Adriana Dvoršak

DOI:10.33179/BSV.99.SVI.11.CMC.16.3.6

NORMATIVNA VLOGA ZAVEZNIŠTVA PRI NEKONVENCIONALNIH VARNOSTNIH GROŽNJAH – KIBERNETIČNA OBRAMBA ČLANIC

THE NORMATIVE ROLE OF THE ALLIANCE IN NON-CONVENTIONAL SECURITY THREATS – CYBER DEFENCE OF MEMBER STATES

Povzetek Vloga mednarodnih varnostnih organizacij je oblikovanje konsenza o vrednotah, normah in pravilih, ki se nanašajo na kibernetsko bojevanje. Nato proizvaja kibernetske politike, skrbi za izobraževanje in izmenjavo informacij, tudi s publicistično dejavnostjo, nekoliko manj pa je razvil operativne zmogljivosti za skupno kibernetsko obrambo in kibernetsko bojevanje.

V Natu lahko pričakujemo pobude za tesno sodelovanje pri kibernetski obrambi in gradnji skupnih kibernetskih zmogljivosti, kar je racionalen odgovor na nekonvencionalne grožnje. Pridobitve članic, ki bodo izšle iz sodelovanja na področju kibernetskega bojevanja, se bodo med seboj razlikovale. Največ pridobitev avtorica pripisuje ZDA, ker je njihova ekonomija najbolj odvisna od informacijsko-komunikacijskih tehnologij, najbolj globalizirana in domnevno najpogostejša tarča kibernetskih napadov.

Ključne besede ***Kibernetska obramba, mednarodne varnostne organizacije, mednarodno pravo.***

Abstract The role of international security organizations is to create a consensus on values, norms and rules relating to cyber warfare. NATO produces cyber policy and provides for education and the exchange of information also through publicistic activity. To a lesser extent it has also developed operational capabilities for joint cyber defence and cyber warfare.

NATO can expect initiatives for close cooperation in cyber defence and the establishment of common cyber capabilities, which are all rational responses to unconventional threats. The benefits stemming from such cooperation differ by state. The author is nonetheless convinced that the United States will benefit the most from the said cooperation as their economy is the most dependent on information and communication technology, the most globalised and allegedly the most frequent target of cyber attacks.

Key words *Cyber defence, international security organizations, international law.*

Introduction

Amid a growing number of cyber attacks, reflections on cyber conflicts and, consequently, the most effective national organization for their prevention and management are becoming more frequent. Although Slovenia is responding to the phenomenon of cyber conflicts, its responses are not proactive. On the other hand, its active adjustment to external influences can be easily perceived. The paper focuses on the role of international security organizations in the management of the member states' behaviour in cyber conflicts on the one hand, and on national security needs on the other. At the abstract level, we will address the role of international organizations in the formation of consensus on values, norms and rules referring to cyber warfare, or the normativisation and the structure-unit relationship. At the practical level, we will address the relationship between NATO and Slovenia.

In international organizations, consensus is built around an institution's legitimacy for cooperation in the field of unconventional threats and a member state's participation in policy programming. The attainment of consensus is part of the output of international security organizations that may be dissected into policy programming, information activity and operations (Rittberger & Zangl, 2006). International security organizations' information activities are also the categorization of actions that will be perceived by member states as activities leading to cyber conflicts, the dissemination of information and the analysis of examples and good practices.

Until now, the international community has not been able to produce a unique interpretation of the current rules and principles of international law regarding cyber conflicts and cyber warfare. However, the areas of international law that are especially important for the development of international norms in cyberspace may nonetheless be identified: *jus ad bellum, jus in bello* and the neutrality of a state. The nature of cyberspace as such hinders the implementation of the principles of necessity, proportionality, distinction and neutrality in cyber warfare. In the international community, however, the legal discourse is not a quest for an objective truth waiting to be discovered (Johnstone, 2003), but rather a discourse on committed acts and practices that originate from common understanding and beliefs forming the background of cyber conflicts and cyber warfare. We must distinguish between the legislative and normative role at the national level and normativisation, i.e. the full process, from the introduction of the principled of international law to the creation of international rules and treaties, at the international level. The discussions on the role of national legislation and national development are not the subject of this paper.

