NATO Road to Cybersecurity

Wiesław Goździewicz, Mateusz Krupczyński,
Joanna Kulesza, Miron Lakomy, Michał Matyasik,
Kate Miller, Tomasz Romanowski, Ryszard Szpyra,
Magdalena Szwiec, Joanna Świątkowska
Editor: Joanna Świątkowska

The Kosciuszko Institute

NATO Road to Cybersecurity

Wiesław Goździewicz, Mateusz Krupczyński, Joanna Kulesza,
Miron Lakomy, Michał Matyasik, Kate Miller, Tomasz Romanowski,
Ryszard Szpyra, Magdalena Szwiec, Joanna Świątkowska

Editor: Joanna Świątkowska

The Kosciuszko Institute

If you appreciate the value of the presented Report as well as The Kosciuszko Institute's mission, we kindly encourage you to support our future publishing initiatives by making a financial contribution to the association.

NATO Road to Cybersecurity

Wiesław Goździewicz, Mateusz Krupczyński, Joanna Kulesza, Miron Lakomy, Michał Matyasik, Kate Miller, Tomasz Romanowski, Ryszard Szpyra, Magdalena Szwiec, Joanna Świątkowska

Editor: Joanna Świątkowska

Proofreading: Justyna Kruk
Cover design, layout and typesetting: Małgorzata Kopecka

The Kosciuszko Institute
Ul. Feldmana 4/9-10
31-130 Kraków, Poland
e-mail: ik@ik.org.pl
Telephone: +48 126329724
ww.ik.org.pl
ISBN 978-83-63712-29-7

Contents

The views expressed in this publication are those of the authors and do not necessarily reflect any views held by the Kosciuszko Institute and the publication partners. They are published as a contribution to public debate. Authors are responsible for their own opinions and contributions and the authors do not necessarily support all of the opinions made by others in the report.

NATO's Road to Cybersecurity – towards bold decisions and decisive actions

Joanna Świątkowska, Ph.D.
Programme Director of the European Cybersecurity Forum,
Senior Research Fellow
The Kosciuszko Institute

When it comes to cybersecurity, the North Atlantic Alliance has come a long way. It can broadly be divided into three stages: the first one was when cybersecurity was treated more as a technical challenge which was supposed to be faced separately by the Atlantic Alliance and its institutions in relation to the ICT infrastructure used by NATO, and separately by the Member States with regard to their national ICT networks; the second one was when the topic became an important political issue (the process was primarily initiated during the Riga Summit and subsequently stepped-up following the cyberattacks against Estonia); and finally the third one when NATO declared cybersecurity to be a strategic challenge, requiring a coordinated response on the part of the entire Alliance and all Member States, perhaps even under Article 5 of the Washington Treaty (conclusions of the Wales Summit). NATO's journey towards cybersecurity has not come to an end yet; on the contrary, it will take a lot of effort and further bold decisions to move closer towards achieving the goal.

The NATO Summit in Warsaw has a chance to become the next important stage in the process. We have already heard announcements that NATO will recognise cyberspace as an operational domain, next to land, sea, and air. In conjunction with the conclusions of the Wales Summit where the possibility to invoke Article 5 of the North Atlantic Treaty in the event of a cyberattack was confirmed, it becomes clear that the Alliance recognises the strategic importance of challenges of contemporary cyberspace.

These are indeed important steps towards enhanced cybersecurity; however, a real breakthrough requires even bolder decisions to be made.

In this report, the Kosciuszko Institute invited authors to take up the most pressing cybersecurity challenges facing the Alliance. The NATO Summit in Warsaw should begin the discussion about these key areas. Everything indicates that in the coming years, the discussions on the direction of the Alliance's involvement in cyber operations will be dominated by two issues.

The first one concerns the need for the Alliance to specify exactly the activities carried out in the framework of collective defence and the development of NATO's capabilities, also offensive, to operate in cyberspace.

The second one, which is frequently brought up in the discussion about the cybersecurity of the Alliance, is the need for comprehensive measures to be implemented to counter hybrid threats, including the multi-dimensional use of cyberspace as one of the most critical elements.

Considering the first issue, one of the most important recommendations made in this report is to demand that a serious debate about the Alliance's capability to use offensive cyber weapons is started. While this way of thinking is a natural consequence of recognising cyberspace as another domain of warfare, it also increases the number of options for launching operations in the framework of collective defence. It is necessary to bear in mind that activities carried out in cyberspace, including offensive operations, may be far more humane and often more commensurate than conventional actions. This means that a conventional (kinetic) response to cyber operations would not always be adequate. Therefore, offensive operations are the key to the future – from the point of view of both deterrence and defence.

Considering the role and importance of cyber operations, we put forward very specific solutions, namely the establishment of a Cyber Component Command or a Cyber Planning Group.

Taking into account the fact that since activities below the threshold of war and taking the form of hybrid threats will be increasingly used by opponents of the Alliance, the report devotes much space to this issue. Cyber operations perfectly fit the hybrid warfare strategy: they exploit the capacity to carry out actions aiming to destabilise, misinform, and destroy and at the same time evade responsibility for them. It appears that the use of ambiguity is particularly easy in cyberspace and thus "attractive" for aggressors.

Our main message is that the Alliance must not only adapt its operational strategy to these new challenges, but also establish strong cooperation arrangements with partners, especially with the European Union, to effectively combat hybrid threats. The nature of hybrid threats combines military and non-military activity. Combining the efforts of the military organisation such as NATO with the political and economic organisation such as the EU is necessary to effectively face this brand new challenge.

The authors have adopted a comprehensive perspective to deliberate on the cybersecurity of the Alliance. Among other things, they carried out an analysis of the legal and practical aspects of offensive actions in cyberspace. Drawing upon specific examples of exploiting cyberspace in hybrid conflicts, they indicated possible means to prepare the Alliance for countering these threats. Finally, they proposed that new areas of cooperation with various actors should be explored, including the private sector and other public organizations.

The report starts with the analysis of the Alliance's hitherto engagement in cyber operations carried out by Commander Wiesław Goździewicz. At this point the entire team would like to express their wholehearted thanks the Commander who in addition to authoring the analysis offered inestimable help and advice when working on the substantive content of the entire report.

The report concludes with a set of key recommendations that we hope will prove useful for shaping future decisions considering NATO's engagement in cyber operations. Our recommendations are far-reaching and bold – exactly as NATO's activities should be in this area.

Recommendations for NATO

The following recommendations are based upon the key theses propounded in the articles included in this report as well as discussions that took place during the European Cybersecurity Forum – CYBERSEC 2015.

1. In order to build effective NATO capabilities, Member Nations must first enhance their own capabilities, both defensive and offensive. According to Article 3 of the Washington Treaty, the member countries are obliged to build their own cyber capabilities, as reiterated in the Wales Summit Declaration. Strong nations constitute strong NATO.

2. The member states should urge for the signing of the Second Generation Memoranda of Understanding on cyberdefence in line with the 2014 Enhanced NATO Policy on Cyber Defence.

3. It must be emphasised that offensive capabilities can serve defensive and deterrent purposes. Currently, in accordance with the Enhanced Cyber Defence Policy, NATO does not allow for offensive cyber actions to be taken and offensive cyber capabilities to be developed. Therefore, the decision whether offensive cyber capabilities can be developed has to be discussed and made at a national level. However, it is strongly recommended that a bold and decisive discussion begins about the possible use of offensive cybercapabilities by NATO.

4. In addition to planning, the Alliance needs to consider its offensive cyber capabilities in this area. Therefore, it is recommended that a Cyber Planning Group is established.

5. NATO should consider creating Cyber Component Command aside from the existing Land, Air, Maritime and Special Operations Component Commands.

6. NATO Specialised Cyber Defence Force should be built and trained in a manner similar to NATO Response Force.

7. More funding needs to be allocated to cybersecurity. One of the solutions is to apply a rule known from the area of conventional security (chosen percentage of GDP spent on security – in this case cybersecurity).

8. In order to effectively operate in cyberspace, NATO requires forces and personnel that are trained to the highest standard, ready, and equipped with best-in-class technical capabilities. This requires a sustained effort in the frame of which NATO members should man, train, and equip its forces and personnel over the next years.

9. A practical and accurate definition of a cyber armed attack is needed.

10. There is a pressing need for NATO's clear position on state responsibility for cyberattacks originated by non-state actors.

11. The principle of Article 5 of the Washington Treaty should not be used to respond to cyberattacks targeting less vital, second-tier targets within a member state's digital domain, such as websites, e-mail servers, or even government databases. On the contrary, only the most serious incursions that are successful in crippling critical infrastructure and/or military capabilities should be perceived as a sufficient condition for triggering NATO's collective cyberdefence mechanism.

12. NATO and its member states should focus their efforts on the development of cyber reconnaissance and intelligence structures, which would possess enough technical and political expertise to track down actors responsible for cyber incursions.
    Such a system should combine CYBINT (cyber intelligence, especially techniques of cyberattack attribution), HUMINT ("conventional" human intelligence), SIGINT (signals intelligence, e.g. satellite images), OSINT (open source intelligence), as well as political analysis.

13. Information campaigns should constitute the core objective for every NATO operation. They should definitely be more oriented towards cyber sphere since it provides the most effective and the fastest means of communication. Such campaigns should be designed together by military and civilian structures of NATO. Due to rapidly changing environment in information sphere NATO should develop a dynamic 24/7 coordination procedure for information campaigns, especially in the cyber domain. Optionally, such a procedure could be founded on the Military Staff Committee Operation Division supported by the analytic capabilities of the scientific community and the NATO Cooperation Cyber Defence Centre of Excellence or the NATO Strategic Communication Centre of Excellence.

14. The Alliance needs to strengthen its multi-disciplinary approach to cybersecurity education by supporting inter-university collaboration, building a network of internships, involving "cyber veterans", and fostering cooperation with the EU. By supporting these initiatives, NATO would become a direct beneficiary of exceptional capabilities developed by potential future leaders.

15. Close cooperation between NATO and the EU is essential for the effective countering of multi-dimensional hybrid threats.
    - In order to increase awareness, this cooperation should aim at:
      a. Building effective platform for intelligence sharing and engaging NATO's experts in the EU process of creating indicators and characteristics of hybrid threats.
      b. Developing joint, strategic communication (also conducted in cyberspace).

    - In order to build resistance, this cooperation should:
      a. Strengthen the cybersecurity of critical infrastructure of EU member states and NATO.
      b. Harmonize EU and NATO initiatives aimed at developing public-private cooperation in the field of cybersecurity.

16. In order to counter and respond to crisis situations as well as to overcome their effects:
    The EU and NATO should develop and practise joint response scenarios to respond to potential hybrid threats, with special emphasis put on actions undertaken in cyberspace. These actions should draw upon the DIMEL model which presupposes that achieving specific goals requires all available instruments and resources (D – diplomatic, I – Information, M – military, E – Economic, L – Legal) to be used.

From Riga to Wales. NATO's Road to Collective Cyberdefence

CDR Wiesław Goździewicz, Legal Advisor
NATO Joint Force Training Centre

Cyberspace is nowadays considered one of the global commons, offering its users great advantages in political, military, economic, social and information domains. At the same time, however, cyberspace can be the source of threats non-existent in other environments. For almost a decade now, the North Atlantic Treaty Organisation (NATO) has analysed the threats emanating from cyberspace as well as security challenges brought by the geometric growth of the Internet traffic and technological developments related to the use of the World-Wide Web and other computer networks and computer systems. Let us examine how NATO's approach to cyberthreats and cyberdefence has changed over the years.

Although first reference to cyberattacks was made in the 2002 Prague Summit Declaration,[1] one might say that first steps towards collective cyberdefence were made during the Riga Summit in 2006. Measures aimed at countering the cyberthreat, among other efforts meant to prepare the Alliance for contemporary challenges, were mentioned in Paragraph 24 of the Riga Summit Declaration.[2] The aim described in the Riga Summit Declaration was to create a reliable information network capability, allowing a secure and timely exchange of data, information and intelligence, especially in support of Allied operations. At the same time, the Member Nations strived to improve the protection of NATO's key information systems against cyberattacks.

As a result of the Riga Summit, NATO approved its first cyberdefence policy in January 2008, following the cyberattacks against Estonia. From that moment on, the Alliance has been devoting more and more attention to the issues of cyberdefence. Paragraph 47 of the Bucharest Summit Declaration[3] reaffirmed the Alliance's commitment to strengthening the defence of NATO's key information systems against cyberattacks and building structures and authorities responsible for the implementation of the Cyber Defence Policy. The need for both NATO and the Member Nations to protect information systems was stressed. NATO committed itself to assist Allies in countering cyberattacks and to develop NATO's cyberdefence capabilities in close cooperation with the national authorities of the Member Nations.

1 http://www.nato.int/docu/pr/2002/p02-127e.htm (access: 01.11.2015).
2 http://www.nato.int/docu/pr/2006/p06-150e.htm (access: 01.11.2015).
3 http://www.nato.int/cps/en/natolive/official_texts_8443.htm (access: 01.11.2015).

The Lisbon Summit in 2010 was a true milestone in NATO's cyberdefence capacity building. In the Declaration,[4] the Nations declared to *"(…)take into account the cyber dimension of modern conflicts in NATO's doctrine(…)"* and *"(…)to accelerate NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012 and the bringing of all NATO bodies under centralised cyber protection."* In addition, the Nations committed to utilise the operations planning process *"(…)to promote the development of Allies' cyber defence capabilities, to assist individual Allies upon request and to optimise information sharing, collaboration and interoperability."* The requirement for cooperation with international organisations, such as the UN and the EU was stressed, and a commitment to implement a revised in-depth cyberdefence policy was made.

It was recognised that cyberattacks, becoming more frequent and better organised, could inflict costly damage on government administrations, businesses, economies and potentially also on transportation and supply networks as well as other critical infrastructures, reaching a threshold that could threaten national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups were listed as possible sources of such attacks.[5] Due to the growing dependence of countries on vital global trade routes and international economic exchange, both in the "real world" and in cyberspace, it was indicated that certain significant technology-related trends would have a major global influence on NATO's military planning and operations.[6]

Following Lisbon Summit, in 2011 NATO adopted the Cyber Defence Concept, Policy, and Action Plan. As a result of the NATO Command Structure and Agencies' reform, NATO's centralised cyber protection was assigned to the NATO Communications and Information Agency (NCIA), with the NATO Computer Incidents Response Capability (NCIRC) becoming part of the NCIA. Paragraph 49[7] of the Chicago Summit Declaration reaffirmed the cyberdefence commitments made at the Lisbon Summit. The goal of making the NCIRC fully operationally capable (FOC) by the end of 2012, including *"(…)protection of most sites and users(…)"*, was set. NATO committed itself to bringing all its entities under centralised cyber protection. The Alliance confirmed the individual and collective commitment to identify and deliver *"(…)national cyber defence capabilities that strengthen Alliance collaboration and interoperability, including through NATO defence planning processes."* as well as *"(…)to engage with relevant partner nations on a case-by-case basis and with international organisations, inter alia the EU, as agreed, the Council of Europe, the UN and the OSCE(…)."* The expertise offered by the Cooperative Cyber Defence Centre of Excellence (CCD COE) was highlighted.

