Staša Novak
DOI:10.33179/BSV.99.SVI.11.CMC.18.2.2

NATO IN KIBERNETSKO ODVRAČANJE

NATO AND CYBER DETERRENCE

Povzetek Vpliv kibernetske tehnologije na sodobno družbo je pomemben. Države se morajo prilagoditi spremenjenemu varnostnemu okolju, da bi bile zmožne zagotoviti varnost in stabilnost svojih ozemelj ter prebivalstva. Odvračanje, ki gre po navadi z roko v roki z obrambo, pomeni preprečevanje spopadov z odvračanjem napada morebitnih agresorjev. V kibernetiki so pravila drugačna kot pri tradicionalnem odvračanju zaradi posebnih značilnosti kibernetskega okolja. Zato sta nujna nova miselnost in bolj celosten pristop k odvračanju.

Pristop Nata k odvračanju temelji na ustrezni mešanici konvencionalnih, jedrskih in raketnih zmogljivosti. Kljub temu pa po sprejemu izboljšane politike o kibernetski obrambi (Enhanced NATO Cyber Defence Policy) iz leta 2014 Nato v resnici izvaja nekatere elemente kibernetskega odvračanja, ki temeljijo na močni obrambi, deklaratorni politiki in odzivnih ukrepih. Odzivni ukrepi ne pomenijo Natovih ofenzivnih kibernetskih zmogljivosti, temveč možnost za odzivanje kolektivne obrambe na kibernetski napad, pri čemer se uporabijo vsa sredstva, ki so na voljo. V članku so predstavljeni trenutna Natova kibernetska politika in mogoči prihodnji dogodki, povezani s kibernetskim odvračanjem na ravni zavezništva.

Ključne besede ***NATO, obramba in odvračanje, kibernetsko odvračanje, kibernetska obramba, kolektivna obramba, mednarodno pravo.***

Abstract The impact of cyber technologies on the modern societies is significant. States have to adapt to the changed security environment to be able to ensure the security and stability for their territories and populations. Deterrence, which usually goes hand in hand with defence, is about preventing conflicts by dissuading potential aggressors to attack. With regard to cyber, the rules of deterrence change when compared to traditional deterrence, because of the special characteristics of the cyberspace. What is needed is new way of thinking about deterrence and a more comprehensive approach to it.

The North Atlantic Treaty Organisation's (NATO) approach to deterrence is resting upon the appropriate mix of conventional, nuclear and missile defence capabilities. However, following the 2014 Enhanced NATO Cyber Defence Policy, NATO is *de facto* already pursuing certain elements of cyber deterrence based on strong defence, declaratory policy and responsive measures. Responsive measures are not NATO offensive cyber capabilities, but the possibility of a collective defence response to a cyber attack, which implies a response with all available means. The article is providing an insight into NATO's existing cyber defence policy and possible future developments of cyber deterrence at the level of the Alliance.

Key words ***NATO, defence and deterrence, cyber deterrence, cyber defence, collective defence, international law.***

Introduction

Globalisation and rapid development of technology mark modern society. Almost everything and everyone have become highly dependent on digital information and communication systems. The world has become more interdependent and interconnected. Against this background, the cyberspace, with all its potential opportunities and threats, has become not only a matter of national security, but also a matter of concern for the North Atlantic Treaty Organisation (NATO).

The article explores the implications of the 2014 NATO Enhanced Cyber Defence Policy from the perspective of cyber deterrence. It starts with the contextual background and the analysis of the security environment, and continues with the chapter on deterrence. It provides an overview of the basic concepts of the theory of deterrence, stemming from the Cold War, their possible application to the modern cyber environment and challenges connected to it. It also gives an insight into overall NATO defence and deterrence posture, by aspiring to analyse the cyber elements of it, with a special emphasis on NATO's declaration that cyber defence is part of a collective defence and that cyber attacks can reach a threshold to invoke Article 5.

The attention of the analysis rests only on NATO and not on individual Allies.[1] Although research was limited to the analysis of the secondary literature, relevant documents and other publicly available information, due to its primary focus on NATO's declaratory policy and political and legal implications of linking cyber defence with collective defence, the article provides an insight into some of the questions that might be addressed by NATO in the future.

[1] *The author uses NATO definitions, where available and applicable, or relevant definitions from secondary sources.*

1 CONCEPTUAL FRAMEWORK

1.1 Cyberspace

According to Trujillo (2014, p. 44), cyberspace is comprised of three components: the hardware, the virtual, and the cognitive. The physical element consists of information technology infrastructure (routers, fiber optic and transatlantic cables, cell phone towers, satellites, computers, smartphones, any devices connected to the Internet or local networks). The virtual element encompasses the software and data. And finally, the cognitive component includes its users, which can be anonymous and multiplicative, state or non-state actors. While the physical elements might reside in the sovereign territories of states, the virtual spaces do not.[2]

"Equally important to what cyberspace *is* is what it *does* (Hunker, 2013, p. 173). The information in cyberspace *controls* directly a wide variety of physical and electronic activities (e.g. Supervisory Control and Data Acquisition (SCADA) networks control many industrial processes); cyberspace data also *informs* decisions that people make" (*Ibid.*) Another special feature of cyberspace is its mostly civilian nature. A lot of infrastructure, data, and networks are owned by private entities, which can significantly affect the idea of cyber defence and deterrence, not only by the need to consider public-private cooperation but also to protect civil liberties and privacy.

1.2 Cyber attack

There are several understandings of cyber attacks, ranging from online protests, to cyber frauds, espionage, sabotage or acts of war (Singer and Friedman, 2014, pp. 67-68). NATO Glossary of Terms and Definitions provides the definition of a computer network attack, which is considered as a type of a cyber attack, but there is no specific definition of a cyber attack as such. Computer network attack is defined by NATO as an "Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself" (NSA, 2014, p. 2-C-11; definition from 22 January 2010).

The Tallinn Manual on the International Law Applicable to Cyber Warfare (further on: Tallinn Manual),[3] which was published under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE), defines cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Schmitt, 2013, p. 106). Tallinn Manual is also using the term cyber operation, which can include,

[2] *Despite the fact that cyberspace is usually defined as a borderless domain and compared to the high seas, international airspace or outer space, it has been established that the components of cyberspace, such as cyber infrastructure, are not immune from the territorial sovereignty or national jurisdiction (Heinegg, 2013, p. 126 in Roscini, 2014, p. 23 and UN Doc. A/68/98, 24. June 2013 in Roscini, 2014, p. 23).*

[3] *Tallinn Manual on the International Law Applicable to Cyber Warfare was published in 2013. It was prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD CoE). It does not reflect the NATO doctrine or the official position of any state or organisation (Roscini, 2014, pp. 30-31). Nevertheless, it has developed as an important point of reference on the subject of cyber.*

but is not limited to, cyber attacks, as the "employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace" (Schmitt, 2013, p. 15, 76).

Additionally, Singer and Friedman (2014, pp. 68-72) describe cyber attack as an attack that uses digital means, a computer action, instead of kinetic force. Unlike a conventional attack, it is not constrained by geography or political boundaries. It can be directed against multiple targets, whereby the first target is always a computer and the information within it, although the intended result might be to achieve a physical damage. Harrison (2012, pp. 65-74) distinguishes cyber attacks from the conventional attacks in terms of their indirectness with regard to finding the actual perpetrator as well as intangibility in terms of methods and consequences.[4]

2 SECURITY ENVIRONMENT

Understanding the security environment and assessing the threats is fundamentally important in order to establish better awareness on the risks individual states or international organizations, such as NATO, are accepting, and on the responses they are adopting.