Nonetheless, we will try to define the strategic, directional, developmental and doctrinal role of the armed forces, this definition pertaining more to the military science than the international political sciences. At the national level, the strategic role of the armed forces consists of the development of the national strategy for cyber security and defence. It refers to the modernization of the legislation on information society and defence with a view to providing support to national measures, and reflects the level of national dependence on information and communication technology. The military sub-system's developmental role is oriented towards ensuring the Slovenian Armed Forces with a position and a role in the provision of effective response to cyber threats, and towards the organizational placement and coordination of all capabilities for incident management and cyber security provision. The directional role is defined by the formation of objectives, different forms of civil-military cooperation and the identification and definition of goals in cyber incidents management. The doctrinal role includes the development of optimum techniques, tactics and procedures (TTP) for the provision of national security.

The paper is based on a constructivist theory of international relations (Onuf, Kratochwil) and post-structuralism (Der Derian) in which the use of statistical data is more of an exception than a rule. Slovenian contribution to science that should be mentioned in this context is the Svete's concept of information and communication technologies in the form of social and technical networks, which is also based on constructivism (Svete, 2005). The paper uses the descriptive and the comparative method, focusing on the following research questions:

(1) Are large states leading in the normativisation of unconventional security threats in international organizations?

(2) Are the changed challenges in the environment facing the international security organization with new security needs of their members?

1 ORIGIN OF CYBER WARFARE RULES

The member states' benefits deriving from their participation in international security organizations differ. Cyber conflict management turns out to be most profitable for the USA, as their economy is the most dependent on ICT, the most globalised and allegedly the most frequent target of cyber attacks. Hence, the USA are most interested in the promotion and most eager to promote such conversion of national needs in the international arena, as they will benefit the most from it. For the USA, intergovernmental negotiations are one of the most beneficial standard ways of conversion of the member states' needs into the result of the international community's work increasing national and international security; in NATO, the USA have resources for effective mobilization at their disposal. To complete the picture, let us list other manners of conversion of such needs: polling, use of standardized procedures and regulations, management policy and rational choice (Rittberger & Zangl, 2006).

Small countries with a low level of involvement in the international economic flow, whose economies are not strongly based on ICT, and countries that are less at risk due to their peaceful external policies, are less interested in the participation in the field of cyber defence. Their motivation to participate is additionally reduced by the security dilemma which has an overall negative influence on cooperation. In a cyber security dilemma, certain dimensions are accentuated, since the relativization of the level of threat is even greater than for conventional threats, the secrecy and the lack of transparency in the use of cyber weapons are large and they even provide the national security system with a decisive advantage (Axelrod & Iliev, 2014). However, unlike with conventional threats, here exists a possibility of restoration of the information structure. The cyber security dilemma reduces the possibility of cooperation between the states.

NATO produces cyber politics (Nato, 2011), provides for education and the exchange of information in the excellence centre, and the publicistic activity. It is a little less involved in the development of the member states' operational capabilities for joint cyber defence and cyber warfare. In the field of operations (computer network operations – CNO), NATO, as documented, supported the USA's activities in the context of the Allied Force operation in 1999 (Lambeth, 2002) through offensive methods, but did, however, not respond to Estonian calls for assistance in 2007 (Meyer & Ummelas, 2007, May 17). In 2014, the USA expressed doubt whether Article 5 of the North Atlantic Treaty may be invoked in the event of a cyber attack. Following the Ukrainian crisis and the strained security situation of East European member states, a predominant belief emerged in the America's elite that Article 5 might lead to failure; as affirmed by the former head of the Central Intelligence Agency (CIA) John McLaughlin, a direct call for solidarity might thoroughly shake NATO's foundations (Calabressi, 2014).

Essential for the understanding of the method of warfare and the introduction of organizational changes is the understanding of cyberspace in relation to the new assignments of the armed forces. Notions from the field of cyber security help define the phenomenon, overcome conceptual problems in cyber defence and cyber warfare, study new concepts such as cyber resistance, and indicate new possibilities for the management of cyber threats (Rantapelkonen, 2014). The nature of cyber defence is oriented inwards. Nevertheless, as stated in the comparison study of the Geneva Centre for the Democratic Control of Armed Forces (DCAF), armed forces carry out the new non-conventional internal assignments without armament (Schnabel & Hristov, 2010). Even the offensive cyber weapons cannot be classified as classic armament, as they are in fact a computer programme called "weaponized code" in jargon. Numerous companies develop codes for attacking vulnerabilities in target operations systems and applications. Military and intelligence organizations buy such equipment on the open market, at which the USA lead in terms of value and the complexity of the purchase (Menn, 2013).