The Wales Summit Declaration[8] was a major step forward in acknowledging the challenges posed by complex cyberattacks. It was the first official document in which the Member Nations of the Alliance confirmed the possibility of a cyberattack to cross the threshold of an armed attack and thus become the basis for invoking Article 5 of the North Atlantic Treaty. It was reiterated that cyberthreats and attacks would continue to become more common, sophisticated, and potentially damaging. In Paragraph 72, the Alliance Nations declared that:

> "Cyberattacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."

This clearly demonstrates the Alliance's view whereby cyberattacks can cross the threshold of an armed attack, allowing individual or collective self-defence to be invocated under both Article 51 of the UN Charterand Article 5 of the North Atlantic Treaty. Moreover, for the first time since NATO took on the topic of cyberdefence in 2006, it was explicitly stated that cyberdefence became part of the Alliance's collective defence tasks and efforts.

The Member Nations adopted the Enhanced Cyber Defence Policy (ECDP) which reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence and clearly states that *"(…)the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks."* The ECDP recognises the applicability of international law to cyber operations, including the International Humanitarian Law (IHL) or the Law of Armed Conflict (LOAC).

The Nations committed themselves to further develop their national cyberdefence capabilities and enhance the cybersecurity of their networks, upon which the Alliance depends. NATO's top priority for cyberdefence is the protection of NATO-owned communications and information systems (CIS); however, the Alliance will assist the Nations in defending their national networks considered critical for NATO's missions. For this purpose, the Alliance cooperates with national authorities to ensure an appropriate level of cyberdefence of national CIS. Such cooperation is being formalised in Memoranda of Understanding (MOUs) signed between the Cyber Defence Management Board and the respective nations. Cyberdefence MOUs are based upon a template developed in the Cyber Defence Action Plan in line with the principles of the ECDP. They set the foundations for mutual support in the area of cyberdefence, including information sharing, participation in training and exercises as well as the provision of reciprocal assistance in the form of intelligence and "manpower" (CIS specialists and cyberdefence experts). The Czech Republic was the first NATO Nation to sign such a MOU on 12 October 2015.[9] Assistance to Allies may be provided by one of the Rapid Reaction Teams formed by the NCIA as part of the Alliance's collective cyberdefence capability.[10]

4 http://www.nato.int/cps/en/natolive/official_texts_68828.htm#cyber (access: 01.11.2015).

5 *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010*, http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (access: 02.11.2015), p. 11.

6 *Ibidem*, p. 12.

7 http://www.nato.int/cps/en/natolive/official_texts_87593.htm#cyber (access: 02.11.2015).

8 *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, http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease (access: 30.11.2015).

9 *NATO and Czech Republic bolster cyber defence cooperation*, 2015, http://www.nato.int/cps/en/natohq/news_123857.htm (access: 02.11.2015).

10 *Men in black – NATO's cybermen*, 2015, http://www.nato.int/cps/en/natohq/news_118855.htm (access: 02.11.2015).

The Wales Summit Declaration further provided for a continued integration of cyberdefence into NATO operations and operational and contingency planning, as well as the enhancement of information sharing and situational awareness among Allies. The key role of partnerships in addressing cyberthreats was stressed.

Also the ECDP requires NATO to include cyberdefence aspects in the defence planning process. This has been achieved by implementing respective cyberdefence annexes in Operations Plans (OPLANs) developed for real-life operations, training and exercises as well as contingency plans. The training and exercise programme has grown to include cyber-specific exercises such as Cyber Coalition and Locked Shields. In addition, an extensive cyberdefence play has been incorporated into more "classic" training and exercises, including the biggest NATO exercise over the last decade – Trident Juncture 15 and Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX), to which the Joint Force Training Centre has been the proud host for the last five years.[11]

One of the most important aspects of the NATO ECDP is cooperation in broad terms: with NATO Nations (as described above), Partner Nations, international actors such as the UN and the EU, industry and academia. Cooperation with industry has been formalised in the NATO Industry Cyber Partnership (NICP), which was founded and endorsed by the Alliance based upon the conclusion that NATO and industry faced shared risks in cyberspace, and that addressing these challenges required new frameworks for action. Within the NICP framework, the NCIA has launched the cybersecurity incubator concept tasked to develop a new model for NATO-industry cooperation with the aim to decrease the time required for NATO to develop its cyber response capabilities, based upon the results of research and development programmes already run by industry and academia.

There are many other cooperation frameworks such as the Cyber Information and Incident Coordination System (CIIS), a web-based application developed for sharing cyberdefence information within a trusted community and available to all NATO Nations and Partner Nations as well as commercial organizations.

NATO does not develop offensive cyber capabilities. Although the Alliance focuses on defence against cyberattacks, it does not preclude particular Member Nations from developing their own national offensive cyber capabilities. In fact, there are nations who openly admit they pursue such capabilities involving *"(…)countering (disorganising, jamming and destroying) the sources of threats (active defence and offensive actions) (…)"*.[12] As a matter of fact, NATO Rules of Engagement[13] in Series 36 (Information Operations) envisage the possibility of conducting offensive computer network operations (namely Computer Network Attacks – CNAs); however, none of these offensive ROEs have been authorised so far by the North Atlantic Council in operations or exercises.

11 Schiller F., *CWIX – Achieving Federated Interoperability – NOW*, 2015, http://www.jftc.nato.int/news-archive/news/news-stories/cwix-achieving-federated-interoperability-now, (access: 02.11.2015); Kubiczek R., CWIX Jubilee, 2015, http://www.jftc.nato.int/news-archive/news/news-stories/cwix-jubilee (access: 02.11.2015).

12 *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej (Cybersecurity Doctrine of the Republic of Poland)*, Biuro Bezpieczeństwa Narodowego, 22 January 2015, ISBN: 978-83-60846-25-4, p. 9.

13 MC 362/1, *NATO Rules of Engagement*, June 2003.

This short text hopefully illustrates how NATO's approach to cyberdefence has evolved over the last decade to culminate in a clear and unambiguous declaration that cyberattacks can trigger the invocation of Article 5. While the Alliance is committed to assist Allies in their defence efforts, it encourages the Member Nations to develop their own cyberdefence capabilities in the spirit of Article 3 of the North Atlantic Treaty. This evolutionary approach should be continued to ensure the adaptation of the Alliance's cyberdefence policy to new trends in cyber operations, including the development of response options to e.g.:

1) cyber actions amounting to armed attacks;
2) the possibility of a broader application of cyber means and methods of warfare in future conflicts;
3) terrorist acts with the use of cyber means.

Adaptability and flexibility as well as a broad range of response options are a must in the world where the vulnerabilities of critical infrastructure are no secret and neither is the reliance of countries on critical infrastructure which in many cases is shared between two or more countries.

Pre-emptive Cyberattacks in International Law[1]

Joanna Kulesza, Ph.D.
University of Lodz
Expert of the Kosciuszko Institute

In the third quarter of 2015, DDoS attacks on the Internet infrastructure layer nearly doubled when compared with the respective period of 2014.[2] The EU alone suffers losses of roughly 300 billion Euros a year due to attacks on electronic resources located within its member states. With new cyber superweapons such as Stuxnet or Flame and their destructive effects on most vulnerable physical infrastructure, the once purely fictional doomsday scenarios for the collapse of civilisation caused by a machine malfunction seem more plausible. It has now been over a decade since states first started pondering upon appropriate responses to online attacks resulting in serious offline threats to national security or sovereignty. While initial state reactions to cyberthreats referred to traditional notions of armed aggression, with major powers such as the U.S., China and Russia, declaring their capability to engage kinetic responses to cyberthreats, time has moderated the debate and despite the increasing gravity of attacks, no traditional military action against locations hosting or individuals originating them has yet been launched. This is not only due to the technical difficulties in identifying the physical location of the attackers, the hardware they use and the infrastructure they rely on, but also due to the difficulties in attributing a cyberattack to a given state. It is rather the effect of an enhanced international debate on cyberthreats, cyberattacks, and cyberwarfare, resulting in the general consensus on the need to find new ways of solving old conflicts that have found a new reflection in the unique online environment.

As one of the first forums to put cybersecurity on international agenda, NATO has been leading this dialogue since 2002. Its most recent document, the 2014 Wales Summit Declaration, reaffirms the Organization's commitment to cybersecurity with e.g. the adoption of the Defence Planning Package, putting cyberdefence on equal footing with air operations, intelligence, surveillance, and reconnaissance. The Enhanced Cyber Defence Policy reaffirms the indivisibility of members' security and prevention but, more significantly, recognizes international law, including international humanitarian law and the United Nations Charter (UNC), as applicable to cyberspace. Furthermore, it is the NATO-sponsored Tallinn Manual and its expected 2016 second edition (Tallinn Mannual 2.0) that are broadly considered a fundamental reference

1 The author would like to thank Polish Navy Commander Wiesław Goździewicz, the JFTC Legal Advisor, for his insightful and helpful comments on an earlier draft of this paper.

2 Akamai's state of the internet report, 2015, (access: www.stateoftheinternet.com).

for the interpretation of international law in the context of new and emerging cyberthreats.[3] However, despite this tremendous progress in the international debate on cybersecurity in general and legal qualification of cyberattacks in particular, this area of international relations is far from being uncontroversial. This paper is a modest attempt to tackle one of the most contentious issues of international cybersecurity and allowed self-defence against "cyberattacks" – the question of admissibility of pre-emptive cyberattacks.

Defining a cyberattack

While the issue of a legal definition might seem purely academic and thus obsolete, it nevertheless holds much practical value. Only when the scope of a term has been determined can any state action be assessed for its legality, i.e. set against appropriate norms. Online generated threats to national security and stability have been referred to with a variety of terms: cyberattacks, cybercrime, cyberthreats, cyberwarfare, or information warfare. This undesired variety of terminology adds to the confusion on the appropriate legal qualification of online generated threats.

The NATO Enhanced Cyber Defence Policy clearly indicates that not all online threats are to be treated equally and only some "cyberattacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability".[4] It pinpoints the existing scholarly controversy and political differences on the very definition of a "cyberattack", when emphasizing that "a decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis".[5] This clearly shows that despite the through discussion on the definition ofa cyberattack as well as the key neighbouring terms such as the "use of force" or an "armed attack", no practical consensus on the legal qualification of cyberattacks has yet been found.

Fundamental for the NATO legal analysis behind a prospective joint armed response to cyberattacks, the Tallinn Manual offers a thorough summary of the last decade in academic writing and political debates on the issue. Reflecting the status quo of the debate, it tends to emphasize controversies rather than provide specific and undisputed guidance. It is also the case with the key definitions which reflect the existing political controversies rather than offer reliable help.

A cyberattack is defined 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".[6]

While the Tallinn Manual provides much background on the scope of attacked "objects" and "persons", it fails to indicate what the notion of a "reasonably expected" injury implies. When is an injury to be "expected" in this unique context? As some rightfully point out, not only it is difficult to recognize an already unfolding attack, it is usually impossible to foresee it, not to mention assessing the injury it might cause? With this in mind, what are the "reasonable" criteria to apply when "expecting" the threat? Who should be able to "reasonably expect" the damage and based on what standards? Is it only the attacker who can assess the potential damage as it is him who intended the damage? In practice, even an individual conducting the operation can rarely precisely indicate its scope. Or is it rather the unsuspecting victim who may not only be technically unable to foresee the attack and its consequences, but also incapable of realizing he is being attacked? Finally, is it possibly the North Atlantic Council who measures the foreseeability of the damage when deciding on the character of an individual, ongoing or planned, cyber operation on a case-by-case basis?[7]

Answers to these questions will hopefully be provided in the upcoming Tallinn Manual 2.0, covering e.g. the practical issues of setting a "state of the art" standard of awareness and resilience in the cyber domain, and introducing possible platforms for exchanging good practice among the states so that they can "reasonably expect" certain damage caused by a cyberattack. This notion, however, seems to particularly refer to "pre-emptive measures" and "due diligence", both terms thoroughly discussed in the international law doctrine and practice as concerning the assessment of potential damage generated by a given activity. In this context, it is worth noting that a "cybersecurity due diligence" has been identified as an "emerging norm" of state responsibility for omissions in the 2011 US International Strategy for Cyberspace.[8] The key notion of due diligence in international law in general and in the context of cybersecurity in particular seems to be a crucial element missing from the discussion on the Tallinn Manual's definition of a cyberattack.[9]

Another element that seems to be missing from the definition of a cyberattack is the reference to "critical infrastructure". When speaking of international cybersecurity, other international organizations, including, but not limited to, the EU, describe "critical infrastructure" as installations and networks the security of which should be granted with particular care. While this definition is not free from controversy, a reference to this category of "objects", particularly vulnerable to "damage or destruction" in the context of the NATO dialogue, is needed. While the term "critical infrastructure" appears in the Tallinn Manual on several occasions, it clearly fails to define criteria for qualifying the scale or the gravity of a cyberattack. Nevertheless, using critical infrastructure as a criterion for identifying an operation as a use of force or an armed attack might prove useful in the context of the ongoing international debate and should be considered.

Other pressing issues, arising from the ambiguous definition of a cyberattack, are closely related to the concepts of an "armed attack" and the "use of force" in general, and are discussed below.

3 Tallinn Manual on the International Law Applicable to Cyber Warfare, M.N. Schmitt (ed.), Cambridge 2013.

4 NATO Enhanced Cyber Defence Policy, available June 28th, 2016 at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

5 Ibidem.

6 Tallinn Manual, p. 106.

7 Some guidance on this issue has been provided by academia, including M.N. Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, International Law Studies, Vol. 87/2011.