Rapid technological advancement has lead into increased connectivity between computerized devices, a phenomenon known as the Internet of Things, and into dependence on information and communication technology in our everyday lives (Symantec, 2015, p. 5). We are living in an era of digital globalisation, where cyberspace became a vital enabler of modern society, but also its weak link (Kerschisching, 2012, pp. 5-8). In fact, cyber threats are continuously evolving, and with cheaper and more readily available technologies and communications channels, malicious activities of all kinds can blossom (Symantec, 2015, p. 23). The general rule is that any system can be successfully attacked if sufficient effort is made (Hunker, 2013, p. 164 and Singer and Friedman, 2014, p. 56).[5]

Growing and more complex cyber threats to the governments, public sector and critical infrastructure[6] led many countries to strengthen their cyber defences, and,

[4] *See also Hunker, 2013, pp. 156-157, Heinegg, 2013, p. 125 and Yannakogeorgos and Lowther, 2014, p. 51.*

[5] *Practice is showing great persistence of the attackers and their exploitation of 'zero-day' vulnerabilities, which is known as "advanced persistent threat" and includes a more sophisticated level of planning, organization, intelligence, complexity and patience. Zero day is "An attack that exploits a previously unknown vulnerability" (Singer and Friedman, 2014, pp. 299).*

[6] *Critical infrastructure refers to a system of physical networks and facilities that enable societies to survive. Its protection is of mayor importance for the national security of each state. It includes commercial key assets, government facilities, power plants, dams, sectors such as agriculture and food, chemicals and hazardous materials, banking and finance, defence industrial base, energy, water, transportation, telecommunications. Critical information infrastructure became indispensable for the functioning of most critical infrastructure (Kerschischnig, 2012, p. 41-42).*

in some cases, even develop offensive military capabilities (Symantec, 2015, p. 5).[7] Cyber became regarded as a fifth operational domain, besides land, sea, air and space (Gray, 2013, p. ix).[8] Not only nations, but also international organisations became more aware and are increasingly dealing with cyber threats.[9]

Despite the raising awareness that cyber attacks on the critical infrastructure can potentially lead to substantial physical damage, loss of civilian lives, and country's destabilisation, the extreme or worst potential of cyber operations in terms of damaging and disabling critical infrastructure and inflicting physical harm on the people, has not yet materialised (Kerschisching, 2012, p 17).[10] Gray (2013, pp. x-xi) argues that the effects of cyber are going to be the greatest (or most dangerous) as an enabler of joint military operations, while stand-alone strategic cyber attacks are at this point not so likely.[11] Also, Libicki (2013) is of the view that although the risk of devastating cyber attack is real, the perception of the risk is often greater than it actually is.[12] At the same time, cyber threat assessment cannot totally rule out the possibility that a cyber attack will result in a worst case scenario, which means decision makers, nationally or in the international framework, must take decisions based on assessment of likelihood and consequences (Hunker, 2013, pp. 161). In this regard, deterring cyber attacks and providing for a strong defence becomes even more important in the first place.

---

[7] *See NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) for the overview of the national cyber security documents at https://ccdcoe.org/strategies-policies.html [Accessed 19 August 2015].*

[8] *Information and communication technology plays an important part with regard to the military equipment, training, logistics, communications, on the battlefield, and as a possible weapon (Kerschischnig, 2012, p. 85). Militarisation of cyberspace can be seen also from the incorporation of cyber operations in military doctrines, and in the creation of cyber units and commands within the armed forces (Roscini, 2014, p. 10).*

[9] *Several international organisations are dealing with matters of cyber security, such as Council of Europe (2001 Budapest Convention on Cybercrime), European Union, Organisation for Economic Cooperation and Development (OECD), the United Nations General Assembly (UNGA), the International Telecommunication Union (ITA), the Organisation for Security and Cooperation in Europe (OSCE), the World Summit on the Information Society (WSIS), the Internet Governance Forum (IFG) etc.*

[10] *Known cyber attacks offer the insight into what might develop in the future, such as the 2007 attacks against Estonia, 2012 attacks on the company Saudi Aramco, 2010 Stuxnet attack on Iran's Natanz uranium enrichment facility, 2014 Dragonfly attacks of cyber espionage, mainly in the energy sector, or attacks that were carried out as a part of military operations, such as 2008 operation in Georgia, to name just a few (Roscini, 2014, pp. 4-9, Kerschischnig, 2012, pp. 52-56, and Symantec, 2015, p. 65). More recently, cyber threats have evolved further with the attacks on NATO Allies and partners. More recently, the December 2015 cyber attacks on Ukraine power grid represent the first cyber attack taking down the power grid and with this the increased level of sophistication in committing cyber attacks against critical infrastructure, possibly by other states (Sanger, 2. 3. 2016, p.5). This attack came after states agreed in the UN framework norms, rules and principles for the responsible behaviour, which include restraint to intentionally damage critical infrastructure or otherwise impair the use and operation of critical infrastructure to provide services to the public (UN Doc A/70/174, 22 July 2015, para. 13.(f), pp. 7-8).*

[11] *Similar view on the unlikelihood of stand-alone cyber attack or "cyber Pearl Harbor" is expressed also by Gill and Ducheine, 2013, pp. 459-463, Morgan, 2010, p. 58, Waxman, 2013, p. 120 and Harrison, 2012, p. 5, 7.*

[12] *Libicki has been warning against escalation in cyberspace and calling for prudence in managing the cyber crisis. See: Libicki, Martin C., 2013. Cyberwar Fears pose Dangers of Unnecessary Escalation. [Online] Available at: http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cyberwar-fears-pose-dangers-of-unnecessary-escalation.html [Accessed 19 August 2015]. Libicki, Martin C., 2012. Crisis and Escalation in Cyberspace. [pdf] Santa Monica, CA: Rand Corporation. Available at: http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf [Accessed 2 November 2014].*

3 NATO AND CYBER DETERRENCE

3.1 Traditional deterrence

While the concept of deterrence, which can be broadly defined as anything that dissuades an attack (Hunker, 2013, p. 174), has been part of military practice for centuries,[13] most of the analysis has focused on the use of conventional and nuclear weapons during the Cold War (Trujillo, 2014, pp. 43-44 and Goodman, 2010, p. 103).[14] Therefore, before going into cyber deterrence and NATO's approach to it, it is important to understand basic presumptions of classical deterrence theory to see if and how they can be applied to cyberspace.

Deterrence is a concept mostly known in traditional security theory and realist views on international relations (Haley, 2013 and Cooper, 2009, pp. 12-20). Usually, it is linked to the concept of mutually assured destruction (MAD), which basically means that an attack is going to be met with an overwhelmingly destructive counter attack. It rests on the assumptions that the world stability can be maintained if the costs and consequences of war far out-weight its benefits; and that strategies that make defence cheaper and offence more expensive decrease the likelihood of the conflict.[15]

Most often deterrence is brought down to deterrence by denial (the ability to discourage the attack; for example with strong defence) and deterrence by punishment (the treat of retaliation) (Libicki, 2009, p. 7).[16] Hunker (2013, p. 162) adds a third, declaratory and diplomatic, element. More broadly, elements of deterrence include everything from an interest, a deterrent declaration ("do not do this, or that will happen"), to capabilities for denial or penalty, credibility (it has to be believable), as well as reassurance (if the interest is not attacked there will be no penalties). To make it work, both parties have to engage in the regular exchange of deterrent messages or a continuous dialogue (Goodman, 2010, pp. 103-108).[17] Deterrence has to be clear and understandable to everyone. Strategic communication is an important aspect in this regard.