How are the armed forces to perform their new assignment, which is something in between computer forensics and deliberate cooperation, with top-notch mathematicians and computer experts and the purchase of appropriate offensive code on the open market? The American model that again offers itself does not correspond to the capabilities and the needs of a small state with limited resources as Slovenia. On the inside, the Slovenian Armed Forces require organizational solutions that enable intensive cooperation with other competent bodies in state administration, new partners among the telecommunication companies and companies for information security, and a system-based approach in the provision of human resources.

Table 1: Average number of affected users by sector in 2013
Source: Symantec, p. 41 (Symantec, 2014).

Sector	Average number of identities per incident
accounting	673,916
administration and human resources	150,650
agriculture	37,000
civil society and non-profit sector	34,614
computer hardware	100,000
computer software	12,761,182
education	100,267
finance sector	11,884,222
government sector	99,893
healthcare	67,519
tourism	2,034,232
information technology	4,500,230
insurance business	114,775
police	1,119
military	26,500
retail trade	8,692,318
social networks	**16,083,333**
telecom	3,029,286
transportation business	243,390
engineering	20,000

Table 2: Statistics of relevant incidents in Slovenia
Source: SI-CERT, p. 10 (SI-CERT, 2014).

TYPE OF INCIDENT	2012	2013
scanning and attempt of scanning	51	43
botnet	12	16
Distributed Denial of Service (DDoS)	47	76
harmful code	258	417
service abuse	9	8
hacking	76	61
abuse of a user's account	9	37
webpage defacement	125	80
attacks on the application	17	22
Total technical attacks:	**604**	**760**
identity theft	67	56
fraud	161	210
spam	74	50
phishing	139	209
dialer	1	0
Total frauds, deceptions:	**442**	**525**

Attacks on military networks, as recorded by Symantec in 2013, were not widespread (Internet Security Threat Report (ISTR), 2014). On the basis of the data in Table 1, most cyber attacks are qualified as criminal acts. Social networks are that sector in which most users are infected and in which the infections are spreading the most. As the reporting of an attack to the European Network and Information Security Agency (ENISA) is currently voluntary, states seldom report of attacks on the critical infrastructure. The EU is now starting to gradually strain this legislation.

According to the SI-CERT data listed in Table 2, there were altogether 1,513 incidents in Slovenia in 2013, which means a **21 percent increase from 2012 when** 1,250 incidents were dealt with. What stands out in particular is the increase of the harmful code incident, and an over 50 percent increase of phishing and the number of internet frauds and deceptions (SI-CERT, 2014).

In the international sense, our question is how the states should act to each other in a cyber environment, at which we perceive the characteristics of a bad cyber neighbourhood, the increasing distrust in internet services due to cyber crime, resistance to mass control and other transnational phenomena. Values in the background of international discussions are subjective; however, international law on cyber conflicts is not an objective reality waiting to be discovered but rather a product of customs, norms and the resulting rules. Hence, the rules of cyber warfare collected and presented in the NATO Talinn Manual will also most likely influence the establishment of international law.

The emerging rules of cyber warfare address questions on which consensus is yet to be reached among the professionals, in the institutions of the Slovenian Armed Forces and the state, the politics and international organizations. To the author's belief, the most important questions for Slovenia are those pertaining to ethics and norms as well as their resultant which is an optimum structure for the provision of national cyber security. In terms of cyber security provision, the armed forces are only in the second place; primary security refers to information security which is the responsibility of companies, individuals and the police. Non-military actors also play an important role in cyber defence (computer network defence – CND); however, offensive operations already call for activities governed by the international law, the answers to which may be found in the Talinn Manual. These are: types of warfare, allowed use of cyber weapons, prohibitions, definition of the intermediate area of intelligence activities that are subject to civilian and military intelligence agencies, and the protection of individual groups, such as reporters, humanitarian and medical workers, children and other.

International organizations classify categories of problems defining their priority order and identifying their actors (Sil & Katzenstein, 2010). With its cyber policy, NATO follows this logic of problem classification. We could even claim that NATO forms recommendations for the management of actors, i.e. members of the Alliance. The author offers two examples of recommendations that have not yet been issued despite a clearly expressed need in the environment, namely the recommendations for the limitation of purchase on the black market and the export of technologies for mass control to authoritarian states.