8 The White House, US International Strategy for Cyberspace, 2011, p. 10.

9 For a detailed discussion on this issue see e.g.: Kulesza J., *Due Diligence in Cyberspace* [in:] *Organizational, Legal, and Technological Dimensions of Information System Administration*, I. M. Portela, F. Almeida, IGI Global: Hershey PA 2014, p. 76–95.

Cyberattack as a use of force

Following legal scholars and national authorities, the Tallinn Manual refers to the well-recognized terms of "armed attack" and "use of force" when setting the line for justified self-defence or possible pre-emptive measures in the cyber domain. This reference needs to be discussed in the light of well-known arguments on the nature of international aggression.

The NATO definition of the "use of force", as presented in the context of cybersecurity in the Tallinn Manual, follows undisputed principles of international law and, reiterated, confirms that mere acts of economic or political coercion should not be recognized as the use of force justifying self-defence, even if those coercive measures result in a threat to territorial integrity and political independence.[10] This old argument was decided among states back in 1970s when the questions of the U.S. blocking bank accounts of foreign governments was on the agenda of the United Nations General Assembly. However, it did gain a new dimension with e.g. the 2007 Estonia cyberattacks which caused no physical damage, but significantly disrupted the operation of the Estonian community for several days, resulting in economic losses and political unrest. Involving world's leading powers such as the U.S. or China, the ongoing economic and political cyber espionage also bears no traits of physical damage, yet it brings significant economic losses. In view of this fact, but also in the light of the standpoint of the states regarding this form of cyberattacks, these well-recognized limits of the notion of aggression should be carefully verified, confirmed, or modified.

More controversially, the Tallinn experts follow the ICJ in its Nicaraguan *contras* decision to recognize that the mere acts of financing harmful activities, including those initiated online, do not amount to a use of force. However, when the funding takes on the form of providing organized groups with malware and training necessary to use during cyberattacks against another state, this kind of assistance may be tantamount to the use of force. Simultaneously, a majority of the experts opted against qualifying the crucial cases of states offering "safe haven" for the cyberattackers as equivalent to a use of force, regardless of the size of damage caused by the deployed malware. This last argument might be seen as valid insofar as attribution of an attack originated by private individuals to a state requires detailed evidence indicating that those individuals acted under the state's authority and that the state has provided them with suitable instructions. However, this reasoning as a whole seems inconsequent as it might be interpretedas encouraging the harbouring and financing of non-state actors performing cyberattacks as long as no direct transfer of software or know-how can be proven to the state. This threat does not seem well deterred with the ambiguous statement on "the provision of sanctuary coupled with other acts (…), could, in certain circumstances, be a use of force."[11]

The experts' testimony lacks, therefore, a clear stance on the legal consequence of states harbouring cyberattackers, vaguely summarizing their status as "controversial".[12] The position referred to in the Tallinn Manual remains undecided, with the majority of the Expert Group recognizing non-state actions amounting to an armed attack as grounds for state self-defence while at the same time counter weighing the ICJ's reluctance to follow this interpretation of Article 51 of the UNC.[13] In effect, a clear NATO's stance on the legal qualification of cyberattacks originated by non-state actors would be highly desired as the current lack of precise criteria leaves too much room for legal uncertainty. Also the questions on state responsibility for non-state actors or their groups originating cyberattacks remain unanswered in the current NATO dialogue.[14] This lack of conclusive interpretations on international law theory and practice is particularly surprising in the context of the ongoing heated debate on international responsibility of states harbouring terrorists. While the law of war does not directly cover the question of international terrorism, the rapid evolution of asymmetric threats, especially in the context of the cyber domain, gives rise to the need for well-justified and objective answers to questions on state responsibility for actions performed bynon-state actors. Those have not yet been answered for the purpose of NATO's operation in the cyber domain.

This analysis, which examines the legal nature of states harbouring individuals performing cyberattacks, is crucial to the question of international prevention of cyberthreats. The reason is twofold. First, states are persistently reluctant to confirm their involvement in cyberattacks, including those engaged from within their territory, and also those initiated by private individuals. Second, contemporary cyber forensics makes it considerably difficult to verifiably confirm the role of state authorities in such attacks, not only for the purposes of national military authorities considering countermeasures, but also for possible future international court proceedings, attributing cyberattacks to a responsible state. The narrow approach taken on in the Tallinn Manual, as reflective of the current state of international law, necessarily limits the applicability of the law of armed conflict and state responsibility to rare cases when a cyberattack can indeed be attributed to state authorities while at the same time disregarding the role of states "harbouring" cyberattackers. It is, however, the latter scenario that appears in the vast majority of contemporary cyberattacks: states deny any involvement in cyber operations, even when they are initiated using infrastructure located within their territory.

The brief reference in the Tallinn Manual to a state failing "to police its territory in order to prevent the launch of cyber operations" as not amounting to a use of force only deepens this undesired legal uncertainty as it fails to address the applicability of the law on state responsibility to cyberattacks originated by non-state actors. With the Tallinn experts highlighting the undesired vagueness of the issue of due diligence, it is therefore to be expected that NATO will indeed deal with the question of state responsibility for the breach of its international obligations by internationally harmful omissions in the context of international cyberattacks. In these circumstances, a reference to e.g. the body of work on international environmental law or the protection of aliens would allow the criteria of cyberthreats prevention applicable to all NATO member states to be identified.

10 Tallinn Manual, p. 46.
11 Tallinn Manual, p. 47.
12 Tallinn Manual, p. 58.
13 Tallinn Manual, p. 59.
14 Tallinn Manual, p. 59.

Cyberattack as an armed attack and the right to self-defence

Under Article 2(4) of the United Nations Charter (UNC) and Article 1 of the North Atlantic Treaty (NAT), any "use of force" is prohibited and may be considered a breach ofan international obligation of states. However, according to Article 51 UNC and Article 5 NAT, it is only when the "use of force" amounts to an armed attack the right to armed self-defence is triggered.[15] Therefore, those two terms are not synonymous in meaning and scope. The line between the "use of force" and an "armed attack" has always been blurred in international legal scholarship and the dispute surrounding this ambiguity is well reflected in the domain of cybersecurity.[16]

As per Rule 13 of the Tallinn Manual, qualifying a cyber operation as an armed attack directly depends on the factual circumstances of the case, in particular on the "scale and effects" of a given "operation".[17] Here again the Tallinn experts rely on the ICJ Nicaragua case decision with regard to the key criterion of "scale and effects" of the use of force amounting to an armed attack, confirming a case specific assessment of a given cyber threat.[18] What is more, the experts refer to the general opinion of the international community as one of the criteria states need to rely upon when verifying whether they have fallen victim to a cyber armed attack, advising them to be "highly sensitive to the international community's probable assessment" of individual operations as constituting the use of force.[19] However, neither indications of such "sensitivity" nor verifiable ways of identifying a "probable assessment" of the "international community" as a whole are provided in the report, thus offering little help or guidance to states in practical terms.

In addition, the manual offers a novel interpretation of an "armed" attack as one which does not necessarily involve the use of weapons, but is rather quantified by its results.[20] This controversial notion may not only be subject to scholarly and political criticism, but, more significantly, it may also follow the dangerous route of broadening the exception of allowed use of force in international relations, which might be done under the guise of adapting laws to technological realities. With that in mind, the notion of an "armed attack" ought to be discussed in more detail in order to provide general guidance for NATO members on the characteristics of cyberattacks. This needs to be done in recognition of the legal principle prohibiting the broadening interpretation of exceptions to legal rules (*exceptiones sunt strictissimae interpretationis*).[21]

Should one assume, however, that a particular case of a cyber operation amounts not only to the use of force, but in its scale and gravity to an armed attack, international law allows for armed self-defence measures to be deployed. The Tallinn Manual authors agreed that until the publication of the book in 2012, no cyberattack had "unambiguously and publicly" reached the level of an armed attack as per the opinion of the "international community". There was, however, a serious doubt expressed by some of them on whether the 2010 Stuxnet worm incident and its consequences did not in fact amount to damage quantifiable of an armed attack.[22] Leaving aside the vague indication of "unambiguous and public characterization by the international community" as a criterion for identifying a cyber armed attack, the gravest thus far 2010 cyber operation, which might have reached the necessary level of seriousness, was considered as a possible case of anticipatory self-defence.[23] What this means in terms of cybersecurity and whether cyberattacks may be exercised in this context is discussed below.

Necessity, proportionality, imminence and immediacy

Any act of self-defence, when performed in accordance with international law, must meet the basic preconditions of necessity, proportionality, imminence and immediacy.[24] This means that any act of self-defence, whether individual or collective, may only be deployed when no other measure can meet its purpose, is proportionate in the scale and effect to the original attack and immediately follows an imminent attack. Therefore, the use of force in self-defence needs to be the only effective measure to repel or defeat an ongoing attack. The experts note that the criterion of "necessity" is to be verified by the attacked state.[25] This clearly goes against the instructions included elsewhere in the manual on the need to recognize the unambiguous "public" qualification of a given operation as an armed attack by the "international community".

Nevertheless, the most difficult criterion to apply to cyberattacks used in self-defence is the notion of proportionality, namely the need to use only as strong of a measure as necessary to repel the attack. While the proportionality criterion does not directly refer to using in-kind measures, the experts go as far as to approve the use of kinetic force against cyberattacks' originators "relatively invulnerable" to cyber operations.[26] However, in the discussion on self-defence against a cyber armed attack, the question of proportionality seems to be one of the most complex issues. In light of the imminent technical shortcomings of contemporary cyber forensics and the lack of trusted information exchange platforms, the scale of actual damage or scope of attack might show extremely difficult to ascertain. More guidance on what the notion of proportionality implies in the context of cyberthreats would be desired. This observation goes back to the points made above, referring to the verifiable measures of predicting an attack and measuring its results.

Cyberattacks as pre-emptive measures

More significantly, however, the Tallinn experts seem to intentionally equate self-defence operations following an armed attack with those of so-called pre-emptive self-defence, i.e.

15 Tallinn Manual p. 55.
16 For a fairly recent summary of this debate see e.g.: Tom Ruys *"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice"*, Cambridge 2010. See also: M. N. Schmitt, Classification of Cyber Conflict, 89 INT'L L.STUD.233(2013), 233-251.
17 Tallinn Manual, p. 54.
18 Tallinn Manual, p. 55.
19 Tallinn Manual, p. 48.
20 Tallinn Manual, p. 55. For the arguments on the possibility to foresee the results of a cyberattack see section 1 above.
21 This argument follows the long going debate on the character of the Article 51 exception, see e.g. Fu-Shun Lin, Self-Defence - A Permissible Use of Force under the U.N. Charter, 13 DePaul L. Rev. 43 (1963).
22 Tallinn Manual, p. 58.
23 Tallinn Manual, p. 58.
24 Tallinn Manual, p. 60.
25 Tallinn Manual, p. 62.
26 Tallinn Manual, p. 63.

one targeted against a planned attack which has not yet commenced.[27] While the right of self-defence against an armed attack remains undisputed in international law, the status of pre-emptive self-defence remains highly controversial. One might wish for NATO to discuss the question of pre-emptive cyber self-defence in more detail, with due regard to the current disaccord among international legal scholars, focused on the notion of "clear and convincing" evidence of an imminent attack, but also differing positions among state authorities, particularly those outside NATO.[28]

The notion of pre-emptive self-defence remains strongly controversial. While international law prohibits the "use of force" as well as the "threat" of it, referring to actions preceding the actual breach of Article 2 (4) UNC as equally prohibited, there is no clear reference to the "threat" of an "armed attack" as justifying armed self-defence. One might actually argue to the contrary, indicating that any permissible self-defence must follow an immediate and serious attack.

In this context, the above mentioned criteria for "clear and convincing" evidence of an imminent attack would turn out to beeven more challenging in the cyber domain than in case of kinetic threats. The questions that need to be answered focus on the verifiable techniques to identify and prove not only the planned armed attack, but also the intended scale of damage rising up to an armed attack, with the latter criteria posing significant problems of its own and discussed hereinabove. One might even go as far as to claim that given the contemporary state of cyber forensics, any peremptory cyber self-defence operation cannot be applied as there are no verifiable ways of corroboratingan imminent cyberattack with "clear and convincing" evidence.[29]

Should NATO follow the Tallinn Manual in recognizing a state's right of peremptory self-defence operations in the cyber domain, more guidance on the specific issues listed below is needed:

- What measures and means are to be considered as verifiable proof of an imminent cyberattack?
- How to ascertain the scale of damage following the attack in order to classify it as an armed attack, justifying the use of force in self-defence?

Conclusions and recommendations

While the Tallinn Manual neither represents the official stand of North Atlantic Council nor is binding for its decisions on individual cyber threats, it does provide stance on the novel area of international cybersecurity and hints at how NATO is likely to interpret any new advancements in this domain. With that in mind, it must be noted that the work provided by the members of the International Group of Experts is novel and unique on the global scale and as such serves as a solid base for further discussion. It is clear, however, that national or local interpretations of key terminology and legal principles are bound to vary not only among NATO member states, but more significantly, among those not party to the Organization.

27 Tallinn Manual, p. 60.

28 For a debate on this issue see e.g. Roscini M., *Cyber Operations and the Use of Force in International Law*, Oxford University Press, 2015, p. 80.

29 See e.g. the UK House of Commons Defence Committee, Defence and Cyber Security 6th Report, 2012, p. 24. For more reference see: Roscini M., *Cyber Operations and the Use of Force in International Law*, Oxford University Press, 2015, p. 90.

Key recommendations argued for in this policy paper indicate the following issues:

1. A practical and accurate definition of a cyber armed attack is needed.

2. There is a pressing need for NATO's clear position on state responsibility for cyberattacks originated by non-state actors.

3. There is a pressing need for a clearer definition of "reasonable expectations" of damage, conditioning the qualification of an operation as a cyberattack. This will allow the needed pre-emptive measures and a cybersecurity due diligence standard for cyberthreats prevention to be determined.

4. The issue of the proportionality of cyber countermeasures and pre-emptive self-defence needs to be further examined, with the latter focusing on verifiable and technically applicable means of evidencing the sources, origins, and prospected results of cyberattacks.

5. An enhanced engagement with other forums, such as the UN GGE, as well as the EU Digital Agenda policy is needed for the NATO work to be reflective of contemporary international law and relations.

6. A reference to "critical infrastructure" in the context of a cyberattack "reasonably expected to cause (…) damage or destruction to objects" is necessary for applying the NATO legal framework for the purpose of international cybersecurity cooperation.