---

[13] *In the History of the Peloponnesian War Thucydides quotes Hermocrates as stating "Nobody is driven into war by ignorance, and no one who thinks that he will gain anything from it is deterred by fear." (Trujillo, 2014, p. 43).*

[14] *In the 1950s the term "nuclear deterrence" was coined by the American military strategist Bernard Brodie. In the 1960s, Thomas Schelling developed theory forward by arguing that the nuclear capacity of a state that possesses nuclear weapons is used as bargaining power, and is most successful when it is held in reserve. See: Brodie, Bernard, 1959. "The Anatomy of Deterrence" as found in Strategy in the Missile Age. Princeton: Princeton University Press, pp. 264–304. Schelling, Thomas, 1966. The Diplomacy of Violence. New Haven: Yale University Press, pp. 1–34.*

[15] *Offense-defence theory argues that there is an offense-defence balance among adversaries, which determines the relative effectiveness of offensive and defensive strategies (the logic of the security dilemma). If the balance shifts to offense than the likelihood of competition and war increases; if the balance shifts towards defence then cooperation among adversaries becomes easier (Shaheen, 2014, p. 78).*

[16] *See also Rühle, 2015, Singer and Friedman, 2014, p. 145 and Haley, 2013.*

[17] *In NATO the idea of deterrence and dialogue, as two concepts that go hand in hand, was introduced in the 1967 Harmel Report ("Report of the Council on the Future Tasks of the Alliance"). This paved the way for the East-West political détente in the 1970 (NATO, 11. 11. 2015).*

In essence, however, deterrence is about the "ability to alter an adversary's action by changing its cost-benefit calculations" (Singer and Friedman, 2014, p. 145). Deterrence is successful when an actor is convinced that restraint from action is acceptable. It is a state of mind of the adversary and thus a psychological relationship (Morgan, 2010, p. 56). It is the adversary who determines whether deterrence is working (Trujillo, 2014, p. 45). Therefore, for successful deterrence it is important to know who to deter or whose mind we would like to change (Singer and Friedman, 2014, pp. 145-147). Deterrence has to be tailored to potential adversaries. During the Cold War, deterrence theory was based on the assumption of rational state adversaries, while now in the changed security environment, where we are faced with increased variety of state and non-state actors, and new relationships among them, this assumption is under question, which makes deterrence even harder.[18]

3.2 Cyber deterrence

Many authors argue that due to the unique characteristics of cyberspace it is difficult to just translate nuclear and conventional deterrence to cyberspace;[19] nevertheless, the majority of them in principle build on the traditional concept of deterrence by denial and deterrence by punishment (defence and offence).

The analysis has shown that the first element of cyber deterrence is a strong defence (Trujillo, 2014, p. 45; Libicki, 2012, pp. 159-162; Haley 2013; Morgan 2010, pp. 75-76; Singer and Friedman, 2014, p. 137, 155; Shaheen, 2014, pp. 78-79; Rühle, 2015). This includes rather passive defensive measures including the enhancement of security and resilience of computer systems, such as: prevention, protection, detection, mitigation, recovery, awareness raising, policies and legal framework, partnerships, information and intelligence sharing etc. Strong defence prevents most intruders to get access into the network or even keep potential intruders from trying, due to the low probability of success. It requires adequate infrastructure and human capital ranging from governmental to private actors, from the industry and academia, from a national to international level. In addition to this, an important part of cyber defence is also the active promotion of arms control and related management in cyberspace. If states could enhance cooperation at the broader international level by developing common standards, arms control measures, or at least confidence building measures, this would lead to greater transparency and trust among them and would improve the chances for attribution.

---

[18] *"As long as both sides act "rationally", i.e. according to a cost-benefit calculus, and if none of them is suicidal, their military potentials will keep each other in check" (Rühle, 2015).*

[19] *Libicki (2009, pp. 41-71) in Trujillo (2014, pp. 47-49) point out some of the challenges: difficult attribution; broad and cheap availability of technology; first-strike advantage cannot be deterred, because in cyberspace many vulnerabilities are unknown; cyberspace actors have a different risk tolerance compared to those operating in strictly physical domain, due to their perceived anonymity, invulnerability, and global flexibility; complexity due to the involvement of third parties (possibly even private companies), unpredictability of consequences etc.*

The second element is active exercise of military influence and threat of retaliation (offensive capabilities). Between the two is a thin line of stronger defence that rests on more advanced capabilities that can already defend against more serious and more sophisticated attacks by applying some initial retaliatory capabilities (Morgan 2010, pp. 75-76).

Successful deterrence by punishment (retaliation) in the cyber domain requires attribution, signalling and credibility. This means the target for deterrence needs to be identifiable, the message needs to be communicated to the intended audience and it has to be believable, which requires a certain level of demonstration of capability (Trujillo, 2014, p. 45). Capabilities for a response can range from cyber, military, economic, political measures and public disclosure (Morgan 2010, pp. 75-76). Even cyberspace deception can fall under this category in a way that cyberspace operations have the ability to manipulate decision-making and thus help to gain advantage and inherently add to deterrence (Trujillo, 2014, p. 47). Most notably, however, deterrence by punishment implies the need for offensive cyber capabilities, which is important to bear in mind with regard to NATO and its cyber capabilities, which, as we are going to see later on, are on the defensive and not offensive side.

The most important element of deterrence is the psychological one. Successful deterrence means affecting the behaviour of potential adversary. For deterrence to work it has to be understood by potential adversaries. It is about dialogue, issuing declarations, warnings and influencing the decisions of potential adversary, including by preserving certain level of ambiguity in policy (Hunker, 2013, pp. 164-165). There are no universal characteristics of adversaries' decision-making that would make deterrence easily effective. There are several factors that need to be considered when preparing the strategy of deterrence, including personal characteristics of a decision-maker, religion, ideology, government structure, culture, geopolitics, broader political context (Payne, 2013, pp. 3-34). Some of these factors are harder to influence than others; even more so in the cyber environment marked by anonymity and multiplicity of actors, ranging from state and non-state, governmental and private, military and civilian actors, each acting in their own specific frameworks; some have a responsibility towards the people, the other can act alone and with nothing to lose. There is a rapid growth of diverse relationships among them, creating multi-dimensional interests and influence and thus demanding new approaches to cyber deterrence, based on social-networks, to affect their perceptions and decision-making calculations (Cooper, 2009, pp. 47-53).[20]

To conclude, it is highly unlikely to eliminate the occurrence of all cyber attacks, but broader and more comprehensive deterrence can help to reduce them (Haley, 2013).

---

[20] *Cooper (2009, p. 95) argues that modern international system appears to act like a large organism comprised of dynamic networks of relationships. The so called "network deterrence" calls for better understanding of these networks and social relationships between their members – cooperation, competition and conflict (Dr. Lochard in Cooper, 2009, pp. 104-124).*

While cyber deterrence often comes down to strong cyber defence, including also a clear declaratory policy, and responsive capabilities (cyber or other), it needs to go beyond the cyber realm, and how this applies to NATO is going to be seen in the next chapters.

3.3 NATO and Cyber Deterrence

Cyber deterrence as a standalone concept does not exist in NATO; what exists is a classical understanding of deterrence as convincing potential aggressor that the "consequences of coercion or armed conflict would outweigh the potential gains" (NSA, 2014, p. 2-D-6). In 2010 NATO devoted an entire chapter of the Strategic Concept to defence and deterrence and Allies pledged to ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of its populations (*Ibid*., para. 17 and 19). In 2012, NATO reviewed its defence and deterrence posture, which now builds on the mix of nuclear, conventional and missile defence forces (NATO, 20. 5. 2012). In 2014, with the changing security environment, deterrence has re-emerged in the context of NATO (Rühle, 2015). With the crisis in Ukraine, which is seen as an example of hybrid warfare, non-military aspects of deterrence became more important, such as cyber, energy and strategic communications, which demands from NATO to update its concepts and tools of deterrence to fit the 21st century threats.