1.1 Armed Conflict

Let us move from the formation of rules for international cyber conflicts to a more detailed definition of procedures and rules in NATO. The manual does not define NATO's rules for offensive operations, yet it authorises the use of Article 5 of the North Atlantic Treaty only if the conditions regarding the criteria for an armed attack are met.

1.1.1 Criteria for an Armed Attack: Effect, Conduct

The answer to the question whether a cyber attack may qualify as an armed attack depends on its scope and effect – something we could verify objectively only after the attack. However, the group of participating experts agreed that an estimate of reasonably predictive consequences of such an attack suffices for making a decision on whether the measure meets the conditions for an armed attack. If we make an unambiguous conclusion; the decision whether a cyber attack is an armed attack is a matter of consequence assessment. Schmitt (Schmitt, 2014) claims that a response with force, whether kinetic or not, may be justified only when cyber operations present an armed attack. A response using force is a subject of the international humanitarian law; however, we still lack responses regarding the consequences of cyber operations.

Additional criteria for an armed attack refer to the characteristics of the conduct of a cyber attack, that is the operation of a computer programme *weaponized code*. These assessments are listed in the manual: we are referring to necessity and proportionality (rule 14), imminence and directness (rule 15). However, each individual offensive cyber activity must be analysed before it could be defined as an armed attack by a state or by NATO member states. Forensic definition of an armed attack, appropriate international legal argumentation and diplomatic action are of great importance when referring to Article 5 of the North Atlantic Treaty.

Essential for the activation of the article from the formal point of view is the invitation of the state under attack and the agreement of member states on whether the attack meets NATO criteria. When justifying its decision, the state under attack may resource to the following questions (Schmitt, 2013):

- What is the damage caused and the number of victims due to the attack?
- How quickly did the malicious code cause an effect?
- Did cyber attack cause an effect directly or was the effect increased due to any other reasons?
- How invasive was the activity? Was it oriented towards a specific protected network?
- How measurable is the effect? Is the calculation of the effect reliable?[1]
- Did the activity have a military character?

[1] *Poor defence adds to the effect.*

– Could the act qualify as use of force under the international law?
– Is the state involved directly or indirectly?

For such interdisciplinary reasoning, participation of experts from different fields is essential. The definition of the level of invasiveness, in particular, requires the cooperation of information security experts who by default assess and analyse each attack according to the selected standards.[2] The experts that often come from the private sector enjoy international reputation and provide their advice to a number of different governments that require their assistance.

To this end we will try to systemise the needs of small and large states in the provision of national cyber security, with the researchers of the relationship between states and networks already being aware of the fact that security and securitization have become leading elements in internet management (Mueller, 2010). The taxonomy of cyberspace management will be used for sorting key activities of state actors in the provision of national security. The units are divided into two groups; the groups of small and large states at which the group of large states includes NATO members such as France, Canada, Germany, Great Britain and the USA, while all other members belong to the group of small states.

Table 3: The taxonomy of cyberspace management for purposes of national security

	Strategic objective	Jurisdiction	Management control
Large states	predominant in the cyberspace	Strive towards extraterritoriality of the national legislation, unilateral globalism	high, formal, hierarchical
Small states	choice between proactive adaptation and accommodation and the emerging regime	erodes	based on trust, reciprocity, resources sharing
Regardless of the size	digital human rights (privacy, mass control, data protection), programming of joint resources for network management (TRIPS, IP, DPI, international institutions such as WIPO, ICANN, WTO, IGF), adjustment of the content, response to security globalisation (uninterrupted cooperation of the international community, shared values, norms and principles, stability and immunity of networks)		

[2] *Characteristic information for an attack model and the selection of forensic experts are: the classification of an attack, description of the code functioning, target vulnerability, method of attack, the attacker's objective, sources, skills and knowledge for the implementation of attack, solutions for stopping the malicious code, description of circumstances and references.*

Based on the taxonomy of cyberspace management for purposes of national security presented in Table 3, it can be concluded that cyberspace has confronted the states with new security requirements that they were not familiar with at the time before the national economies became vitally dependant on cyberspace. Table 3 depicts key activities of states in cyber management from the aspect of network security provision. It should be mentioned that only state actors, and not non-governmental organizations, are included in the table, and as far as priority management tasks are concerned, national security is essential, while any solutions of technical and operator problems are neglected.