Offensive Aspects of Military Cyber Activity

Professor Ryszard Szpyra
National Defence University
National Security Faculty

It is well known that the armed struggle exists because someone initiates armed attacks. Anyone who needs to defend oneself reaches out for offensive elements to increase the effectiveness of defence.

Regardless of the basic nature of the military strategy (more defensive or more offensive), it is offensive military capabilities that are widely developed. Principally, any military operation comprises at least two elementary components; the essence of each is represented by defensiveness and offensiveness. They are two sides of the same coin – warfare.

Today, thanks to the progress in the implementation of the information civilization and, above all, thanks to the development of information technology and the Internet, a new space of human activity emerged – cyberspace. In this space, all forms of human activity are developing very quickly, in the form of both cooperation and combat.

According to the *American DoD Cyber Strategy:*

> "The increased use of cyberattacks as a political instrument reflects a dangerous trend in international relations. Vulnerable data systems present state and non-state actors with an enticing opportunity to strike the United States and its interests. During a conflict, the Defense Department assumes that a potential adversary will seek to target U.S. or allied critical infrastructure and military networks to gain a strategic advantage. Beyond the attacks described above, a sophisticated actor could target an industrial control system (ICS) on a public utility to affect public safety, or enter a network to manipulate health records to affect an individual's well-being. A disruptive, manipulative, or destructive cyberattack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected."[1]

1 *The DoD Cyber Strategy*, The Department of Defense, Washington 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Moreover, "it seems that distrust among the global players and the ambitions of some to develop offensive capabilities"[2] have led to acceleration in a cyberspace arms race. According to the DoD cyber strategy, "to operate effectively in cyberspace, DoD requires forces and personnel that are trained to the highest standard, ready, and equipped with best-in-class technical capabilities."[3] This requires a sustained effort in the frame of which MoD should man, train, and equip its forces and personnel over the next years.

Over the past years in Poland, it was political correctness that stimulated discussions mainly on the defensive aspect of cyber military activity. However, the current cyber security doctrine speaks now of offensive cyber operations. Offensive cyber capabilities and skills may also be useful for strategic defence and as an element of deterrence. Additionally, offensive actions[4] can be applied to the asymmetric domain to deter hostile adversarial actions in cyberspace.

In 2012, "Iran continually demonstrated its intentions to continue enriching uranium despite the European Union and United States economic sanctions and international disapproval levied against it. Therefore if the unknown U.S. official's admission of deploying Stuxnet is true, it can be interpreted as removing any doubt over U.S. involvement in trying to impede Iran's nuclear development. Not only would it have demonstrated the United States' sophisticated capabilities in the development of advanced cyber weaponry; but it also would have shown that it could «touch» Iran's most secret nuclear development facilities any time it wanted.(…)If true, President Bush's decision to employ a cyber weapon of this caliber was commendable in the fact that he saw this as a viable non-lethal option as opposed to approving a conventional military strike."[5]

In some circumstances, in the same way as conventional attacks, a preventive cyberattack is acceptable by international law. Furthermore, it may be useful for any type of retaliation.

Thus, it is necessary to have "a range of retaliatory options to use against a range of threats (…), given the speed with which threats might change. Thus, cyberattacks should be no more tolerable than major attacks on strategic infrastructure."[6]

"By stopping even small infractions, one creates a cumulative effect that deters hostile actors from escalating to more serious behaviour."[7] It is not possible to "retaliate for every attack, but visible retaliation will manifest the risk for potential attackers, affecting their cost-benefit analysis. Those cyberspace actors contemplating attacks on"[8] NATO countries "will have to consider the potential reaction that such an attack might invite. Similarly, those who own and maintain the cyber infrastructure will have to weigh the risks of allowing

2 Even S., Siman-Tov D., *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 May 2012 INSS, Tel Aviv 2012.
3 *The DoD Cyber Strategy*. . . op. cit.
4 Iasiello E., *Cyberattack: A Dull Tool to Shape Foreign Policy*. K. Podins, J. Stinissen, M. Maybaum (Eds.), "2013 5th International Conference on Cyber Conflict Proceedings", CCDCOE Tallinn 2013, p. 453.
5 Ibidem, p. 459.
6 Sterner E., *Retaliatory Deterrence in Cyberspace*. "Strategic Studies Quarterly" Spring 2011 Vol. 5, No. 1, p. 75.
7 Ibidem.
8 Ibidem, p. 76.

their infrastructure to be used at will by various cyberspace attackers. Presumably, at least a portion of them will improve their situational awareness and be more accommodating to cyberspace defenders, lest they become retaliatory targets themselves."[9]

We "cannot adopt such a posture tomorrow or simply through declaratory statements. It will require carefully tailoredrules of engagement, careful mapping of global cyber networks to better anticipate secondary or tertiary consequences, accelerated development of advanced forensic tools, and improved retaliatory capabilities, ranging from cyber weapons and limited war plans to presidential sanction authority and international cooperation to identify cyber-attackers and the lawful means of responding to their actions. Careful study of the potential unintended consequences (also political) will be necessary. Finally, it will take a series of visible response actions – political, economic, diplomatic, military, and cyber – over time to create a reasonable, if not certain, expectation of the risk for potential attackers to face the consequences of their actions. These specific measures go well beyond the scope of this article. Moreover, developing these tools may take years, while the cyber threat is here now."[10]

Another factor stems from logical reasoning that the knowledge of the adversary's cyber offensive capabilities, strategies, weapons, and tactics helps us develop a more effective defence strategy. In such a situation, it is necessary to look for an answer to the question of how to wage offensive cyber military operations. There are many ways to conduct offensive operations in cyberspace. However, "the offensive cyber operations mission set concentrates on gaining and maintaining access to enemy areas of cyberspace without detection. The nature of offensive cyber operations requires operators to carefully plan missions"[11] in order to learn the characteristics of enemy networks to exploit them later on. "Consequently, tool development and deployment are an important aspect of this mission area.

Although offensive cyber operations operators provide a very real set of strategic alternatives to combatant commanders, the effects are specific and limited in scope"[12]; nonetheless, they may also be of informational and physical nature.

> "To exploit an adversary's system, offensive operations require detailed knowledge of the target network, which can be obtained by performing network reconnaissance with sophisticated techniques, tactics and procedures. Once operators have identified vulnerabilities, they must then develop either a technique or a weapon or select one from an existing repository prior to choosing the specific delivery mechanism. After they have accessed their target, operators establish a permanent presence on the machine while cloaking indications of the incursion, allowing them to maintain access indefinitely. Such persistent presence lets them effectively exploit information on the target in support of war fighters' objectives.

9 Ibidem.
10 Ibidem.
11 Poirier W.J., Lotspeich J., *Air Force Cyber Warfare. Now and the Future*, "Air & Space Power Journal", September–October 2013, p. 84, http://www.dtic.mil/dtic/tr/fulltext/u2/a589641.pdf.
12 Ibidem.

> In light of the long lead time necessary to perform target reconnaissance and establish persistent access, offensive operations typically require advanced planning and a lengthy time horizon to offer effective options.
>
> The weapons used by operators are similar to the ordnance that a pilot employs to carry out a given mission. Certain weapons are better for the desired purpose than others, and some work against a particular set of targets while others are ineffective against that objective.
>
> One major difference, however, is their fragility. Since defenders can block a weapon using a signature once they have detected it, use of a given technique or weapon to gain or maintain access carries a risk that the attacker will discover and counter it, rendering the technique or weapon useless for future operations. As a result, operational planners must assess the technical gain/loss associated with the employment of offensive cyber operations as they would with regard to regular weapons or weapon systems. If the desired effect is not substantial enough to justify the potential loss of an offensive cyber operation weapon, then they should consider other methods."[13]

One of the main components of armed warfare is manoeuvre. "Cyber manoeuvre most differs from its kinetic counterparts in offensive operations. While the goal of manoeuvre, to secure positional advantages in respect to an enemy or competitor state, remains relatively consistent with kinetic manoeuvre, the means to do so is vastly different given that manoeuvre is conducted at machine speeds inside a virtual construct."[14]

S. D. Applegate distinguishes between offensive and defensive cyber manoeuvre. The offensive one is composed of Exploitive Manoeuvre and Positional Manoeuvre.

> "Exploitive Manoeuvre is the process of capturing information resources in order to gain a strategic, operational or tactical competitive advantage. (…)
>
> Positional Manoeuvre is the process of capturing or compromising key physical or logical nodes in the information environment which can then be leveraged during follow-on operations. (…)
>
> Influencing Manoeuvre is the process of using cyber operations to get inside an enemy's decision cycle or even to force that decision cycle though direct or indirect actions."[15]

13 Ibidem, p. 84-85.

14 Applegate S.D., *The Principle of Maneuver in Cyber Operations*. C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) "2012 4th International Conference on Cyber Conflict" NATO CCD COE Publications, Tallinn 2012, p. 188.

15 Ibidem.

As far as the defensive form is concerned

> "to date, defensive manoeuvre in cyberspace generally resembles its kinetic counterparts. Perimeter defences, intrusion detection, and defence-in-depth is almost identical in concept whether executed in a kinetic defence or in the virtual world of cyberspace and the Deceptive Defence is somewhat akin to an ambush, luring in an attacker although for somewhat different purposes. The Moving Target Defence is unique to the cyberspace and relies on technical mechanisms that do not have a true analogy in the physical world. (…)
>
> Perimeter Defence & Defence in Depth – line Defence is the Maginot Line of cyberspace and like this historic example; it is highly susceptible to manoeuvre. (…) Defence in depth is mitigation strategy that attempts to mitigate the vulnerabilities of the line defence by hardening the interior of the network and individual systems as well. (…)
>
> The Moving Target Defence uses technical mechanisms to constantly shift certain aspects of targeted systems to make it much more difficult for an attacker to be able to identify, target and successfully attack a target. (…)
>
> Deceptive manoeuvre is the cyberspace analogy to an ambush. Deceptive manoeuvre uses processes to lure an attacker in to committing actions which will reveal their methodology or assist the defender in attribution. (…)
>
> The counter attack is another form of defensive manoeuvre, the execution of a counter attack in cyberspace is complicated by the difficulty of attribution and the fact that many attacks originate from compromised, third party systems. Taking these issues into account, counter attacks may prove necessary to restore critical operations even at the cost of disabling or damaging a compromised third party system. In situations where attribution has been established, the use of a counter attack can allow a defender to stall an attack and regain the initiative."[16]

This brings up the question of the types of weapons used in cyberattack. In the history of wars and conflicts, achieving victories only through defence was something unique. Attacking is needed to gain advantage over the enemy, even during defensive operations. A basic characteristic of a weapon is its ability to be used for both defence and attack. But what is a cyber weapon in the context of the new environment cyberspace is?

The essence of any weapon[17] lies in its capacity for destruction or incapacitation, namely its destructive or incapacitative effect it has on people, their tangible and intangible assets and

16 Ibidem, p. 190.

17 Szpyra R., *Bezpieczeństwo militarne państwa*, AON Warszawa 2012.

surroundings. In reality, this effect may be achieved only by using energy or information; that is why any weapon is a combat tool capable of energy or information destruction or incapacitation of people and the elements of their environment, producing unacceptable consequences for the opponent.

Therefore, by analogy, a cyber weapon is a cyber tool designed for combat, capable of energy or information destruction as well as causing damage to the elements of cyber infrastructure or information in cyberspace in order to produce unacceptable consequences for the opponent.

Thomas Rid and Peter McBurney define a weapon as

> "a tool that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things." And, cyber weapons are a subset of weapons, or in general terms, a "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."[18]

Developing a cyber weapon[19] for attacking industrial control systems is very simple. Because these systems are insecure by design, it requires only a small team and access to the target product. An organization that wants to attack the critical infrastructure of a potential adversary must first learn what system the adversary has. Once the vendor and product are known, the attacker must gain access to his hardware and software. This is not as difficult as it sounds. Critical infrastructure in many countries is controlled or tightly regulated by government. There is a limited number of popular systems in each infrastructure, so the chance that the adversary's system will already be owned or accessible by the offensive cyber team is very strong. Once access to the system has been established, cyberattack options available range from simple to complex. Their complexity and difficulty increase depending on how sophisticated the attack and the modification processes are.

"Reverse-engineering and analysis of malicious code used in recent sophisticated cyberattacks have revealed four common characteristics that help provide a clearer and more useful definition for a cyber weapon:

1. A campaign that may combine multiple malicious programs for espionage, data theft, or sabotage.
2. A stealth capability that enables undetected operation within the targeted system over an extended time period.
3. An attacker with apparent intimate knowledge of details for the workings of the targeted system.
4. A special type of computer code to bypass protective cybersecurity technology."[20]

18 Rid T., McBurney P., *Cyber-Weapons*. "RUSI Journal 157", no. 1, February 6-13, 2012.

19 Peterson D., *Offensive Cyber Weapons: Construction, development, and Employment*. "The Journal of Strategic Studies", 2013 Vol. 36 No. 1 120-124, http://dx.doi.org/10.1080/01402390.2012.742014.

20 Wilson C., *Cyber weapons: 4 defining characteristics*. "GCN Industry Insight", p. 1 https://gcn.com/Articles/2015/06/04/Cyber-weapon.aspx?Page=2# Jun 04, 2015.

"The next generation of cyber weapons will increasingly target and destroy physical equipment in industrial and military facilities, and the time may come when we also begin to see human casualties."[21]

Possible areas of targeting in cyber warfare originate from understanding what cyberspace is.

According to the International Telecommunications Union (ITU) of the United Nations, cyberspace is "the physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks and their computer programs, computer data, content data, traffic data, and users."[22]

This and other definitions of cyberspace imply that cyberspace comprises three layers: human, logical, and physical.

"For each of the layers (…) there are different offensive – related activities pertaining to the domain, for example:

a. Actions in cyberspace aimed at the human layer designed to change user conduct, such as transmitting informational messages (open or hidden) through cyberspace to the enemy.
b. Logical penetration (by means of software) for purposes such as espionage, attacks on enemy computers in order to withhold cyberspace benefits from the enemy, and attacks on machines and installations in the physical domains controlled from cyberspace, e.g., disrupting thermal control mechanisms that could lead to the explosion of a security plant (an effect in the land domain) or disrupting an altimeter that could lead to damage of aircraft (an effect in the air domain).
c. In the physical layer, damage to hardware that serves as the foundation for the logical layer, as well as actions outside cyberspace aimed against infrastructures on which the domain relies, e.g., firepower and electronic warfare to damage or paralyze communications components and energy systems on which cyberspace depends."[23]

All these layers are recognized as possible target areas.