Specifically on cyber deterrence in NATO, we can see that elements of it are nevertheless already present. Its main focus is on building a strong cyber defence. Deterrence by punishment is mainly framed through Article 4 consultation and Article 5 invocation of collective defence. NATO does not have offensive capabilities, but several nations do, and they could be used as well (Healey and Tothova Jordan, 2014, p. 6). At the same time, there might be a need for NATO itself to consider more responsive cyber capabilities for greater credibility (Hunker, 2013, p. 164). Above all, to increase the success of deterrence, NATO has to provide credible and convincing declaration that it takes cyber threats seriously and is ready to respond with decisive actions, which is to some extent done by the 2014 Enhanced NATO Cyber Defence Policy, as we are going to see in the next chapter.

3.3.1 NATO Cyber Defence Policy

The protection of key Alliance information and communication systems, has always been important for NATO, even more so with the global spread of technology and with growing attempts from the side of adversaries (state and non-state actors) to try to exploit and disrupt the Alliance's increasing reliance on information systems (NATO, 30. 9. 2014 and Strategic Concept, 1999, para. 23). Cyber defence appeared on NATO's political agenda in 2002 after its systems were attacked from activists in Serbia, Russia and China during the Kosovo Conflict (Kerschischnig, 2012, p. 97 and Healey and Tothova Jordan, 2014, p.1). At the 2002 Summit in Prague, NATO Heads of State and Government decided to strengthen the capabilities to

defend against cyber attacks (Prague Summit Declaration, 2002, para. 4.f). At the Summit in Riga in 2006 the need to improve the protection of key information systems against cyber attacks was reiterated (Riga Summit Declaration, 2006, para. 24).

After the 2007 cyber attacks on Estonia, Allied Ministers of Defence agreed, in June 2007, to step up the efforts, which led to the adoption of the first Policy on Cyber Defence in 2008 (NATO, 30. 9. 2014 and Kerschischnig, 2012, 97). The policy emphasised that the responsibilities for the protection of key information systems lie with NATO and nations; it further reiterated the importance of developing cyber defence capabilities, and it called for sharing of best practices and providing "a capability to assist Allied nations, upon request, to counter a cyber attack" (Bucharest Summit Declaration, 2008, para. 47). In the same year, the conflict in Georgia revealed the potential of linking cyber attacks to the conventional attacks (NATO, 30. 9. 2014).

In 2010 the Heads of State and Government agreed to enhance cyber defence capabilities, in light of rapidly increasing and more sophisticated cyber threats (Lisbon Summit Declaration, 2010, para. 2, 40). They recognised, in the NATO Strategic Concept (2010, para. 9-15), that cyber attacks are among the threats and challenges that are directly or indirectly affecting the security of the citizens of NATO countries. Strategic Concept (2010, para. 12) also acknowledged that "cyber attacks are becoming more frequent, more organized and more costly in the damage they inflict on government administrations, businesses, economies, and potentially, also transportation 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 services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks". Therefore, cyber defence capabilities became part of the whole set of capabilities necessary to deter and defend against any threat to the safety and security of the populations (*Ibid*., para. 19).

In June 2011, NATO Defence Ministers adopted the second Policy on Cyber Defence, which set the framework for more coordinated efforts throughout the Alliance in strengthening cyber defence capabilities (NATO, 30. 9. 2014 and Chicago Summit Declaration, 2012, para. 49). And three years later they adopted the third policy called an Enhanced Cyber Defence Policy (NATO, 30. 9. 2014 and Wales Summit Declaration, 2014, para. 72).

From the comparison of different Summit Declarations, it seems, that the new 2014 policy represents an upgrade from a more technical approach of the protection of communication and information systems, to the higher comprehensive political framework. The policy reaffirms the principles of indivisibility of Allied security, of prevention, detection, resilience, recovery, and defence; it recalls the primary responsibility of NATO to defend its own networks, and of Allies to develop their

own cyber defence capabilities for the protection of their networks (Wales Summit Declaration, 2014, para. 72). There is no mentioning of the offensive capabilities, the only focus rests on defence.[21]

The policy also recognises that international law, including international humanitarian law and UN Charter, applies in cyberspace (*Ibid*.). The policy reaffirms that "cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability". And it goes further, by saying that "Their impact could be as harmful to modern societies as a conventional attack", which has led the Heads of State and Government, in Wales, to declare for the first time that cyber defence is part of collective defence (*Ibid*.). They have further specified that a "decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis." (*Ibid*.). Assistance of Allies is addressed in the spirit of solidarity.

It is important to note also that 2014 policy was adopted in the time when the Alliance has started to face significantly changed security environment with Russia's aggressive actions against Ukraine and growing instabilities in NATO's southern neighbourhood, from the Middle East to North Africa, have altered (Wales Summit Declaration, 2014, para. 1). A new quality of threats emerged – hybrid warfare threats, which include a "wide range of overt and covert military, paramilitary, and civilian measures /which/ are employed in a highly integrated design" (*Ibid*., para. 13). Cyber threats are seen as one of the components of hybrid warfare (Blum et all, 2015), as such the need to defend against and deter cyber attacks should become even more important for NATO.

3.3.2 Cyber Defence as part of Collective Defence

As enshrined in the current NATO policy, cyber defence is part of collective defence (Wales Summit Declaration, 2014, para. 72), which is an important declaratory statement with significant deterrence value, but what does this mean in practice.

The principle of collective defence, as enshrined in Article 5 of the North Atlantic Treaty, is at the centrepiece of NATO. Article 5 states that an armed attack against one or more Allies shall be considered an attack against all Allies, which is reflecting the spirit of solidarity and assistance within the Alliance (NATO, 2.

[21] *NATO's approach to cyber threats is defence and not offense. It is, however, not identified, whether it is active or passive defence, whereby both terms are defined in NATO Glossary of Terms and Definitions. Active defence is defined as "Active measures taken against enemy forces to prevent, nullify or reduce the effectiveness of any form of enemy attack" (NSA, 2014, p. 2-A-2; definition from 25 January 2005). And passive defence are "Passive measures taken for the physical defence and protection of personnel, essential installations and equipment in order to minimize the effectiveness of hostile action" (NSA, 2014, p. 2-P-2; definition from 17 January 2005).*

6. 2014).[22] With the invocation of Article 5, Allies can provide assistance they deem necessary in a given situation to restore and maintain the security of the North Atlantic area. So far, Article 5 was invoked as a response to 9/11 attacks in 2001; however, reassurance measures to enhance defences of Allies were applied also more recently as a response to Russian aggressive actions in Ukraine in 2014 (NATO, 2. 6. 2014).

In the future, cyber threats relevant for NATO might come as a component of a larger conflict or as a tool of a major state power used during periods of tension. As in the past, cyber attacks may come as a response to NATO's engagements, its operations and its posture. It is more likely to envision cyber attack on an Ally than a conventional attack. There is also a risk of cyber attacks committed by terrorists or political extremists, even cyber attacks committed by accident or as part of cyber espionage (Hunker, 2013, pp. 159-160).

Response to an actual cyber attack, like a conventional attack on an Ally, would be approached on a case-by-case basis, as it is stated in NATO's policy on cyber defence itself (Wales Summit Declaration, 2014, para. 72). NATO does not respond automatically, but based on a request from an Ally. That Ally decides when it needs assistance from the Alliance. NATO's response is framed by the provisions of the North Atlantic Treaty and requires consensus. Assistance is not automatically collective defence or a military response. It can be any action deemed necessary in order to restore and maintain security. Response also does not have to be mathematically equal to the type and scale of the attack. It could be a political action, declaratory support or, if so decided, even technical assistance.