Network security is a security requirement that states try to meet in the international arena. It is such a great challenge that NATO officially recognised it as a new security requirement of member states in the context of the policy Defending the Networks (NATO, 2011). The new security requirement of states is stability and the immunity of networks. It was named by NATO as the standardization of processes leading to the increase in the immunity of national networks and the critical infrastructure, which is the purpose of cyber defence. The purpose of all defence politics, activities and measures is to increase immunity. The latter is considered a capability to predict natural disasters or man-made disasters, to avoid them, minimize them and recover from them (O'Neil, 2009).

The need for state security is thus realized through the conversion of a state's requirements by interfering with the management of networks and the world web, the regulation of content, the allocation of domains and the monitoring of other management means. As claimed by Mueller, there exists a possibility of occurrence of a regulatory coalition between the content regulators, the defenders of intellectual property and the defenders of security for hierarchic control over the internet based on the national principle (Mueller, 2010).

1.2 Use of Force

A cyber attack is considered use of force, regardless of the type of weapons used, which in our case is a computer programme, also called the "weaponized code". The use of force is prohibited in the international environment; however, in accordance with the decision of the Permanent Court of International Justice, in general all activities not expressly forbidden by international law are allowed (The Case of the S.S. Lotus, France v. Turkey). It is therefore important to know which Slovenian cyber activities could be considered as the use of force before the Permanent Court of International Justice, as they would also be perceived as such by the UN and NATO. A response that is in accordance with Article 51 of the UN Charter is allowed for a cyber attack that is considered as the use of force. The use of force, however, is not yet equal to an armed attack in the event of which a signatory of the North Atlantic Treaty could ask for collective defence based on Article 5.

However, no state, even if its national scientific circles, professionals and the politics fail to reach a consensus on whether cyber operations (CNO) are to be considered as the use of force, can plead ignorance before an international court. States are obliged to comply with the international law under which false consciousness cannot be considered protective consciousness. The use of force is hence perceived as a key concept for the establishment of cyber defence at the national level.[3]

The behaviour of a state in the cyber environment is founded on its strategic culture; however, certain activities, such as spying (computer network exploitation – CNE), are expected and silently approved of in international relations. Such activities also exist in the part of the international law referring to cyber warfare. However, a preventive attack on a potential attacker who has cyber capabilities at his disposal but who has no intent to commit an armed attack is in contradiction with the international law.[4]

The technical characteristics of the course of an attack, e.g. for the zero-day vulnerability, render the incorporation of cyber attacks into the time and cause-effect dimension difficult. There is a very thin line between the use of force and an armed conflict that is especially difficult to define in a cyber environment. Any incorrect or biased interpretations may cause a decline of confidence in international law and in the abilities of international security organizations to manage the behaviour of states at a normative level.

Cyber warfare allows for actions that might not even be possible in a kinetic environment, but can be expected in a cyber conflict. Following is a list of a number of interesting and inspiring legitimate ruses:

- Transmission of false information and intelligence;
- Transmission of false orders or an intent to issue an order;
- Establishment of virtual networks, simulated by non-existing forces;
- Use of faulty identifiers and computer networks (e.g. Honeypots also used by the police in peacetime);
- Use of virtual cyber attacks under the condition that panic does not spread among the civilian population;
- Use of enemy markings, signals and paroles, but not the markings of humanitarian or medical organizations.

In cyber environment, psychological operations units obtained a new important dimension for the development of the skill of deception. It is wise to ask oneself how much a small state can influence the perception of the state's soft (cyber) power through deception using the new policy to its benefit. Digital diplomacy is a good start, while the system answer is once again the development of appropriate constructivist theories and models. Recent attempts can be found in the models

[3] *More on the permissibility of offensive activity (computer network attack CNA) in the context of cyber defence (CND) in Slovenia can be found in the discussion on the development of offensive cyber capabilities in the author's published papers (Dvoršak, 2014).*

[4] *Compare the justification of the attack on Iraq in 2003 and the response of the old Europe stating that the sole existence of the weapons of mass destruction is not merely a causus belli.*

of social and technical networks (Svete, 2005) and the military-industrial-media-entertainment-net (MIME-net) (Der Derian, 2001). The likely responses of a state to cyber operations are limited by international law. It is therefore clear that spying does not classify as an armed conflict or an armed attack under Article 51 of the UN Charter, hence no response based on the law of armed conflict is justifiable. Mutual spying is acceptable. It is a little less clear what the case with the purchase of equipment and programmes is and the information and communication technology that does not correspond to integrity requirements. In short, is responsibility attached only to the purchaser or do the states that have asked the manufacturers to install the malicious code on the new equipment also bear part of that responsibility? A similar ethical question appeared when companies of the West European states exported mass control technology to non-democratic regimes.