Conclusions and recommendations

1. Cyberspace has become yet another battle space.

2. Every military operation is composed of two inseparable elements of attack and defence. Therefore, by analogy, both defensive and offensive cyber capabilities are necessary to conduct operations in cyberspace.

21 Ibidem, p. 2.

22 *ITU Toolkit for Cybercrime Legislation*, www.itu.int/cybersecurity.

23 Even S., Siman-Tov D., *Cyber Warfare: Concepts and Strategic Trends*. "Memorandum No. 117" May 2012 INSS, Tel Aviv 2012, p. 15-16.

3. NATO should have the capacity to respond to the full spectrum of military threats as well as threats that endanger critical infrastructure of states in cyberspace. It should also be able to adapt quickly to dynamically changing threats in cyberspace.

4. Offensive cyber capabilities and skills are useful for NATO's strategic defence and as an element of deterrence.

5. Necessary offensive cyber capabilities are inextricably associated with the need for systematic staff training supported by state-of-the-art hardware and software. This, in turn, requires a long-term systematic and planned effort.

Conditions to Invoke the Principle of Article 5 of The North Atlantic Treaty in Case of a Cyberattack or a Cyber Conflict[1]

Miron Lakomy, Ph.D.
Department of International Relations
Institute of Political Science and Journalism
University of Silesia
Expert of the Kosciuszko Institute

Cyberattacks are becoming an increasingly important challenge for contemporary international security. In contrast to the traditional theatres of war such as land, sea, and airspace, incidents in cyberspace are usually more elusive and harder to assess. It is mostly due to the specific characteristics of this unique human-made domain which allows some of the physical constraints, such as geographical boundaries, to be bypassed, granting easily achievable anonymity to the attacking side.[2] It is not surprising, therefore, that cyberspace has become an environment in which various actors such as states, terrorist organizations, criminal groups, or hacktivists pursue massive, repetitive, and harmful activities, which is manifested by millions of cyber incursions daily.[3] A majority of them are relatively simple and unsophisticated, aimed to harm individual Internet users or private sector companies, often unaware of threats emanating from the digital domain. Some incursions, however, stand out among the plethora of computer attacks, posing a significant threat to national and/or international security. Sometimes they reach a level of intensity that allows them to be denominated as "cyber conflicts." Despite the fact that these phenomena are frequently analysed by academics and various international bodies, so far no general agreement on how to perceive and categorise these incidents has been worked out within the Euro-Atlantic zone or worldwide. This is not just a purely theoretical issue since the security policy instruments must be adapted nowadays to the specific characteristics of harmful activities in cyberspace.

In recent years, this problem has become especially apparent for the North Atlantic Treaty Organization (NATO). As the world's most powerful political and military alliance, it is considered a high-value target in cyberspace. The Organization's and the member states' ICT infrastructures contain classified data and control crucial systems which could be exploited by potential adversaries to endanger Euro-Atlantic stability and security. It has already been partially proven by the *casus* of Estonia and the cyberattacks the country experienced in 2007.

1 The author would like to thank Prof. Mieczysław Stolarczyk, dr. Marek Madej, cmdr. Wiesław Goździewicz and dr. Joanna Świątkowska for comments on an earlier draft.

2 See Schreier F., *On cyberwarfare*, DCAF Horizon 2015 Working Paper, No. 7.

3 See for example: *2012 Norton Cybercrime Report*, Symantec 2012, p. 4.

This incident revealed a dire need for updating NATO's cyber security solutions in order to adapt to the new types of threats emanating from the digital domain. Wide-ranging reforms that the Alliance's decision makers pushed through as a result were crowned by the decisions taken during the Wales summit in 2014. At the conference, the Organization's leaders affirmed that cyberdefence is part of NATO's core task of collective defence, based on Article 5 of the North Atlantic Treaty (the Washington Treaty). They declared that

> "Cyberattacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."[4]

Although important and widely expected, the statement paradoxically created another challenge for the NATO cyber security policy, mainly because of the manner in which it was formulated, namely that the decision whether to invoke the principle of collective defence would be "taken (…) on a case-by-case basis. "What it basically signified was that the Organization did not define specific conditions in which Article 5 of the Washington Treaty could be used to respond to cyberthreats. On the one hand, it ensured the necessary flexibility of this instrument which was adapted to many qualitatively different cyber incursions. Broadly speaking, such elasticity is useful as it may deter potential enemies, which remains uncertain on the Atlantic Alliance's reaction to serious cyberattacks. On the other hand, it has to be emphasised that the North Atlantic Treaty was drawn up in a different strategic situation, dominated by the logic of the Cold War. Therefore, the Treaty's provisions were adjusted to conform to the risks of traditional warfare, including the use of nuclear weapons. It was perfectly illustrated in the provisions of Article 6.[5] As mentioned above, cyberspace is a unique domain where many traditional mechanisms and instruments of the security policy may sometimes be insufficient or inadequate. In light of the provisions of the North Atlantic Treaty, a serious cyberattack crippling the prosperity and safety of a member state may not necessarily deplete its armed forces. Plus, the relationship between cyberspace and territory (understood in geographical terms) is still a subject of the ongoing scientific debate.[6] This, in effect, may cause unnecessary interpretation disputes among the decisionmakers in case of a serious computer attack against NATO. Furthermore, in contrast to the traditional theatres of warfare, cyberspace is a domain where incidents targeting the Alliance members' defence systems occur regularly and

4 *Wales Summit Declaration*, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales from 4 to 5 September 2014, NATO, 05.09.2014.

5 It stated that „For the purpose of Article 5, an armed attack on one or more of the Parties is deemed to include an armed attack: on the territory of any of the Parties in Europe or North America, on the Algerian Departments of France (2), on the territory of or on the Islands under the jurisdiction of any of the Parties in the North Atlantic area north of the Tropic of Cancer; on the forces, vessels, or aircraft of any of the Parties, when in or over these territories or any other area in Europe in which occupation forces of any of the Parties were stationed on the date when the Treaty entered into force or the Mediterranean Sea or the North Atlantic area north of the Tropic of Cancer". See *The North Atlantic Treaty*, Washington 04.04.1949, http://www.nato.int/cps/en/natolive/official_texts_17120.htm (access: 15.08.2015).

6 There are multiple views on the subject among the academics. For example, Fred Schreier indicated that „Cyberspace is qualitatively different from the sea, air, and space domains, yet it both overlaps and continuously operates within all of them". See F. Schreier, *On cyberwarfare*, DCAF Horizon 2015 Working Paper, No. 7, p. 13.

massively. A NATO-level reaction to each of them is impossible, meaningless, and counterproductive. Therefore, there should be a threshold separating cyberattacks bearing importance for the entire Euro-Atlantic community from the plethora of less significant computer attacks. Finally, it is often difficult to determine the attribution of computer attacks. This means that the boundaries between the "mainstream" cybercriminal activity and acts of political and military significance are somewhat blurred. Thus all these pending issues need to be addressed and clarified if the system of collective cyberdefence should be fully operable. The Wales summit resolutions made no reference to them, which may, in specific circumstances, lower the efficiency of this mechanism by leaving too much room for evasive interpretation in the most problematic cases.

Certainly, the decision to invoke the principle of Article 5 of the Washington Treaty will always be based on cautious political and military calculations, but there is a dire need for outlining some basic characteristics of serious cyber incidents, which will allow targeted member states to demand support from the Alliance. It would also be helpful for the Organization's decision-makers to distinguish less significant incursions from full-scale cyber conflicts. The urgency of this matter is constantly proven by thousands of high-profile cyberattacks against NATO-alone systems every year.[7]

In this context, it has to be stressed that the following proposals, maintaining a high degree of generality, were designed for the official documents published by the North Atlantic Treaty Organization, such as strategic concepts or summit declarations. They should, however, be clarified and concretized as much as possible in the classified documents, i.e. contingency plans.

Conditions necessary to invoke the NATO principle of Article 5 in case of cyber incursion

Designing system solutions within the security policy area should always take into account their simplicity, in accordance with the well-known adage of Hans Hofmann: "The ability to simplify means to eliminate the unnecessary so that the necessary may speak."[8] The resolution of the aforementioned problem should be founded on such logic in order to avoid unnecessary confusion and political disputes.

Bearing this in mind, the NATO cyber security policy should generally take into consideration only two major conditions, the fulfilment of which should trigger the mechanism of Article 5 of the North Atlantic Treaty.

First, in case of a noticeable cyberattack(-s) against a member state, the Alliance's analysts and decisionmakers should pay attention to targeted objects as well as the direct and indirect effects of these attacks. From this perspective, cyber incursions can be divided into three major categories: attacks aimed at military objectives and capabilities, critical infrastructure,

7 *The history of cyberattacks – a timeline*, NATO Review, http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm (access: 13.08.2015).

8 Efron B., Tibshirani R.J., *Introduction to the Bootstrap*, Boca Raton 1993, p. XIV.

and other assets which are less important from the point of view of national and international security. The first group generate no controversies as constituting military aggression would perfectly fit the scope of the Article 5 mechanism. The third group may include hacks against targets such as a central government or private sector websites, e-mail servers, computers and networks owned by individuals, enterprises, or local governments. These attacks, despite being frequently inconvenient, usually pose little threat to the core of nation's security. The second group, however, involves incursions which are potentially far more dangerous. According to the *Tallinn Manual on the International Law Applicable to Cyber Warfare,* critical infrastructure may be defined as "physical or virtual systems and assets under the jurisdiction of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment."[9] CI is composed of elements such as financial, communication, transportation, and defence systems, water and power lines or health services.[10] The proper functioning of each of these components is crucial for the safety and security of states.[11]

Successful cyberattacks against critical infrastructure, which nowadays is largely permeated by ICT, may manifest in various ways such as a stock market crash, the collapse of the banking system, the paralysis of crucial communication networks, or a power outage. Such scenarios are frequently analysed by many researchers who even admit the possibility of a computer attack against CI which would bring a nation state to its knees within seconds or minutes since a successful hack. Despite the fact that such an overpowering incursion is very difficult to conduct and rather unlikely, so far there have been multiple cases proving that critical infrastructure is vulnerable. One of the most symptomatic examples was the famous Stuxnet worm that caused widespread physical damages in the Iranian uranium enrichment plant in Natanz, slowing down the national nuclear programme.[12]

In this context, it has to be stressed that due to its importance, the NATO's collective defence principle should not be used to respond to less significant attacks, against second-tier targets, such as government websites, e-mail accounts or private sector databases, both with intention of intelligence gathering and destruction of digital information. Although these hacks are sometimes difficult to cope with and threatening from the perspective of national security, they are usually easier to counter and to recover from. Moreover, such an intention was visible in the aforementioned point 72. of the Wales summit declaration which stated that

> "The policy [Enhanced Cyber Defence Policy – M.L.] reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks."[13]

9 Schmitt M.N., ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge 2013, p. 211.

10 See Moteff M., Parfomak P., *Critical Infrastructure and Key Assets: Definition and Identification*, CRS Report for Congress, 2004.

11 See Świątkowska J. et al., *Bezpieczeństwo infrastruktury krytycznej. Wymiar teleinformatyczny*, Instytut Kościuszki 2014.

12 Langner R., *To Kill a Centrifuge*, The Langner Group 2013, p. 18.

13 *Wales Summit Declaration*, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales from 4 to 5 September 2014, NATO 2014.

By contrast, a serious violation of critical infrastructure integrity through cyberspace may lead to the loss of life of citizens or to the loss of ability to defend against internal or external threats. It may also cause enormous economic losses and endanger constitutional order. From this perspective, only the occurrence of extreme, most shattering computer attacks should be classified as a sufficient condition to invoke the principle of Article 5 of the Washington Treaty. This also means that collective cyberdefence should not be triggered in case of massive but unsuccessful attacks against critical infrastructure.[14] Such a solution would ensure that the principle of NATO's collective defence would not be used hastily and witlessly, which would discredit the very idea behind this instrument in the long run.

A second prerequisite to trigger NATO's collective defence in cyberspace should concern the identification of perpetrators behind cyberattacks. This solution is crucial for several reasons. To begin with, NATO Article 5 is a way too serious mechanism to treat it carelessly. Therefore, it should only be used in cases where the likelihood of committing an error concerning the attribution of computer attacks is almost non-existent. Otherwise, the consequences of decisions taken on false premises by NATO could be disastrous for the whole international community. Moreover, the knowledge of the perpetrator's identity is not only necessary to initiate proper defensive measures, but also to prepare potential offensive counter-reaction. And finally, as mentioned above, there is a crucial need for distinguishing between standard cybercriminal activity and acts bearing political or military significance. By no means should conventional cybercrime trigger any NATO's collective defence reaction. It is due to the fact that there are other, more well-suited international organizations and instruments available to respond to these threats. One can mention for example the European Union or MLATs (Mutual Legal Assistance Treaties).[15] Only acts which cannot be classified as "standard" cybercriminal hacks (like cyberwarfare or cyber terrorism), and committed by actors such as state intelligence agencies, military units, or organized armed groups, should be considered by NATO's decision makers. As the reaction to the WTC terrorist attacks has proven, the Organization is prepared to respond to harmful activities conducted by non-state actors. This may as well apply to cyberspace.[16]

However, this solution poses a major practical problem as the attribution of hacks is very difficult and often based on premises instead of hard evidence. Cyber units may track down IP addresses of culprits, analyse and point out specific features of malware or utilized hacking techniques. Unfortunately, it does not mean it is always possible to identify a person sitting behind a desk or its direct employers. At times, some state actors are even accused of hiring

14 Obviously, there should be a firm NATO-level reaction, but not on the grounds of Article 5. Article 4 of the North Atlantic Treaty could be considered as one of the most suitable tools to use in such a situation.

15 See Skrzypczak J., *Bezpieczeństwo teleinformatyczne w świetle Europejskiej Konwencji o Cyberprzestępczości*. "Przegląd Strategiczny" 2011, No 1.

16 Some academics may argue that the NATO cyber security policy should be adjusted to counter the cyber activities of state actors only, recognizing decisions taken after the 9/11 as an exception. However, considering the rising scale of terrorist activities in the digital domain and their developing capabilities to conduct cyberattacks, such a solution would be counterproductive. Moreover, NATO's collective defence mechanisms in this area should be as flexible as possible. And finally, nowadays it is frequently possible to respond to cyber terrorist attacks with the use of conventional tools, such as aerial bombing or special forces operations. This practice could therefore have a strong deterrent effect.

cybercriminal groups to conduct computer attacks against their enemies' networks in order to conceal their identity. One of the most inculpated countries to do so is Russia.[17] In this situation, from the point of view of the victim, a politically motivated cyber incursion could be misperceived as a purely criminal act. This is surely a major obstacle for any collective cyberdefence reaction of the Alliance as there should be a very high level of certainty concerning the identity of the inculpated state or non-state actor. Therefore, the technical and forensic analysis of a cyberattack(s) should provide enough evidence to initiate the international, NATO-level response against its perpetrator. This is nowadays one of the most significant tasks for the Atlantic Alliance cyber security policy that is fundamental for its long-term effectiveness.