An Ally could invoke Article 4 consultations or Article 5. While any state could declare that specific cyber attack falls under Article 5 (act of war/use of force), acting upon that declaration is another thing. At the same time, even in the event of a serious and devastating cyber attack, there is no obligation to invoke Article 5. North Atlantic Council (NAC), which has the authority to decide in such a situation, would consider specific political, strategic and other circumstances. Most likely NAC is going to consider the scope (are the effects spreading through wider geographical area or the effects on the critical infrastructure), duration (is it a single attack or part of a longer campaign), intensity/scale (has it caused physical damage or deaths) and external actor (is it foreign or a domestic attacker) (Healey and Tothova Jordan, 2014, p. 7). The actual decision on NATO's reaction to a cyber attack will depend on the perceptions of an attack by Allies and on consensus

[22] *Article 5 is complemented by Article 6 of the North Atlantic Treaty, which stipulates that such armed attack is an attack on NATO territory or on the forces, vessels, or aircraft of any Ally (North Atlantic Treaty, 1949, Article 6). The primary responsibility for the maintenance of international peace and security rests with the UN Security Council (North Atlantic Treaty, 1949, Article 7). Other two important basic principles or the Alliance are encompassed in Article 3, whereby the Allies are pledging to take care of their defences and build, individually and collectively, their resistance to armed attacks; and in Article 4, which offers a basis for consultations, when territorial integrity, political independence or security of any of the Allies is threatened (North Atlantic Treaty, 1949).*

needed to take decisions on the level of the Alliance (Hunker, 2013, p. 161). In the end, it is going to be a political decision.[23]

There is no need to define precisely when a cyber attack might constitute an armed attack and as such a threat to the security, because it is exactly this ambiguity that constitutes certain level of deterrence on potential cyber adversaries. Namely, collective defence response to a cyber attack would mean that there is the whole range of NATO capabilities at its disposal, politically and military, reaching from the conventional to nuclear forces, in the framework of the international law.

Despite declared policy, Healey and Tothova Jordan's (2014, p. 4) assess that it is very unlikely that the NAC would invoke collective defence unless there were significant kinetic effects such as damage and deaths (comparing it with 9/11 response). NATO members have been cautious in the past. When the attacks on Estonia happened in 2007 the discussions on cyber defence were framed in the context of Article 4 of the Washington Treaty calling for political consultations, rather than Article 5, collective defence (Harrison, 2012, p. 39 and 57). Such a response, where NATO would be divided or unable to respond decisively, might negatively affect its credibility and would have a negative effect on deterrence.

3.3.3 International law and its application to responding to cyber attacks

NATO's response to cyber attacks is bound to follow the framework of the international law. What this means in practice and how is this going to affect the decisions taken by the Alliance in the context of possible Article 5 invocation, is going to be the subject of the analysis in this chapter.

Cyber attacks are a new challenge to the international law since they represent a new method of warfare (Harrison, 2012, pp. 279-280). There are no special rules and legal principles for the use of force in cyberspace, but there seems to be an agreement among states that the existing international law, existing treaties and customary norms apply (Gill and Ducheine, 2013, p. 439, Heinegg, 2013, pp. 123-124). This is also the approach NATO is taking with the 2014 policy, which acknowledges that

[23] *The invocation of Article 5 is not necessarily immediate and in the context of cyberspace it could take even more time. When Article 5 was invoked as a response to 9/11 attacks it started with the NAC statement condemning the attacks on 11 September 2001, which was followed by the invocation of the principle of Article 5 on 12 September 2001, with the explanation that Article 5 will apply if it is determined that the attack on the United States was directed from abroad, and finally, the invocation of Article 5 was confirmed on 2 October 2001 with the finding that the attack was directed from abroad (NATO 12. 9. 2001a, NATO 12. 9. 2001b, NATO, 2. 10. 2001). Once Article 5 was invoked, NATO acted in the framework of collective defence. This did not prevent NATO from taking action in the interim nor individual NATO Allies to offer bilateral assistance.*

international law, including international humanitarian law and UN Charter, applies in cyberspace (Wales Summit Declaration, 2014, para. 72).[24]

International law governs the right to wage war and the conduct in warfare through the law of armed conflict, including the rules addressing the legality of war (*jus ad bellum*) and rules regulating the conduct of hostilities (*jus in bello* or international humanitarian law) (Kerschischnig, 2012, 102). The key treaties are 1945 UN Charter, 1899 and 1907 Hague Conventions, four 1949 Geneva Conventions and their two 1977 Additional Protocols (Roscini, 2014, pp. 19-21). The question is how this applies to the concept of cyber attacks.

Threat or use of force in international relations against the territorial integrity or political independence of any state, or in any other way inconsistent with the purposes of the UN, is prohibited (Article 2 (4) UN Charter), with the exception of self-defence (Article 51 UN Charter) and collective measures authorized by the Security Council (Articles 42 and 53 UN Charter) (Kerschischnig, 2012, pp. 105-110). A cyber attack that constitutes a threat or use of force against the territorial integrity or political independence of any state, or that is in any other way inconsistent with the purposes of the UN, is thus unlawful (Tallinn Manual, Rule 10 in Schmitt, 2013, p. 42).

The next question is under which conditions can the cyber attacks be classified as a "use of force"? A cyber attack constitutes a use of force when its scale and effects are comparable to non-cyber attacks rising to the level of use of force (Tallinn Manual, Rule 11 in Schmitt, 2013, p. 45). Each attack has to be assessed on its own merits.

So, when does self-defence come into play? The most serious and dangerous form of the illegal use of force and a crime against international peace is the aggression.[25] Armed force is one type of aggression.[26] Element of armed force is important for the establishment of the right to self-defence. Self-defence comes down to the question whether the use of force amounts to an armed attack (Kerschischnig, 2012,

---

[24] *A certain degree of consensus among the experts on the applicability of international law to cyber attacks can also be found in the Tallinn Manual on the International Law Applicable to Cyber Warfare, which also concludes that general principles of international law apply to cyberspace (Schmitt, 2013, p. 13). Similar conclusion was also reached by the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) (UN Doc A/68/98, 24 June 2013, p. 8 and UN Doc A/70/174, 22 July 2015, pp. 12-13). The Group of Experts identified following principles of the UN Charter and other international law that apply in cyberspace: "sovereign equality; the settlement of international disputes by peaceful means and in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States" (UN Doc A/70/174, 22 July 2015, p. 12, para. 26).*

[25] *UN General Assembly, Definition of Aggression, GA Res. 3314 (XXIX) of 14 December 1974.*

[26] *Article 3 GA Res. 3314 provides examples for acts of aggression, such as: invasion or attack by the armed forces, bombardment by the armed forces of one State against the territory of another State, blockage of ports or coasts by the armed forces of another State, an attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State, one State allowing another State to use its territory for perpetrating an act of aggression against a third State, sending of armed bands, groups, irregulars or mercenaries to another State to carry out acts of armed force (Kerschischnig, 2012, p. 112).*

pp. 112-113).[27] The burden of proof rests with the state exercising the right of self-defence (Kerschischnig, 2012, p. 141 and Harrison, 2012, pp. 99-102).