The most tangible result of NATO cyber politics is the preservation or reproduction of security at the national and regional level. In its representative and perceptive dimension, security is not a measurable value for constructivists, but merely a feeling of security inherent to the entities of security, i.e. citizens of NATO member states, national elites and the international elite. We have perceived conflicts between the interests of the economic and technical elite in the export of technology for mass control and the interests of citizens due to non-democratic potential of these technologies, used by the political elites for control of the citizens in both authoritarian and non-authoritarian states.

1.3 Sabotage

Let us look at an example of sabotage that is seldom addressed in the literature on armed conflicts. The situation is even more fluid with the sabotage of critical infrastructure and dual-use technology in the time of peace. For purposes of defining sabotage in military networks, Article 5 of the IV Geneva Convention should be taken as a basis. The convention states that an individual shall lose protection provided by the conventions if he carries out activities hostile to the security of a state (Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, 1949).

An activity hostile to the security of a state offers two presumptions. First, that a certain fact has already taken place or that a certain event has already occurred, which has already been established. Second, that the adjective hostile does not indicate an intention or the finality of this event that is hostile or in other words malicious.

It is difficult to offer a unified definition of committed acts with hostile intent. It is most likely that the IV Geneva Convention included all intelligence activities and sabotage inherent to the hostile state in this definition. Indirectly, Article 5 defines sabotage as an act the intent or objective of which is to damage material property of the opponent's armed forces or the property used by the armed forces. In contemporary cyber defence language, sabotage affects the integrity and accessibility of networks, while the CNE, on the other hand, affects the confidentiality of networks and data.

In accordance with the interpretation in the Talinn Manual, a state under attack has the right to damage assessment even prior to the actual occurrence of such damage. According to NATO's manual that, in wartime, equates the dual-purpose technology with the technology used exclusively by the armed forces, counter-intelligence activities are intended also for the detection of sabotage and dual-use technology, which represents a large part of ICT and technology that serves as a basis for critical infrastructure and certain companies in state ownership. Due to the above-mentioned, the author believes that the discussion regarding sabotage is particularly interesting for the importing states, Slovenia included, and less interesting for exporters of top-notch technologies.

The militarisation of the cyber environment through sabotage, the testimonials of which are presented in Snowden's public disclosures, increased America's military domination in cyberspace, which can be understood as its legitimate objective. On the other hand, sabotage reduced the security of national networks, which is most often discussed and written by information security experts. All this is also in direct contradiction with the national security interests of states that are distinct net importers of ICT. The arrangement for the provision of the dual-use technology and ICT falls behind the capabilities of the exporting states, in terms of legislation and institutions, to use such technology for their own purposes, either peaceful or hostile. In the future, the tasks and responsibilities of national institutions most responsible for cyber security will increase. In addition, the type of inter-institutional cooperation and the organization of structures providing cyber security in an operational manner will also change, while fresh winds in the theoretical field have been called for for quite some time. The manners in which both large and small states respond to the globalization of security already differ from one another; however, non-state actors, private companies and non-governmental organizations will most likely intervene in the solution of these interests even further.

Conclusion

The intent of this paper is to highlight certain discrepancies between the Talinn Manual and the security requirements of small states. The basic contradiction in the provision of collective security is the conversion of the needs of member states into a relative feeling of security of two entities, e.g. the national economic elites and the citizens. The second contradiction is the structure of such a security organization that would support only America's leading role in the provision of global security and not attempt to meet security requirements of other member states.

NATO can expect to see activities for the increase of cyber capabilities of member states and the search for effective response to non-conventional threats. However, it would be unreasonable to expect that all offers will be equally beneficial to all member states. In the future, members of the Alliance will be faced with the challenge to determine which requirements from the environment are met by the Alliance, if any at all, and which objectives should be met through the Alliance's activities. Events in the environment are a severe test of whether the activities in NATO are oriented enough towards the security of the citizens of the European member states.