Conclusions and recommendations

The principle of Article 5 of the Washington Treaty, used only once on the occasion of the 9/11 terrorist attacks, holds a great significance for the security of the Euro-Atlantic community. Since 2001, NATO has developed other multiple measures to support the security of its member states that are endangered by various international threats. Recently, it was manifested by the augmentation of Turkey's air defence capabilities by its NATO allies (Operation Active Fence).[18] Taking this into consideration, it has to be stressed that NATO's collective defence mechanism should only be used to answer the most serious cyber incursions. The principle of Article 5 should be invoked carefully and only in case of a computer attack(s) which would paralyse or destroy the elements of critical infrastructure and/or military capabilities of a member state, causing substantial physical or virtual damages, or even the death of civilians. Otherwise, the whole mechanism could be discredited in the long run. Above all, the member states themselves should try to secure their national ICT infrastructures without help from other members or the Organization itself, which was stressed during the Wales summit in 2014 and is an obligation under NATO Article 3. Therefore, Article 5 should be used only in extreme circumstances. However, this does not mean that in case of less significant cyberattacks NATO cannot support its members' defensive capabilities.

In this context, it is possible to point out several recommendations concerning the conditions in which the North Atlantic Treaty Organization should deliberate on triggering the collective cyberdefence mechanism:

1. The principle of Article 5 of the Washington Treaty should not be used to respond to cyberattacks targeting less vital, second-tier targets within a member state's digital domain, such as websites, e-mail servers, or even government databases. On the contrary, only the most serious incursions that are successful in crippling critical infrastructure and/or military capabilities should be perceived as a sufficient condition for triggering NATO's collective cyberdefence mechanism.

2. In order to invoke the NATO principle of Article 5, these severe cyberattacks should have a significant impact on the ordinary functioning of a NATO member state. Among others, it may concern such consequences as the death of civilians, enormous economic losses, damage or destruction of objects, the disruption of abilities to defend and protect the society or the infringement of constitutional order.

3. The principle of Article 5 of the North Atlantic Treaty should only be used in cases when serious cyberattacks against a member state are committed by well-identified state and non-state actors, excluding common criminals. They can include hostile governments, international organizations, terrorist organizations, or various rebel groups. NATO should not react to the most serious but standard cybercrime acts as there are other international organizations and instruments which are more well-suited to counter these types of threats.[19]

4. In order to make these solutions efficient, NATO and its member states should focus their efforts on the development of cyber reconnaissance and intelligence structures equipped with enough technical and political expertise to track down actors responsible for cyber incursions. Such a system should combine CYBINT (cyber intelligence, especially techniques for cyberattack attribution), HUMINT ("conventional" human intelligence), SIGINT (signals intelligence, e.g. satellite imagery), OSINT (open source intelligence), as well as a political analysis.

   In this context, if the victim state or the Organization itself cannot provide enough evidence to interpret properly the incidents in cyberspace, the principle of Article 5 should not be used. It is due to the risk of a possible provocation or a mistake, which could have grievous consequences for international security and stability.

   The specific nature of NATO's decision-making mechanism requires a high degree of certainty in the attribution of a cyberattack. Since the decision to invoke Article 5 would be taken by the leaders of all member states, there is a risk that any doubts in this matter could slow down, disrupt, or cripple the process of reaching a consensus.

   This condition is essential to prevent all possible negative effects of misinterpretation of cyberattacks against the member states.

5. The system of response built around the aforementioned principles does not preclude NATO from reacting to less significant incidents in cyberspace experienced by its members. In some cases, below the threshold of Article 5, the Organization may support national cyber security capabilities. Such a solution should be made possible for example if a member state constantly "leaks" classified data concerning the activities of the Organization due to successful, repetitive, and massive cyber espionage hacks. In such a case, it would be in NATO's best interest to prevent further damages to the security and integrity of the Alliance's databases, for instance under Article 3

17 Jones S., *New Twists in Russia's Cyber Campaign Against NATO and Its Members*, Atlantic Council, 04.08.2015, http://www.atlanticcouncil.org/blogs/natosource/new-twists-in-russia-s-cyber-campaign-against-nato-and-its-members (access: 14.08.2015).

18 *NATO support to Turkey: Background and timeline*, North Atlantic Treaty Organization, 19.02.2013, http://www.nato.int/cps/en/natohq/topics_92555.htm (access: 14.08.2015).

19 Obviously NATO does respond to some types of conventional criminal activities, like piracy; however, it does not mean that it should react to standard cybercriminal activities by applyingthe principle of Article 5.

or Article 4 of the North Atlantic Treaty. In principle, these activities should be much more important for everyday cyber security solutions of the Atlantic Alliance. In this context, Article 5 may be considered as a "safety valve", suitable for use in the most extreme situations.

6. In cyberspace, not only member states' but also NATO's computer networks may be seriously damaged. If the Organization's critical communication and information assets (similar in value to a state's critical infrastructure) are destroyed or paralysed by a cyberattack, it should be a sufficient reason to invoke the principle of Article 5.

7. The decision to trigger the collective defence mechanism following cyber incidents could potentially result in firm actions undertaken by NATO in all possible domains. The Atlantic Alliance needs to reserve its right to respond to the most significant cyberattacks with conventional forces. Otherwise, the credibility of Article 5 could be undermined. In this context, however, it is important to stress that kinetic counter-attack would have the most serious consequences. Therefore, NATO member states should develop offensive cyber capabilities which, in some circumstances, would be more proportional to use in response to computer incidents instead of conventional military power.

To summarize, given the aforementioned problems, the system of collective cyberdefence, based on the Wales summit provisions, should only be used in the most severe cases. To ensure its efficiency, the system should be a relatively simple, two-step reaction. It would both secure its necessary flexibility and dispel any doubts concerning the interpretation of the North Atlantic Treaty and other NATO documents. The first step would involve the examination of whether the integrity of critical infrastructure/military capabilities and objects was seriously breached by a cyberattack(s) as any damage to them would significantly impinge on national security, and therefore the security and stability of the whole Euro-Atlantic community. The confirmation would enable the second step concerning the attribution of computer incidents. The NATO principle of Article 5 could be invoked only in cases connected with activities of actors such as states, terrorist organizations, or rebel groups. Standard criminal activity should be addressed by other international organizations like the European Union.

Taking into consideration only these two conditions, the famous cyber incidents in Estonia[20], being a cornerstone of all NATO's cyber security developments, would not be a valid reason to trigger the collective defence mechanism as there was no significant breach of critical infrastructure or military objects and capabilities. But it does not mean that the Alliance should not, in case of similar events, provide additional support (i.e. cyber security experts, know-how) to the attacked member state. On the contrary, a cyberattack against a member of the Alliance, with the consequences similar to the *casus* of the Stuxnet worm, could be considered as a valid reason to initiate a debate over the invocation of Article 5 of the Washington Treaty if perpetrated by a properly identified state or non-state actor.

20 Ruus K., Cyber War I: Estonia Attacked from Russia. "European Affairs" 2008, No. 1-2; Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, pp. 184-201.

Planning for Cyber in the North Atlantic Treaty Organization[1]

Kate Miller
Belfer Center for Science and International Affairs
John F. Kennedy School of Government
Harvard University

1. Planning For Cyber In The North Atlantic Treaty Organization

1.1 Introduction

1.1.1 Over the course of the past decade the North Atlantic Treaty Organization (NATO) has worked to ensure that its mission of collective defence and cooperative security is as effective in cyberspace as it is in the domains of air, land, sea, and space. It has created several bodies and developed a collection of policies to deal with diverse aspects of cyberdefence. With the anticipated elevation of cyberspace to the fifth operational domain of warfare at the 2016 Warsaw Summit, however, the Alliance needs to consider cyber capabilities and undertake planning for operations - including offensive ones - directed beyond its networks. And it should establish a Cyber Planning Group to do it.

1.1.2 Fortunately, while the issue of cyber operations beyond NATO's own networks is a politically difficult one given the complex mosaic of national, transnational (EU), and international law; the role of national intelligence efforts in certain types of operations; and ever-present disputes over burden-sharing, the Alliance already has invaluable experience in developing policies and procedures for contentious and sensitive tools in the form of the Nuclear Planning Group (NPG). This article will thus proceed as follows: It begins with a brief overview of actions NATO has already taken to address cyberthreats. It will then explore why these, while important, are insufficient for the present and any imaginable future geopolitical threat environment. Next, it will address the history of the NPG, highlighting some parallels with the present situation regarding cyber and drawing out the challenges faced by, and activities and mechanisms of, the NPG. Finally, it will make the case that a group modeled on the NPG can not only significantly enhance the Alliance's posture in cyberspace, but can serve as an invaluable space for fostering entente and reconciling differences on key aspects of cyber policy. It concludes that the Alliance needs to consider offensive cyber capabilities and planning, and it needs a Cyber Planning Group to do it.

1 The views expressed are the author's own.

1.1.3 Given NATO's collective defence mandate, a brief note on the use of the terms "defensive" and "offensive" operations and capabilities is appropriate and even necessary. When the term "defensive" is used here, it refers to activities within NATO's own networks, taken either to protect Alliance information systems, enhance resiliency in the event of a breach, or impede and/or remove any unauthorized presence. "Offensive" operations or capabilities cover the range of activities that may take place outside of NATO networks, including dismantling or sinkholing botnets (networks of computers infected with malware and controlled as a group), distributed denial of service (DDoS) activities, the introduction of malicious code into adversary networks, etc.

1.2 Defensive Efforts

1.2.1 The Alliance, as mentioned, has created a number of bodies to address various aspects of defensive capabilities and policies in cyberspace. The NATO Communication and Information Agency (NCIA), for example, provides technical cybersecurity services throughout NATO, and through the NATO Computer Incident Response Capability (NCIRC) Technical Centre responds to "any cyber aggression against the Alliance."[2] Along with the NATO Military Authorities, it is responsible for identifying operational requirements, acquisition, implementation, and operating of NATO's cyberdefence capabilities. The Alliance also has a Rapid Reaction Team of six civilians, which can be deployed to NATO facilities, operational theatres, or to support an Ally enduring a significant cyberattack.[3] The NATO Consultation, Control and Command (NC3) Board provides consultation on technical and implementation aspects of cyberdefence, while the Cyber Defence Management Board (CDMB), comprised of leaders of the policy, military, and technical bodies in NATO that handle cyberdefence, coordinates cyberdefence throughout NATO civilian and military bodies.[4] At the political level, the Cyber Defence Committee is charged with political governance and cyberdefence policy in general and provides oversight and advice at the expert level. Outside of the NATO Command Structure and NATO Force Structure, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, is a research and training facility that offers crucial cyberdefence education, consultation, and research and development.

1.2.2 The Alliance has also developed and endorsed a collection of policies to guide its approach to conflict in or through cyberspace. In late 2007 it adopted the NATO Policy on Cyber Defence that, as stated in the Bucharest Declaration, emphasized NATO's need to protect key information systems, share best practices, and help Allies counter cyberattacks.[5] The Strategic Concept adopted at the 2010 Lisbon Summit tasked the North Atlantic Council with developing an in-depth cyberdefence policy and action plan, mandated the integration of cyberdefence into operational planning processes, and committed to both promote the development of Allies' cyber capabilities and assist individual members on request.[6] The 2011 Cyber Defence Concept, Policy, and Action Plan updated the 2008 policy and called for the Alliance to further develop the "ability to prevent, detect, defend against, and recover from cyberattacks."[7] It also further integrated cyberdefence into existing policy processes by connecting the CDMB efforts with the Defence Policy and Planning Committee.[8] Finally, at the 2014 Wales Summit, NATO endorsed an Enhanced Cyber Defence Policy, which clarified for the first time that a cyber attack on a member state could be covered by Article 5 (the collective defence clause) of the North Atlantic Treaty.

1.2.3 These organs and bodies all serve vital functions, but they do not go far enough. At present, the Alliance has only limited publicly articulated policy regarding the use of cyber tools to target adversaries' computers and networks in response to either cyber or kinetic/conventional attacks.[9] While NATO may have a classified policy or doctrine that goes beyond its statement that it "does not pre-judge any response and therefore maintains flexibility in deciding a course of action" in response to a cyber attack, this suggests a vacuum that undermines the credibility of the Alliance's collective defence and common security.[10] NATO needs to address the lack of policy around how the alliance and member states may use offensive cyber capabilities in both defensive and offensive operations. And it requires a body authorized and equipped to develop that truly comprehensive, integrated cyber policy and situate it within the Alliance's broader strategies and objectives.

1.3 The Need For Offense

1.3.1 The question of whether and how NATO should undertake cyber operations outside of its own networks, even in defensive, counter-attack scenarios, is not new. The Alliance has a long-standing defensive orientation and has stated on multiple occasions that its top priority is the protection of its networks and the cyberdefence requirements of the national networks upon which it relies.[11] This stance risks becoming a cyber "Maginot line" rather than an effective strategy, however, and many have argued that it must extend its focus.[12] The Atlantic Council's Franklin Kramer *et. al*., for example, recently called on NATO to "develop doctrine and capabilities to provide for the effective use of cyberspace in a conflict as part of NATO's warfighting capabilities."[13] James Lewis, Senior Fellow at the Center for Strategic and International Studies (CSIS), has noted that some Alliance members already possess offensive cyber capabilities that are "essential for the kinds of combat operations that NATO forces may carry out in the future" and argues the Alliance needs to enunciate how these would be used in support of NATO

2 Healey, J. and Tothova Jordan, K, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, 2014, http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf (access: 28.05.2016), p. 4.

3 *Men in black – NATO's Cybermen*, 24 April 2015, http://www.nato.int/cps/en/natolive/news_118855.htm (access: 21.06.2016).

4 *Cyber Defence*, 16 February 2016, http://www.nato.int/cps/en/natohq/topics_78170.htm (access: 08.06.2016).