As a result, the attacked state has an inherent right of individual or collective self-defence,[28] until the UN Security Council has taken measures necessary to maintain international peace and security (Article 51 UN Charter).[29] Whether a cyber attack constitutes an armed attack depends on its scale and effects (Tallinn Manual, Rule 13 in Schmitt, 2013, p. 54).[30] This extends beyond kinetic armed attacks; it is not the weapon that is in the forefront but the effects of an attack or its potential consequences (Schmitt, 2013, pp. 54-55).[31] Based on the analysis of national cyber defence strategies, Gill and Ducheine (2013, p. 444) argue that an armed attack could even include a cyber attack on a critical infrastructure of a state, if it would severely undermine state's ability to carry out essential state functions or severely undermine its economic, political and social stability for a longer period of time.[32]

In situations of an armed conflict, international humanitarian law (jus in bello), usually referring to the conduct of hostilities (Hague Conventions) and minimum protection to individuals involved in armed conflict (Geneva Conventions and their Additional Protocols), applies. Thus far there has been no direct link to cyber attacks. Nevertheless, in accordance with the Martens clause, in the event of new situations

---

[27] *Article 49 (1) of the Additional Protocol I to the Geneva Conventions defines attacks as "acts of violence against the adversary, whether in offense or in defence". In: Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Example of elements that constitute an attack can be found also in Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits) (1986) ICJ 14, International Court of justice.*

[28] *States can also use countermeasures that are close to self-defence, such as retorsions and reprisals to deter an adversary and convince him to return to lawful behaviour. This right belongs only to states victims of wrongful acts and not to the third-states, not even under collective self-defence (Kerschischnig, 2012, pp. 123-124). »A retorsion in international law is an unfriendly – but not illegal – act by a state in response to an unfriendly or unlawful act by another state. On the contrary, a reprisal is an act that per se is illegal under international law, but can be justified as a response to an unlawful act of another state. However, only defensive reprisals can be permissible« (Ibid.).*

[29] *Collective self-defence against a cyber attack amounting to an armed attack may only be exercised at the request of the victim state and within the scope of the request (Tallinn Manual, Rule 16 in Schmitt, 2013, p. 67).*

[30] *On the effects see also: Kerschischnig, 2012, p. 141, Chen, 2013, p. 33.*

[31] *See also: Singer and Friedman, 2014, p. 125; Delibasis, 2009, p. 97 and Kerschischnig, 2012, pp. 110-114 and 178-180.*
At the same time, cyber criminal activity, espionage, other forms of unauthorised penetration, theft of data and sabotage of public or private computer systems that do not fall in the definition of an armed attack are not subject to the law relating to self-defence (Gill and Ducheine, 2013, p. 440). However, even if the cyber attack does not rise to the level of a use of force criteria, it does not mean it is permitted. It is likely, that a cyber attack, which is severe enough to raise this question, might be "considered an unlawful interference in the affairs of a state, and may in all likelihood amount to the threat to the peace" (Harrison, 2012, p. 74).

[32] *For similar arguments see also Tsagourias, 2012, pp. 231-232; Schmitt, 2012, pp. 288-289; Sharp in Harrison, 2012, pp. 81-82; Singer and Friedman, 2014, pp. 122-124; and NATO Parliamentary Assembly, Annual Session 2009, Committee Report 173, paras 58-61, available at: http://www.nato-pa.int/Default.asp?SHORTCUT=1782 [Accessed 20 August 2015].*
While the attacks in Estonia in 2007 and in Georgia in 2008 did not reach this level (no loss of life, physical injury or destruction of property as a result of cyber attacks), the 2010 Stuxnet worm would amount to a use of force, but its scale and effects did not appear to have sufficient gravity to amount to an armed attack (Harrison, 2012, pp. 81-82).

or new forms of warfare, customary international law applies (Kerschischnig, 2012, pp. 175-177, Harrison, 2012, pp.127-128 and Schmitt, 2013, pp. 77-78). Cyber attacks executed in the context of an armed conflict are thus subject to the law of armed conflict; in both international and non-international armed conflicts (Tallinn Manual, Rule 20 in Schmitt, 2013, p. 75).[33]

The response to the attack has to be in accordance with the principles of necessity and proportionality (Tallinn Manual, Rule 14 in Schmitt, 2013, p. 61). A state victim may resort to proportionate countermeasures against the offending state, with intention to induce compliance with the international law by the offending state (Tallinn Manual, Rule 9 in Schmitt, 2013, pp. 36-37). Proportionality does not require mathematical equivalence nor does it define the modalities of self-defence (Gill and Ducheine, 2013, pp. 449-450). In essence, states are not restricted only to cyber responses; however, there is a danger of cyber attacks escalating into conventional attacks (Harrison, 2012, pp. 102-104).

Necessity requires an armed attack that is ongoing or imminent (Tallinn Manual, Rule 15 in Schmitt, 2013, p. 63). The principle of necessity is linked to the question of timely response; immediacy requires that self-defence measures must not be duly delayed (see also Tallinn Manual, Rule 15 in Schmitt, 2013, p. 63). This implies reasonable action within a reasonable timeframe in response to an ongoing attack or a clear threat of the attack in the future (Gill and Ducheine, 2013, p. 451).

This opens a question of legality of response in the event of anticipatory or pre-emptive self-defence in case of a manifest and unequivocal threat of attack in the near future or preventive self-defence to a potential attack at some indeterminate point in the future (*Ibid*., pp. 452-458). Gill and Ducheine (2013, pp. 453) argue that there is no universal consensus on either, but while the first is being more or less accepted by the international law and state practice, the second is more controversial. Nevertheless, many nations claim that bona-fides self-defensive actions can only come after an armed attack and not before (Dunlap, 2014, pp. 217). The Group of Experts from the Tallinn Manual took the "last feasible window of opportunity" approach, whereby they agreed that state might act in anticipatory self-defence, cyber or kinetic, when the attacker is clearly committed to launching an armed attack and the victim state will lose its opportunity to effectively defend itself unless it acts (Schmitt, 2013, pp. 64-65).

Moreover, there is also the question of attribution; the importance of knowing the attacker and obtaining reasonably credible and convincing evidence. This is not only the question of identifying the source, a computer, but also the person operating the computer and the 'mastermind' behind the attack. It is very difficult to establish

[33] *Similarly, the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) noted that the established legal principles, including the principles of humanity, necessity, proportionality and distinction apply in cyberspace (UN Doc A/70/174, 22 July 2015, p. 13)).*

with any certainty who is actual perpetrator of the attack, due to the anonymity of the cyberspace, the possibility of launching multi-stage cyber attacks (for example due to IP spoofing or proliferation of botnets)[34] and/or speed with which cyber attack can materialize (Tsagourias, 2012, p. 233). In the end, attribution is a technical, legal and political process. Technical attribution has to be complemented with intelligence and information analysis on the profile, capabilities, intent and affiliations of the authors of the attack, as well as on the political context in which the attack took place (Tsagourias, 2012, pp. 233-234).

A state bears international legal responsibility for a cyber attack attributable to it and which constitutes a breach of an international obligation in a form of an act or omission (Tallinn Manual, Rule 6 in Schmitt, 2013, p. 29). When the actions of non-state actors (private companies, private citizens etc.) can be attributable to the states, in terms of support and control, their actions can qualify as an armed attack subject to the UN Charter (Kerschischnig, 2012, pp. 110-114 and Schmitt, 2013, pp. 26-29).[35]

At the same time we cannot but recognise the possibility that some groups might act on their own, without a state control and influence, and commit an armed attack comparable in scale and effect to an armed attack by states, which would still fall under the law on self-defence and non-state actor could become a direct target of self-defensive action (Gill and Ducheine, 2013, p. 446 and Tsagourias, 2012, pp. 236). In such a case, if the state, where the non-state actor is located, consented, such consent would form a legal basis in addition to or in place of self-defence for taking action by the target state (Gill and Ducheine, 2013, p. 450).[36]

To conclude, besides the legal perspective we need to consider also strategic perspective, linking the right of armed self-defence to the long-term policy interests including security and stability, as well as a political perspective, which is taking into account the situational context of decision making (Waxman, 2013, pp. 110-120). In the end legal analysis comes down to politics. A decision whether cyber attack reaches the threshold of war will be political and a matter of judgement and not automaticity (Singer and Friedman, 2014, p. 126). State practice is still evolving, therefore, it is going to be difficult to build a legal consensus on the question, especially as it seems that major actors in this field have divergent strategic interests (Waxman, 2011, pp. 425-426 and Dunlap, 2014, pp. 213-214).

