***Cooperation***
  - *More widespread cooperation.* It cannot be stressed enough that cooperation with non-state actors is crucial. As it is displayed in the new Policy, NATO should pay serious attention to agents and representatives of different research groups, universities and academies, given

21 HäuSSLEr (2010) p. 103.

22 *International Strategy for Cyberspace.Prosperity, Security, and Openness in a Networked World.*http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf pp. 20-21. (28.01.2013.)

*Department of Defence Strategy for Operating in Cyberspace.*http://www.defence.gov/news/d20110714cyber.pdf pp. 5-6. (28.01.2013.)

23 SCHMITT, Eric – SHANKEr, Thom: *U.S. Debated Cyber warfare in Attack Plan on Libya.* http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1 (20.01.2013.)

24 HEALEy, Jason – BOCHOVEN, Leendert van: *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.* http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf p. 7. (25.01.2013.)
Such demand appeared in the Hungarian Defense Forces as well, see HAIG (2011) p. 26-27.

25 For the relation between deterrence and cyberwar see LIBICKI (2009) p. 39-74.

that these sectors could help the cause both on the level of individual member states and of the alliance.

- *European Union.* The European union could be an important partner in the future as well, considering the significant overlap in the membership of the two organisations. In- frastructures are intertwined; hence the protection of those should be a common inter- est of both organisations. In this collaboration the primary partner could be the Europe- an Defence Agency. The agency (which launched a separate cyber defence program in 2011)[26] primarily serves as a research workshop, however, it can also act as a partner with other international organisations. Anders Fogh rasmussen, NATO Secretary-Gen- eral also called for the launch of a joint project between the Alliance and the Agency.[27]
  Furthermore, the European Network and Information Security Agency (ENISA) could play a crucial role in the cooperation as well. The agency, in addition to monitoring the common networks of the Eu and informing the Commission of any possible threats, is closely connected to the member states as well. The main points of the cooperation mostly include organising joint exercises, sharing relevant experience and holding various confer- ences. This is confirmed by Gábor Iklódy, NATO Assistant Secretary General for emerg- ing Security Challenges, while speaking at a cyber-security conference in May, organized by Microsoft.[28] He added that in case of a major attack joint actions would increase the efficiency of the defence; furthermore he did not rule out the joint protection of relevant systems in the future.

- ***Cyber defence exercises.*** The further implementation of the aforementioned exercises also plays a key role in the development of the cyber defence of the Alliance. These exercises con- tribute to revealing the vulnerabilities in the system, and provide a clear picture on how the participating states are prepared to repeal a possible attack. This means that not only can the collective systems be made more resistant, but also national capabilities could be developed with the focus remaining on prevention.
- ***Thinking on a strategic level.*** The question of cyber defence policy should not be marginal; it should not be a problem to be dealt with on a lower level. It should be stated that cyber security is a pure national security issue, which we have to think about on a strategic level. It is the obligation of all responsible nations and international organisations to establish the necessary legal and organisational framework and to ensure financial resources, because these attacks could cause extreme damage both to the infrastructure of a nation and indirectly to the economy as well.

Conclusion

This paper examined the development of NATO's cyber defence policy and presented the most important organizations and control bodies.

26 *European Defence Agency Annual Report 2011.* http://www.eda.europa.eu/docs/eda-publications/120404_rpannuel2011_def-web (10.01.2013.)

27 HALE, Julian: *NATO Sec Gen Calls for More EDA-NATO Cooperation.* http://www.defencenews.com/article/20110930/DEFSECT04/109300304/NATO-Sec-Gen-Calls-More-EDA-NATO-Cooperation (10.01.2013.)

28 HALE, Julian: *NATO Official Highlights Areas for EU-NATO Cyber Cooperation.* http://www.defencenews.com/article/20120531/DeFReG01/305310005/NATO-Official-Highlights-Areas-eU- NATO-Cyber-Cooperation (28.01.2013.)

To conclude, it can be said that the current direction is beneficial, as it is not only concerned with establishing NATO's central cyber defence – more specifically the protection of its IT sys- tems, networks and infrastructures – but also with the effort on the part of the member states to develop capabilities to ensure their own cyber security.

It is pivotal for the member states to understand the essence of the issue, as the true strength of the Alliance does not lie in itself, but in its constituent nations. That is why it is absolutely neces- sary for the member states to develop and bring their cyber capabilities to the same level.

In the recent years – especially since 2007 – NATO has begun to catch up in the field of cyber defence. Considering the operational capacities of various units and organizations it can be said that NATO in its present form in 2013 is an alliance that can adequately address the threats form cyberspace.