5 Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic council in Bucharest on 3 April 2008, (Press Release (2008) 049), http://www.nato.int/cps/en/natolive/official_texts_8443.htm (access: 30.05.2016).

6 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, (Press Release (2010) 155), http://www.nato.int/cps/en/natolive/official_texts_68828.htm (access: 21.06.2016); *Cyber Defence*, op cit.

7 Chicago Summit Declaration Issued by the Heads of State and Government Participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012, (Press Release (2012) 062), http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en (access: 30.05.2016).

8 Fidler, D., Pregent, R., Vandume, A., *NATO, Cyber Defense, and International Law*, [in] *Articles by Maurer Faculty. Paper 1672*, 2013, http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub (access: 08.06.2016).

9 For an exception, see NATO's Rules of Engagement for Computer Network Operations, contained in Series 36 of the MC-362/1 catalogue.

10 *Defending the networks: The NATO Policy on Cyber Defence*, 2011, https://ccdcoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf (access: 08.06.2016).

11 Ibidem.

12 Fidler, D. et. al, op cit. p. 23.

13 Kramer, F., Butler, R., and Lotrionte, C., *Cyber, Extended Deterrence, and NATO*, [in:] *Atlantic Council: Brent Scowcroft Center on International Security Issue Brief*, May 2016, http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf (access: 03.06.2016), p. 6.

activities.[14] And Jason Healey, director of the Cyber Statecraft Initiative at the Brent Scowcroft Center on International Security, has repeatedly called on the Alliance to at least consider offensive coordination if it cannot develop its own offensive capabilities.[15]

1.3.2 Offensive cyber capabilities serve a number of purposes. They can act as an important force multiplier, especially in asymmetric conflicts. If, for example, conflict broke out in the Baltics, NATO or individual Allies' cyber capabilities targeting an adversary's communications, logistics, and sensors could preclude a *fait accompli* and buy the Alliance precious time to mobilize land, sea, or air forces.[16] This also suggests that in some ways such tools are an extension or evolution of electronic warfare (EW) capabilities, long essential to assuring information superiority and thus NATO's military effectiveness. In the 1950s, NATO promulgated an EW Policy that recognized "the establishment and maintenance of superiority in [EW] is an essential part of modern warfare" and acknowledge that "since all NATO nations and commands will be conducting [EW] operations, it is essential that the coordination and control be exercised at the highest level feasible."[17] As cyber and EW merge and cyber becomes embedded in warfighting, then, a similar policy that outlines responsibilities and national authorities pertaining to cyber operations is needed.

1.3.3 Offensive capabilities also create strategic flexibility, offering an option that falls between talking and bombing. This is particularly important given the hybrid warfare that has taken place in the NATO neighborhood and the low-intensity conflict work that NATO has participated in. While offensive cyber tools can have destructive and disruptive effects, they can also be temporary and/or reversible, and therefore represent an option that certain Allies may view as more palatable or acceptable. Furthermore, not only do adversaries already use offensive cyber capabilities against NATO, but if conflict breaks out they will have vulnerabilities that are best exploited using cyber means. As Matthijs Veenendaal et al. point out in a cyber policy brief for the CCDCOE, if NATO faced an air attack it would not prohibit the use of airpower – limiting itself to air defense systems – in response.[18] For member states to deny the Alliancecyber capabilities, or even the ability to plan for their use by individual Allies, fundamentally undermines NATO's deterrent posture and its credibility among both its own members and its potential adversaries. It also corrodes NATO's ability to prevail as a collective defence entity in a conflict. Finally, while there is no reason a proportional response needs to be symmetric (i.e. confined to the same domain), an enunciated offensive capability and policy on its use would also impact potential adversaries' risk calculations, forcing them to recognize that NATO can respond in kind, as well as kinetically or conventionally.[19]

1.3.4 There are, of course, a number of challenges associated with the use of cyber capabilities, especially in a collective manner. As President Toomas Hendrik Ilves of Estonia noted at the June 2016 CyCon, when it comes to cyber, NATO members are in "intelligence agency mode" where they "share as little as possible and only when necessary."[20] This is to some extent understandable: highly targeted cyber tools often rely on intelligence that is both difficult to obtain and inherently impermanent, making national entities reluctant to share information even regarding a particular tool's anticipated effects. Unlike nuclear weapons, which have more or less the same effect no matter where deployed with the only truly important variable being scale, even partial information about the targeting or functionality of a given cyber capability may allow the target to patch a vulnerability or disconnect a particular device, rendering the tool ineffective or altering its effect. Sharing such information can increase the likelihood it will be leaked and thus result in what is essentially inadvertent unilateral disarmament. Furthermore, intelligence efforts are under the control of national governments and often require enormous amounts of time and effort.[21] Although it is likely that any adversary which attacks NATO is targeted by member states' collection activities, it is an admittedly complicating factor in any Alliance effort to operate effectively outside of its own networks in cyberspace.

1.3.5 An additional issue is the scale and specificity of any given cyber tool (that is, how easily it propagates and limitations on targeting) and the complicated legal environment in which NATO must operate. The Alliance has to navigate a complex web of national, EU, and international law regarding the conduct of military operations and develop policies and strategies that result from and in legal convergence. While there is evidence that software can be highly discriminate and proportionate and its spread controlled, without sufficient preparatory work its effects can be unpredictable and hard to contain. In particular, untargeted entities may be impacted (although, again, if appropriate preparatory effort is made, such entities should not experience deleterious effects even if they are infected with a piece of code or malware). This suggests additional complications for NATO, which must grapple with the risk that certain strategies will reveal or create friction or legal divergence in the Alliance.[22]

1.4 The Nuclear Planning Group Model

1.4.1 Once NATO decides it needs to address offensive capabilities, of course, a key issue will be how it develops plans and policies for their use. This is where the experience of the NPG is illuminating, demonstrating both the limitations such a group will face as well as highlighting reasons to believe in its potential. The Nuclear Planning Group was established in 1966 in order to address nuclear weapons in the European theater: an issue that inflamed debate from the beginning on how they might be used (and the consequences of their use) - much as offensive cyber capabilities have done.[23] The introduction of theater nuclear weapons under U.S. President Dwight D. Eisenhower's "New Look" strategy stripped non-nuclear allies of operational control of the Alliance's military posture and handed it to the Americans (and, to a lesser extent, the British), who owned the weapons and thus had significant influence over the strategies that governed them.[24] This imbalance induced dissatisfaction and stress in the Alliance that was

14 Lewis, J., *The Role of Offensive Cyber Operations in NATO's Collective Defence*, "The Tallinn Papers" 2015, No. 8, p. 3.
15 Healey, J., op cit., p. 6.
16 Kramer, F., et. al, pp. 8-9.
17 *NATO Electronic Warfare Policy* [in] *A Report by the Standing Group to the Military Committee on NATO Electronic Warfare Policy*, (MC 64), 14 September 1956, http://archives.nato.int/uploads/r/null/1/0/104853/MC_0064_ENG_PDP.pdf (access: 03.06.2016), pp. 2-3.
18 Veenendaal, M., Kaska, K., and Brangetto, P., *Is NATO Ready to Cross the Rubicon on Cyber Defence?* "Cyber Policy Brief" June 2016, https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf (access: 21.06.2016).
19 Lewis, J., op cit. p. 7.
20 Ilves, T., *President Toomas Hendrik Ilves's opening speech at CyCon in Tallinn on June 1, 2016*, https://www.president.ee/en/official-duties/speeches/12281-president-toomas-hendrik-ilvess-opening-speech-at-cycon-in-tallinn-on-june-1-2016/index.html (access: 09.06.2016).
21 Lewis, J., op cit., p. 9.
22 Fidler, D., et. al, op cit. p. 13.
23 Buteux, P., *The Politics of Nuclear Consultation in NATO 1965-1980*, Cambridge, 1983, p. 3.
24 Ibidem p. 7.

further aggravated when new weapons were developed or major revisions in strategy (such as the Kennedy Administration's Flexible Response) were proposed. These tensions, in turn, undermined cohesion - and therefore effectiveness and credibility - within the Alliance. The NPG was thus needed not only to address actual force posture and planning issues related to command and control, but to serve the vital political purpose of preserving cohesion. In much the same way, advanced cyber warfighting capabilities are unevenly distributed among allies, and yet just as nuclear weapons were a central element in the Alliance's defensive posture, so these capabilities will be vital in any future conflict. And like theater nuclear weapons before the establishment of the NPG, cyber capabilities lie largely outside the Alliance's institutional framework.

1.4.2 At its inception, only seven states sat on the NPG at any given time: the United States, United Kingdom, Italy, and West Germany were permanently represented while the remaining seats rotated among eligible nations (i.e. those participating in the integrated military structure).[25] (Today, all NATO members with the exception of France participate in the NPG, irrespective of their possession of nuclear weapons). Broadly speaking, the group provided a consultative process on nuclear doctrine within NATO. In particular, it focused on three issues of nuclear planning: (1) how and under what circumstance the Alliance may need to use nuclear weapons; (2) the question of what objectives might be served by the use of nuclear weapons in the European theater; and (3) what kinds of consultation should take place in circumstances where the use of nuclear weapons could be contemplated.[26] The NPG also allowed the Alliance to isolate the issues of nuclear planning and doctrine from other matters, protecting it to some extent from being impacted by disagreements over other alliance policies.[27]

1.4.3 Significantly, the NPG largely avoided issues of ownership, physical possession, and therefore of direct control of nuclear weapons and decisions regarding their use, which resided in national governments. This was in part a response to earlier efforts to address nuclear sharing, wherein the aggregation of agreement on participation in NATO's nuclear policy and agreement on ownership, force composition, and decision-making formulae actually reinforced the intractability of the sharing issue.[28] Instead, the NPG focused on allied consultation and participation in planning, an approach that was both politically and operationally more feasible for countries controlling the weapons (primarily the United States). While avoiding joint control, this ensured non-nuclear allies could have a role in the procedures by which those possessing nuclear weapons reached decisions concerning them, offering an avenue to constrain their behavior. For the states controlling the weapons, those processes served to reinforce cohesion in the Alliance and allowed them to win support and acceptance for their nuclear policies.[29]

1.4.4 The issue of secrecy, mandated on the part of the United States by legislation intended to restrict the spread of nuclear technology, also had a significant impact on the work of the NPG. On the one hand, this legislation, including the Atomic Energy Act, limited the amount of information on nuclear matters the U.S. government could reveal to NATO allies. In particular, the 1958 amendment to the Atomic Energy Act gave the U.S. Congress the power to veto any "atomic cooperation for military purposes with any nation or regional defence organization(…)".[30] On the other hand, as early as 1954, in response to the development of a Soviet nuclear capability, the United States adjusted its laws in order to supply nuclear information and materials to its NATO Allies in order to reinforce its deterrent and collective defence.[31] Furthermore, by 1961 the United States recognized that in order to get other Allies to understand and accept as doctrine its strategic innovations, it needed to relax its approach to nuclear secrecy. This led the United States to offer much more detailed information than it previously had regarding both technical characteristics of the weapons and relative force levels and strategic concepts.[32]

1.4.5 The above considerations offer key insights into how a Cyber Planning Group could function. First, issues of secrecy regarding various capabilities, while they will limit what the Group can discuss, need not prevent it from undertaking consequential work. Identifying circumstances when use might be appropriate and developing procedures for consultation regarding that use require only a general sense of their effects, allowing secrecy regarding precise operation. However, the nuclear experience also suggests that key Alliance members can overcome the habit of secrecy if there is sufficient need for information sharing to reduce friction and facilitate consensus building within NATO. Moreover, there is a sense in some segments of the United States that, as former director of the National Security Agency and Central Intelligence Agency General Michael Hayden has stated, information on U.S. cyber policies is "overprotected" and there is a need to "recalibrate what is truly secret."[33] It may be that as cyber becomes increasingly integrated into military operations, the need for cooperation will outweigh the desire for secrecy.

1.4.6 Another useful lesson that may serve to reduce friction at the outset is that Allied or joint control of offensive capabilities - especially those that rely on extensive intelligence efforts – is likely politically impossible and operationally undesirable. That does not negate the value of consultation and an allied approach to planning for their use, however. Developing a collective understanding of how and under what circumstances these capabilities may be deployed by members on behalf of the Alliance, and the possible consequences of that deployment, can enhance its defensive and deterrent posture by expanding its arsenal and lending credibility to threats to utilize it. It is also vital that interested parties understand what tools and resources are and are not available for their defence in order to assure effective planning.

1.4.7 Furthermore, while Allied use of cyber capabilities that can result in significantly destructive outcomes will likely be highly constrained for the foreseeable future, there is no reason the Alliance should not develop doctrine and/or policies regarding the use of activities such as distributed denial of service attacks or dismantling botnets.[34] These are activities regularly deployed against the Alliance and its member states that, in a time of conflict, may be useful to NATO. Just as the NPG discussed the possibility of using theater weapons to slow a conventional invasion,

25 *Cyber Defence*, op cit.
26 Buteux, P., op cit. p. 89.
27 Ibidem, p. 61.
28 Ibidem, p. 15.
29 Ibidem, pp. 184-186.
30 Nieburg, H., *Nuclear Secrecy and Foreign Policy*, Washington, D.C. 1964, p. 50.
31 Ibidem, p. 19.
32 Buteux op cit. p. 21-22.
33 Hayden, M., *Statement of The Honorable Michael V. Hayden*, (Testimony), Cyber Threats and National Security, House Select Intelligence Committee, (4 October 2011), http://congressional.proquest.com.ezp-prod1.hul.harvard.edu/congressional/result/congressional/pqpdocumentview?accountid=11311&groupid=103838&pgId=43bc3ae6-fbd2-47a7-b887-914ecc3d3224 (access: 21.06.2016).
34 This principle has been acknowledge, allowing work to begin on Allied Joint Doctrine for Cyberspace Operations. It is unclear to the author to what extent this doctrine may address activities outside NATO networks, however.

for example, a Cyber Planning Group should examine how limited offensive tools such as denial of service activities or actively hunting and dismantling a botnet can offer a stopgap measure to disrupt an adversary's malicious activity, even if said adversary is not attacking by cyber means. During the 2008 war between Georgia and the Russian Federation, for example, Georgia's efforts to respond to Russian military maneuvers were impeded by widespread denial of service attacks, website defacements, and related activities that impacted the government's ability to communicate with its populace as well as the outside world.[35] Such capabilities would be useful for NATO and/or its member nations in the event of a conflict.