---

[34] *For example, DDoS Attack in Estonia in 2007 involved a large botnet of approximately 85 000 hijacked computers from around 178 countries (Tsagourias, 2012, p. 233).*

[35] *International Court of Justice uses the term "effective control", which goes beyond mere financing and equipping, and involves also participation in planning and supervision (Schmitt, 2013, pp. 32-33). The mere fact that cyber attack has been launched from governmental cyber infrastructure or was routed through a state is not sufficient evidence for attributing the operation to that state (Tallinn Manual, Rules 7 and 8 in Schmitt, 2013, pp. 34-36). On this see also: Tsagourias, 2012, pp. 236 and Gill and Ducheine, 2013, p. 445.*

[36] *Yannakogeorgos and Lowther (2014, p. 51) have a bit more radical approach in this regard, saying that "rather than individual accountability, nation-states should be held culpable for the malicious actions and other cyber threats originating in or transiting information systems within their borders, or owned by registered corporate entities therein". They are also of the opinion that a global culture of cyber security would help in mitigating the risk of a country being used as a transit or origin point for a cyber attack (Ibid., pp. 51-52).*

Conclusion

Growing and more complex cyber threats are leading many countries and NATO into strengthening their cyber defences and adopting more proactive approaches to cyber security. Even though it is assessed that a strategic standalone cyber attack on NATO or Allies is, at this point, not so likely, it is the perceived risk or potential devastation, in the form of physical damage, disabling of critical infrastructure, loss of civilian lives and destabilisation of states that is the driving force of the decisions taken by the states, nationally and internationally. The states are the ones bearing responsibility for the security of their territories and populations; therefore, it is in their interest to ensure the security in cyberspace and dissuade potential adversaries from attacking them. This cannot be done just by transferring the experiences and approaches from the nuclear and conventional deterrence of the Cold War. Cyberspace is different and demands new ways of thinking and acting.

Cyber deterrence seems to come down to the following elements: strong cyber defence, clear messaging that some actions are unacceptable and will thus have consequences, and credible responsive capabilities, cyber and other. In essence, however, it is a very psychological and behavioural question, which refers to adversary's state of the mind. It is about perceptions; the adversary calculating that the attack is not worth it and that restraint is more acceptable. Each adversary has its own characteristics and deterrence strategy has to be tailored according to them. Cyber deterrence is thus never going to be one hundred percent successful. There is always going to be a risk of a cyber attack. To prevent as many attacks as possible, deterrence has to go beyond cyber and beyond traditional concepts. It has to be broader and more comprehensive.

NATO's defence and deterrence posture rests on the mix of nuclear, conventional and missile defence forces. In the changed security environment, defined also through the hybrid warfare, non-traditional aspects are becoming more important, such as cyber and strategic communications. NATO has made an important step forward in terms of cyber deterrence in 2014 when it declared that cyber defence is part of collective defence. Another important element was ambiguity in its policy, with regard to the activation of Article 5 and possible responses to a cyber attack, which has put all options on the table.

But the question is, if such an approach, resting only on cyber defence and leaving offensive cyber capabilities to individual member states, is enough to successfully deter, to the highest extent possible, future cyber attacks. Allies could offer their offensive capabilities as assistance to other Allies or NATO, if required. However, in the future, following further developments in the cyberspace, NATO, as a military Alliance, could also consider adding such capabilities to its own repertoire. However, just adding offensive cyber capabilities on the list of NATO capabilities is not so simple. NATO has been cautious in the past. Its response to 2007 cyber attacks on Estonia is a case in point. Nevertheless, Estonian experience has pushed forward the development of cyber defence within the Alliance, and possible new cyber attacks on NATO and its Allies or even partners may bring the matter even further.

By developing only defensive capabilities, NATO is portraying itself as a defensive Alliance, which, in itself, is an important political message. Too much emphasis on the offensive cyber responses can lead to an arms race, unpredictable spill-over effects, or even into making the matters worse when applied under the conditions of blurred circumstances of hybrid warfare, where attribution and evidences will not be totally clear. Besides, an important element of constraint is also NATO's adherence to the international law in cyberspace, which is providing a legal framework for its response to a cyber attack. A decision to invoke Article 5 as a response to a cyber attack is always going to be a political one, done on a case-by-case basis, and it will include broader political and strategic considerations, but it has to be legal and legitimate. However, decision might take time and time is not always in abundance when dealing with matters of urgency in a cyber crisis situations. Building consensus within an Alliance is not going to be easy. The future will tell how NATO is actually going to react in a given situation. And this in turn will also going to send an important message for the credibility of the Alliance and will greatly affect the success of its cyber deterrence.

To conclude, effective cyber deterrence goes hand in hand with the overall credible and strong defence and deterrence posture of NATO. A posture that corresponds to the new and emerging security challenges in the ever changing security environment. It is the broader picture that matters. This includes the ability of NATO and its Allies to stand united, be willing and able to respond in a timely manner and act coherently, as well as to generate the required resources (human, financial and technological), invest in defence by developing and maintaining appropriate capabilities and forces. Moreover, it is about the people and new ways of working together. What is needed is greater cooperation and greater sharing of information on every possible level, nationally and internationally, with partner nations, international organisations, industry and academia. A new quality of trust has to be forged to enable such modus operandi. And lastly, this has to be communicated to the public. It is a matter of transparency, generating legitimacy, but also a matter of warnings towards the adversary and thus, a matter of the general success of deterrence.

Bibliography

1. *Blum, R., Evelina, Z., Sadia, R., Soliman, E., 2015. The Future of NATO in the Face of Hybrid Threats. [Online]. Available at: http://www.academia.edu/11044703/THE_FUTURE_OF_NATO_IN_THE_FACE_OF_HYBRID_THREATS [Accessed 29 August 2015].*
2. *Chen, T. M., 2013. An Assessment of the Department of Defence Strategy for Operating in Cyberspace. The Letort Papers. [pdf] Strategic Studies Institute, US Army War College, Carlisle, PA. Available at: http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1170.pdf [Accessed 2 November 2014].*
3. *Cooper, J. R., 2009. New Approaches to Cyber-Deterrence: Initial Thoughts on a New Framework. Prepared under contract number N65236-08-D-6805, Under Secretary of Defence for Intelligence, Joint & Coalition Warfighter Support, Cyber, Information Operations and Strategic Studies Task Order, DWAM80950, 29. 12. 2009. [Online] Available at: http://www.americanbar.org/content/dam/(aba/mitigate/2011_build/law_national_security/new_approaches_to_cyber_deterrence.authcheckdam.pdf [Accessed 16 November 2015].*