References

Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon, 2010. Item 12.
Assured Access to the Global Commons. http://www.act.nato.int/globalcommons (28.01.2013.) BABOS, Tibor (2011): „Globális közösterek" a NATO-ban. In: *Nemzet és Biztonság.* 2011/3.
Bucharest Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. Item 47.
Chicago Summit Declaration.Issued by the Heads of State and Governments participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012. Item 49. CSÁNyI, Benedek: *A NATO Kibervédelmi Kiválósági Központja.* http://www.biztonsagpolitika.hu/?id=16&aid=1148&title=A_NATO_Kiberv%C3%A9delmi_Kiv%C3%A1l%C3%B3s%C3%A1gi_K%C3%B6zpontja (10.01.2013.)
Defending the networks. The NATO Policy on Cyber Defence. www.nato.int/nato_static/assets/pdf/pd- f_2011_09/20111004_110914-policy-cyberdefence.pdf (28.01.2013.)
*Department of Defence Strategy for Operating in Cyberspace.*http://www.defence.gov/news/d20110714cyber.pdf p. 5-6. (28.01.2013.)
European Defence Agency Annual Report 2011. http://www.eda.europa.eu/docs/eda-publications/120404_rpannuel2011_def-web (10.01.2013.)
HAIG, Zsolt (2011): Az információs hadviselés kialakulása, katonai értelmezése. In: *Hadtudomány.* Vol. XXI. 2011/1-2. p. 26-27.
HAIG, Zsolt (2009): Connections between cyber warfare and information operations. In: *Academic and Applied Research in Military Science*. Vol. VIII. 2009/2.
HALE, Julian: *NATO Sec Gen Calls for More EDA-NATO Cooperation.* http://www.defencenews.com/article/20110930/DEFSECT04/109300304/NATO-Sec-Gen-Calls-More-EDA-NATO-Cooperation (10.01.2013.)
HALE, Julian: *NATO Official Highlights Areas for EU-NATO Cyber Cooperation.* http://www.defencenews.com/article/20120531/DeFReG01/305310005/NATO-Official-Highlights-Areas-eU-NA- TO-Cyber-Cooperation (28.01.2013.)
HäuSSLEr, ulf (2010): Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty. In TIKK, Eneken – TALIHärM, Anna-Maria (eds.): *International Cyber Security Legal & Policy Proceedings.* CCD COE Publications, Tallinn. p. 103.
HEALEy, Jason – BOCHOVEN, Leendert van: *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.* http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf pp. 7. (25.01.2013.)
HuNKEr, Jeffrey (2010): Cyber war and cyber power. Issues for NATO doctrine. In: *NATO Defense College Research Paper.* 2010/62.
*International Strategy for Cyberspace.Prosperity, Security, and Openness in a Networked World.*http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf p. 20-21. (28.01.2013.)
JOuBErT, Vincent (2012): Five years after Estonia's cyber attacks: lessons learned for NATO? In: *NATO Defense College Research Paper.* 2012/76. p. 5.
KLIMBurG, Alexander (ed.) (2012): *National Cyber Security Framework Manual.* NATO CCD COE Publication, Tallinn.
KOVÁCS, László (2012): Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I. In: *Hadmérnök.* Vol. VII. 2012/2. p. 308.
LIBICKI, Martin C. (2009): *Cyber deterrence and Cyberwar.* rAND Corporation. p. 39-74.
NATO sets up Cyber Defence Management Authority in Brussels. http://www.computerweekly.com/news/2240085580/Nato-sets-up-Cyber-Defence-Management-Authority-in-Brussels (11.01.2013.)
NATO signs contract for Cyber Defence. http://www.nato.int/cps/en/SID-CA2E493B-54BE65CB/natolive/news_85034.htm (28.01.2013.)
SeBőK János (2007): *A harmadik világháború. Mítosz vagy realitás?* Népszabadság Zrt., Budapest. *NATO Computer Incident Response Capability.* http://www.ncirc.nato.int/index.htm (17.12.2012.) SCHMITT,
Eric – SHANKEr, Thom: *U.S. Debated Cyber warfare in Attack Plan on Libya.* http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1 (20.01.2013.)
Summit Declaration on Defence Capabilities: Toward NATO Forces 2020. http://www.nato.int/cps/en/natolive/official_texts_87594.htm (26.01.2013.)
The Secretary General's Annual Report 2011. http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120125_Annual_report_2011_en.pdf. p. 10. (28.01.2013.)
The Tallinn Manual. http://www.ccdcoe.org/249.html (28.01.2013.)