The most important finding for Slovenia at the abstract level is how consensus-based decision making influences the interests of smaller members and how important a state's position in the organization is (agency vs. structure). These are the questions that are essential for the future of the Alliance.

Bibliography

1. *Axelrod, R., & Iliev, R., 2014. The Timing of Cyber Conflict. Ann Harbor: Ford School of Public Policy, University of Michigan.*
2. *Calabressi, M., 2014.. Inside Putin's East European Spy Campaign. Time. http://time.com/90752/inside-putins-east-european-spy-campaign (30 September 2014).*
3. *Der Derian, J., 2001. Virtuous war: mapping the military-industrial-media-entertainment network. Boulder, Colo.: Westview Press.*
4. *Dvoršak, A., 2014. Developing Framework for Offensive Computer Network Operations in Slovenia. In Čaleta, D., Vršec, M., Ivanc, B., ed. Open Dilemmas in the Modern Information Society, pp. 177 – 186. Ljubljana.*
5. *International Committee of the Red Cross (ICRC). Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention). 12 August 1949, 75 UNTS 287. http://www.refworld.org/docid/3ae6b36d2.html (30 September 2014).*
6. *Internet Security Threat Report (ISTR). (2014) (Vol. 19): Symantec Corporation.*
7. *Johnstone, I., 2003. Security Council Deliberations: The Power of the Better Argument. European Journal of International Law, Vol. 14, No. 3., pp. 437 – 480.*
8. *Lambeth, B. S., 2002. Kosovo and the Continuing SEAD Challenge. AEROSPACE POWER JOURNAL, 16, pp. 8 – 21.*
9. *Menn, J., 2013. Special Report: U.S. cyberwar strategy stokes fear of blowback: Reuters. http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510 (30 September 2014).*
10. *Meyer, H., & Ummelas, O., 2007. Estonia Asks NATO to Help Foil 'Cyber Attack' Linked to Russia: Bloomberg. http://www.bloomberg.com/apps/news?pid=newsarchive&sid=abGseMma5MjU (30 September 2014).*
11. *Mueller, M., 2010. Networks and States, The Global Politics of Internet Governance: MIT Massachusetts Institute of Technology.*
12. *NATO, 2011. Defending the Networks NATO Public Diplomacy Division: North Atlantic Treaty Organization. http://web.archive.org/web/20120310083820/http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (30 September 2014).*
13. *O'Neil, D., 2009. Maturity Framework for Assuring Resiliency Under Stress. The Journal of Defence Software Engineering (September/October 2009).*
14. *Rantapelkonen, J., 2014. The Fog of Cyber Defence / Ethical Hacker (J. Rantapelkonen & M. Salminen Eds.). Helsinki: Finnish National Defence University.*
15. *Rittberger, V., & Zangl, B., 2006. International organization: polity, politics and policies. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.*
16. *Schmitt, M., 2013. Talinn Manual on the International Law Applicable to Cyber Warfare. NATO, CCD COE, Talinn.*
17. *Schmitt, M., 2014. Guest Blogger, Michael Schmitt, delves into the applicability of IHL in cyber space. http://intercrossblog.icrc.org/blog/guest-blogger-michael-schmitt-delves-applicability-ihl-cyber-space (30 September 2014).*
18. *Schnabel, A., & Hristov, D., 2010. Conceptualising Non-traditional Roles and Tasks of Armed Forces. Sicherheit und Frieden / Security and Peace, Vol. 28 (No. 2), pp. 73 – 80.*
19. *SI-CERT, 2014. Poročilo o omrežni varnosti za leto 2013. Ljubljana: Slovenian Computer Emergency Response Team.*

20. *Sil, R., & Katzenstein, P. J., 2010. Beyond paradigms: analytic eclecticism in the study of world politics. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.*
21. *S. S. Lotus (Fr. v. Turk.), 1927. P.C.I.J. (ser. A) No. 10 (Sept. 7). http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm (30 September 2014).*
22. *Svete, U., 2005. Informacijsko-komunikacijska tehnologija in sodobne varnostne teorije Varnost v postmoderni družbi. Ljubljana: Fakulteta za druzbene vede.*
23. *Symantec, 2014. Internet Security Threat Report (ISTR) (Vol. 19): Symantec Corporation.*