4. *Delibasis, D., 2009. Information warfare operations with the concept of individual self-defence. In: Karatzogianni, Athina ed., 2009. Cyber Conflict and Global Politics. Abingdon, UK: Routledge. Ch.7, pp. 95-111.*
5. *Dunlap, C. J., Jr., 2014. Pespectives for Cyberstrategists on Cyberlaw for Cyberwar. In Yannakogeorgos, Panayotis A. & Lowter, Adams B. eds., 2014. Conflict and Cooperation in Cyberspace: The Challenge to National Security. Boca Raton, FL: Taylor & Francis, pp. 211-226.*
6. *Gartner, Int., 2014. Gartner says 4.9 billion connected "things" will be in use in 2015. Press release, Barcelona, Spain, 11 November 2014. [Online] Available at: http://www.gartner.com/newsroom/id/2905717 [Accessed 13 July 2015].*
7. *Gill, T. D., Duchein, P. A. L., 2013. Anticipatory Self-Defense in the Cyber Context. International Law Studies, U.S. Naval War College, Vol. 89, pp. 438-471.*
8. *Goodman, W., 2010. Cyber Deterrence: Tougher in Theory than in Practice? [pdf] Strategic Studies Quarterly, Fall, pp. 102-135. Available at: http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf [Accessed 2 November 2014].*
9. *Gray, C. S., 2013. Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling. [pdf] Carlisle, PA: US Army War College. Available at: http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf [Accessed 2 November 2014].*
10. *Haley, C., 6. 2. 2013. A theory of cyber deterrence. Available at: http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/ [Accessed 20 August 2015].*
11. *Harrison D. H., 2012. Cyber Warfare and the Laws of War. Cambridge University Press, Cambridge, UK.*
12. *Healey, J., Tothova, J, K., September 2014. NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow. [pdf] Issue Brief. Atlantic Council. Available at: http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf [Accessed 2 November 2014].*
13. *Heinegg, W. H., 2013. Territorial Sovereignty and Neutrality in Cyberspace. International Law Studies, U.S. Naval War College, Vol. 89, pp. 123-156.*
14. *Hunker, J., 2013. NATO and Cyber Security. In: Herd, Graeme P. and Kriendler eds., 2013. Understanding NATO in the 21st Century: Alliance Strategies, Security and Global Governance. Abingdon, UK: Routledge. Ch. 10, pp. 154-175.*
15. *Kerschischnig, G., 2012. Cyberthreats and International Law. The Hague: Eleven International Publishing.*
16. *Libicki, M. C., 2009. Cyberdeterrence and Cyberwar. [pdf] Santa Monica, CA: Rand Corporation. Available at: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf [Accessed 2 November 2014].*
17. *Libicki, M. C., 2012. Crisis and Escalation in Cyberspace. [pdf] Santa Monica, CA: Rand Corporation. Available at: http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf [Accessed 2 November 2014].*
18. *Libicki, M. C., 2013. Don't Buy the Cyberhype. Foreign Affairs, [Online] 14 August. Available at: http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype [Accessed 2 November 2014].*
19. *Morgan, P. M., 2010. Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm. [pdf] Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies Press. Available at: http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059436.pdf [Accessed 2 November 2014].*
20. *NATO, 20. 5. 2012. Deterrence and Defence Posture Review. [Online] (Updated 21 May 2012). Available at: http://www.nato.int/cps/en/natolive/official_texts_87597.htm [Accessed 15 July 2015].*

21. *NATO, 30. 9. 2014. Cyber defence. [Online] (Updated 30 September 2014). Available at: http://www.nato.int/cps/en/natohq/topics_78170.htm [Accessed 2 November 2014].*
22. *NATO, 11. 11. 2014. The Harmel Report. [Online] (Updated 11 November 2014). Available at: http://www.nato.int/cps/en/natohq/topics_67927.htm [Accessed 1 December 2015].*
23. *NATO, 2. 6. 2014. Collective defence. [Online] (Updated 2 June 2014). Available at: http://www.nato.int/cps/en/natohq/topics_110496.htm [Accessed 5 November 2014].*
24. *NATO, 12. 9. 2001a. A moment of great tragedy and mourning. NATO Update. [Online] (Updated 14 September 2001). Available at: http://www.nato.int/docu/update/2001/1001/e1002a.htm [Accessed 20 August 2015].*
25. *NATO, 12. 9. 2001b. NATO reaffirms Treaty commitments in dealing with terrorists attacks against the US. NATO Update. [Online] (Updated 15 September 2001). Available at: http://www.nato.int/docu/update/2001/0910/e0912a.htm [Accessed 20 August 2015].*
26. *NATO, 2. 10. 2001. Invocation of Article 5 confirmed. NATO Update. [Online] (Updated 3 October 2001). Available at: http://www.nato.int/docu/update/2001/0910/e0911a.htm [Accessed 20 August 2015].*
27. *NSA (NATO Standardisation Agency), 2014. NATO Glossary of Terms and Definitions.. [pdf] NATO standard AAP-06(2014). Available at: http://nso.nato.int/nso/zPublic/ap/aap6/AAP-6.pdf [Accessed 10 July 2015].*
28. *Payne, K. B., ed., 2013. Understanding Deterrence. New York: Rutledge.*
29. *Roscini, M., 2014. Cyber Operations and the Use of Force in International Law. Oxford, UK: Oxford University Press.*
30. *Rühle, M., 20. 4. 2015. Deterrence: what it can (and cannot) do. NATO Review. [Online]. Available at: http://www.nato.int/docu/review/2015/Also-in-2015/deterrence-russia-military/EN/ [Accessed 15 July 2015].*
31. *Sanger, D. E, 2016. After cyberattack in Ukraine, U.S. tells utilities to be on alert. In International New York Times, 2. 3. 2016, p. 5.*
32. *Schmitt, M. N., ed., 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge, UK: Cambridge University Press. Available at: http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf [Accessed 20 August 2015].*
33. *Schmitt, M. N., 2012. "Attack" as a Term of Art in International Law: The Cyber Operations Context. [pdf] 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn. Available at: http://www.ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf [Accessed 2 November 2014].*
34. *Singer, P.W., Friedman, A., 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press.*
35. *Symantec, 2015. Internet Security Threat Report. Government. April 2015, Volume 20.*
36. *Trujillo, C., 2014. The Limits of Cyberspace Deterrence. [pdf] JFQ/Joint Force Quarterly, 75, 4th Quarter, pp. 43-52. Available at: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-75/jfq-75_43-52_Trujillo.pdf [Accessed 2 November 2014].*
37. *Tsagourias, N., 2012. Cyber Attacks, Self-Defence and the Problem of Attribution. Journal of Conflict and Security Law, 17(2), pp. 229-244.*
38. *UN Doc A/68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013. Available at: http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf [Accessed 20 August 2015].*
39. *UN Doc A/70/174, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [Accessed 20 September 2015].*

40. *Waxman, M. C., 2011. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). [pdf] The Yale Journal of International Law, 36(2). Available at: http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf [Accessed 2 November 2014].*
41. *Waxman, M. C., 2013. Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions. International Law Studies, U.S. Naval War College, Vol. 89, pp. 109-122.*
42. *Yannakogeorgos, P. A., Lowter, A. B., 2014. The prospects for Cyber Deterrence. American Sponsorship of Global Norms. In Yannakogeorgos, Panayotis, A., Lowter, A. B. (eds.), 2014. Conflict and Cooperation in Cyberspace: The Challenge to National Security. Boca Raton, FL: Taylor & Francis, pp. 49-77.*
43. **NATO documents**
44. *Bucharest Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest, 3 April 2008. [Online] (Updated 8 May 2014). Available at: http://www.nato.int/cps/en/natolive/official_texts_8443.htm [Accessed 3 July 2015].*
45. *Chicago Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago, 20 May 2012. [Online] (Updated 1 August 2012). Available at: http://www.nato.int/cps/en/natohq/official_texts_87593.htm?mode=pressrelease [Accessed 3 July 2015].*
46. *Lisbon Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 20 November 2010. [Online] (Updated 31 July 2012). Available at:*
47. *http://www.nato.int/cps/en/natolive/official_texts_68828.htm [Accessed 3 July 2015].*
48. *North Atlantic Treaty. Washington D.C., 4 April 1949. [Online] (Updated 9 December 2008). Available at: http://www.nato.int/cps/en/natolive/official_texts_17120.htm [Accessed 5 November 2014].*
49. *Prague Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, 21 November 2002. [Online] (Updated 18 January 2008). Available at: http://www.nato.int/docu/pr/2002/p02-127e.htm [Accessed 3 July 2015].*
50. *Riga Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga, 29 November 2006. [Online] (Updated 27 February 2009). Available at: http://www.nato.int/docu/pr/2006/p06-150e.htm [Accessed 3 July 2015].*
51. *Strategic Concept: Active Engagement, Modern Defence. Adopted by the Heads of State and Government at the NATO Summit in Lisbon, 19-20 November 2010. Available at: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf [Accessed 2 November 2014].*
52. *The Alliance's Strategic Concept. Adopted by the Heads of State and Government at the NATO Summit in Washington, 24 April 1999. [Online] (Updated 25 June 2009). Available at: http://www.nato.int/cps/en/natolive/official_texts_27433.htm [Accessed 3 July 2015].*
53. *Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5 September 2014. [Online] (Updated 29 September 2014). Available at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm [Accessed 2 November 2014].*