1.4.8 Finally, it is important to appreciate that the establishment of a Cyber Planning Group would constitute a statement of policy in and of itself, regardless of what it may accomplish. Just as creating the NPG signaled to both the Soviet Union and to NATO members that the issue of theater nuclear weapons was a vital one demanding dedicated study by the Alliance, so a Cyber Planning Group could emphasize for Allies and adversaries alike the seriousness with which NATO addresses the issue of comprehensive, integrated cyber operations.

1.5 Conclusion

1.5.1 NATO's member states have proven sensitive to discussing cyber capabilities directed beyond its own networks, let alone the question of whether and how the Alliance may use them them.[36] Rather than indicating that NATO should let the issue lie, however, the contentious nature of the issue and absence of discussion suggest that consultation and efforts to build consensus are important for alliance cohesion in a volatile and divisive international environment. The fact of the matter is that these capabilities are likely to be crucial in any future conflict. Consultative procedures may serve to reveal and then reduce fractures in the Alliance before those conflicts break out.

1.5.2 The Alliance's central mission of collective defence, including in cyberspace, will soon require a comprehensive cyber operations policy in order to maintain the credibility of both its deterrent and defensive posture. It is an admittedly challenging issue, with many conflicting aspects, but to continue to ignore it will limit NATO's ability to serve as a useful mechanism for handling collective defence, common security, and crisis management. Therefore, NATO should take up the invaluable lessons offered by the experience of the Nuclear Planning Group and either expand the portfolio of the current Cyber Defence Committee (and perhaps the CDMB) to include offensive cyber tools and operations or establish a new body modeled on the NPG.

1.5.3 One of the most remarkable features of the Alliance has been its ability to remain relevant by evolving to address changing threats, ranging from Soviet military power in Europe to international terrorism. By engaging in consultations focused on understanding when offensive cyber capabilities will be most useful and appropriate and what objectives they can help achieve, and developing a coherent yet flexible doctrine, a Cyber Planning Group will assure NATO's continued relevance - and thus its future.

35 Bumgarner, J., and Borg, S., *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf (access: 30.05.2016).

36 Fidler, D., et. al, op cit. p. 24.

Hybrid Threats – the New Realm of NATO–EU Cooperation

Joanna Świątkowska, Ph.D.
Programme Director of the European Cybersecurity Forum,
Senior Research Fellow
The Kosciuszko Institute

It is true to say that increasingly sophisticated and intensive employment of hybrid warfare is the future of international conflicts and at the same time one of the most serious challenges for the security of modern states.

Exploiting cyberspace in order to exert a negative influence (understood in broad terms) on an opponent is, in principle, an inherent element of a hybrid strategy. Cyber activities can be undertaken by exercising "soft power" – i.e. when their goal is primarily to affect the perception of the recipient by means of manipulation, disinformation, and fraud etc. – and "hard power" – i.e. when cyberattacks result in the paralysis or destruction of targeted goals, most frequently critical infrastructure.

The next chapters of this report will elaborate more on the aforementioned ways of conducting activities in cyberspace. The aim of this article, however, is to explain the nature of hybrid threats, particularly those aimed at exploiting ICT tools, as well as to highlight actions that should be taken in order to face them.

Paradoxically, the emergence of intensified hybrid threats offers a perfect opportunity to reflect on, redefine, and systematise the existing mechanisms of cooperation between NATO and its partners, especially the European Union (EU). Hybrid conflicts can spur the development of strategic collaboration, which until now has been chaotic and underspecified in many areas.

In order to make strong recommendations concerning NATO's engagement in countering hybrid threats and its cooperation with the EU in this matter, we first need to specify the nature of these threats.

First of all, taking into consideration the fact how complex and multi-faceted the phenomenon is, it is worth making the effort to avoid creating strict definitions. Moreover, a flexible approach in this respect will facilitate a more effective response to the dynamically changing activities instigated within a wide array of hybrid warfare strategies.[1]

With this in mind, it is worth drawing attention to a few common elements, inherent to the majority of operations conducted during hybrid conflicts.[2]

Hybrid Warfare Activities:[3]

- are conducted under the threshold of war;
- are intended to cause chaos and political, military, economic, and social destabilization;
- are conducted by state and non-state actors alike;
- engage a wide range of resources, most notably non-military actions (diplomatic, economic, psychological, activities conducted in cyberspace);
- take advantage of an opponent's weaknesses.

Hybrid conflicts engage a broad spectrum of political, social and military resources. To effectively counter them, a corresponding conglomerate of assets has to be released. Therefore, in order for NATO to brace itself for hybrid threats, the Alliance not only has to revisit its capabilities, but more importantly it needs to step up its cooperation with partners who will complement its operations, most notably with the EU.

As a both political and economic organization, the EU can support the Alliance's military activities in a complementary manner. Distinct nature and diverse accents placed in the areas of activity of these two institutions in a natural way determine different roles and responsibilities of the EU and NATO. Merging them to achieve synergy will provide the best response to multidimensional operations launched in hybrid conflicts.

The cooperation and assignment of responsibilities between both organizations can take on different forms and occur on different levels. The analysis of actions already undertaken by NATO as well as EU's plans presented in the recently published document entitled *Joint Communication To The European Parliament And The Council Joint Framework on countering hybrid threats* a European Union response, can serve as a starting point to define the framework for collaboration and the scope of responsibilities.

1 See: *Joint Communication To The European Parliament And The Council Joint Framework on countering hybrid threats* a European Union response, 06 April 2016.

2 The presented catalogue results from both the observation of specific examples of such activities that have recently occured and analyses prepared by various expert centres.

3 See: Joint Communication To The European Parliament And The Council Joint Framework on countering hybrid threats a European Union response, 06 April 2016; NATO Conference Report, NATO and New Ways of Warfare: Defeating Hybrid Threats (Rapporteur: Professor Julian Lindley-French), 29-30 April 2015; Research Division – NATO Defense College, NATO Parliamentary Assembly, Defence and Security Committee, Hybrid Warfare: NATO's New Strategic Challenge? (General Rapporteur: Julio Miranda Calaha), 1 April 2015.

The document consists of 22 actions aimed at combating hybrid threats and grouped into three main areas: raising awareness, building resilience, and preventing, responding to and recovering from crisis situations. It is important that NATO and the EU develop close cooperation within all of these areas of engagement. A selection of proposals for common actions has been given below.

In Order To Raise Awareness:

- It is necessary to foster cooperation to better understand the nature of hybrid threats that will facilitate early detection of danger. The EU plans to conduct research on hybrid threats to establish early indicators and warnings of hybrid threats. In addition, the EU intends to set up a *Hybrid Fusion Cell* in order to collect and analyse information about hybrid threats.

- The backbone of NATO-EU cooperation in this area should be effective intelligence sharing (it is important to note that intelligence gathered should come from both civil and military sources), but also engaging NATO's experts in the process of identifying indicators and characteristics of hybrid threats.

- There is a need for effective and harmonized cooperation between NATO and the EU to synchronise their strategic communications (also in cyberspace). The cooperation should aim at establishing common narration in fight against disinformation spread by the opponent, including attempts to legitimize his actions by presenting skewed interpretations of international law. In addition, it should also be addressed to the audiences both within and outside the EU and NATO.

In Order To Build Resilience:

- It is necessary to strengthen cooperation to increase cyber resilience of critical infrastructures of the EU and NATO member states. A step in the right direction was the signing of a *Technical Arrangement* between the EU and NATO which provides a framework for cooperation between NCIRC and CERT-EU. This initiative should be further developed.

- It is critical for both organisations to foster synergy and integrate efforts to reinforce public-private cooperation aimed at enhancing cybersecurity (the need for harmonization of work under the EU's Private-Public Partnership and NATO Industry Cyber Partnership is strongly recommended).

In Order To Prevent, Respond To, And Recover From Crisis Situations:

- EU and NATO should develop and practise joint response scenarios to respond to potential hybrid threats, with special emphasis put on actions undertaken in cyberspace. These actions should draw upon the DIMEL model which presupposes that achieving specific

goals requires all available instruments and resources (D – diplomatic, I – Information, M – military, E – Economic, L – Legal)[4] to be used. In light of this, it is necessary to initiate a full and frank discussion about the possibility of adopting offensive methods in cyberspace.

Only by blending NATO's and the EU's distinct characteristics and competences can multi-faceted challenges posed by hybrid threats be effectively countered. To this end, it is necessary to first understand the nature of threats in order to come up with a common response that is aligned to them. The opportunities for cooperation presented herein are merely proposals which, of course, can be further expanded.

Apart from a major shift in the perception of security, hybrid threats also require the existing instruments to be adapted to new circumstances as well as new operational methods and solid cooperation mechanisms to be developed.

On the one hand, it is an enormous challenge; on the other hand, it is an unmissable opportunity for the Alliance and its partners to undertake innovative actions to effectively assure security.

4 This approach also applies to the U.S. crisis response doctrine.

Hybrid Warfare – a Challenge to NATO's Adaptation to Contemporary Security Environment

Mateusz Krupczyński

NATO in the new security environment

The geostrategic shift of power increased its speed constraining the North Atlantic Treaty Organization to adapt its capabilities. Instability is spreading from the Maghreb region throughout the Middle East to the Eastern Europe. In North Africa and the Middle East religious fanaticism escalates across regions. Syria and Libya are failed states providing space for terrorist groups such as Daesh (ISIS) to increase their presence and intimidate people. However, there is also an increase of non-military operations that pose a serious threat to the Alliance – cyberattacks.

In Eastern Europe, Russia continues its aggressive campaign, unveiling its true ambitions and proving that the Georgian-Russian war was not a one-off case. Russia's annexation of the Crimean Peninsula using "little green men" along with a continuous support to rebel groups in the eastern part of Ukraine, Donbas, raised serious concerns in Brussels and among the member states of the Eastern Flank of NATO in particular. NATO-Russia relations have frozen, leaving no room for further cooperation.

Russian interference in Ukraine was conducted by employing hybrid warfare tactics. The hybrid intervention carried out by Moscow included non-military and military elements, using both soft power and hard power. Soft power in Russian understanding is intended to influence or destabilize states by conducting non-military actions, such as cyberattacks or information warfare. Anti-Western propaganda on TV, radio and in newspapers is one of many tools that Russia uses in Ukraine. To destabilize the situation on the ground, the Kremlin used its cyber groups to conduct cyberattacks against Ukraine's critical infrastructure. It is a great example of using cyberspace in parallel to military action. It was clearly part of a wider strategy that enabled Russians to mastermind a grand military operation in Ukraine. James Wirtz observes that "Russia seems to have devised a way to integrate cyber warfare into grand strategy."[1]

1 Wirtz, J., *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*, [in:] Geers, K., *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn 2015, CCDCOE, p.31.

Cyberattacks against critical infrastructure as a threat to NATO

To protect its networks, NATO has developed its cybersecurity policy in accordance **with national cyber strategies**. In Wales, the heads of the states endorsed an already approved Enhanced Cyber Defence Policy, which was a firm step towards a more comprehensive cybersecurity policy. At the 2014 Wales Summit, NATO member states recognized that "international law applies to cyberspace, and that cyber defence is a part of NATO's core task of collective defence."[2] They also stated that Article 5 of the North Atlantic Treaty Organization on collective self-defence "can be invoked in case of a cyber attack with effects comparable to those of a conventional armed attack"[3]; however, the Alliance failed to set detailed criteria for triggering Article 5 in case of a cyberattack. As a result, decisions will be made on a case-by-case basis, which might be "problematic" as far as reaching a consensus at the North Atlantic Council (NAC) is concerned.

The Wales Declaration clearly underlines that NATO's main responsibility is to protect its own networks, including those critical for NATO missions within its member countries. However, with the cyberattacks targeting critical infrastructure on the rise, the Alliance leaders should consider **establishing cross-national mechanisms to increase deterrence**. The latest cyber incidents have clearly shown that there is a tendency to conduct cyberattacks against critical infrastructure in parallel to military operations, most notably against power grids and telecommunications systems.

Cyberattacks against critical infrastructure cause a serious threat to the security of the Alliance. According to the Enterprise Strategy Group's report on the United States, 68 percent of critical infrastructure companies in the United States experienced security incidents over the last two years.[4] Moreover, 36 percent of the critical infrastructure companies stated that cyber incidents caused a disruption in critical operations. Additionally, 36 percent of the critical infrastructure companies reported that cyberattacks resulted in temporary unavailability of critical IT systems. Those disruptions included airline reservation systems, hospital information systems, or SCADA systems[5] and apply only to the United States. This research clearly underlines that companies owning critical infrastructure are under constant threat from cyberattacks.

Russian cyberspace operations in Ukraine

It is unimaginable that Russia could conduct military action against the United States parallel to cyberattacks unleashed against Georgia or Ukraine; however, such a scenario could materialise on NATO's Eastern Flank by striking critical infrastructure prior to a military operation.

2 NATO (2014) *Wales Summit Declaration*, http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease (access: 15.10.2015).

3 Healey, J., and Jordan, T.,K., (2014) *NATO Cyber Capabilities: Yesterday, Today, and Tomorrow* http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf (access: 10.12.2015).

4 Gahm J., Lundell B., and Olstik J., (2015) Cyber Supply Chain Security Revisited, http://www.esg-global.com/research-reports/cyber-supply-chain-security-revisited/ (access: 25.11.2015).

5 Ibidem.

The Russian-Ukrainian conflict had also been escalated in cyberspace by cyber groups such as CyberBerkrut or Sandworm. A number of attacks in cyberspace were registered during the Euromaidan protests, after the Duma's approval of the use of military force in Crimea. Cyberattacks continue to be registered, causing blackouts and disruption of telecommunications systems.

It started with cyberattacks against mobile phone infrastructure originating in the Crimean Peninsula. The attacks also affected the mobile phones of members of the Ukrainian Parliament. The attackers used equipment installed within Ukrtelecom networks located in Crimea.[6] The equipment was blocking telecommunications system, preventing the Ukrainian officials from communicating information about the situation in the country. Most of the communication systems in Ukraine were unprepared for such an attack, which exposed their vulnerability to cyberattacks and easiness to block information flow.

Russian forces targeted Internet Exchange Point (IXP) and Internet infrastructure.[7] Russia's green men seized offices of a telecommunications service provider, cutting off the Internet and mobile infrastructure. Russian troops isolated the region, leaving it without communications capabilities. Furthermore, Russian vessels, placed in the port at Sevastopol, were fitted with jamming equipment in order to block radio communications, leaving Ukrainian forces without communications with their command. The Peninsula also experienced Distributed Denial-of-Service (DDoS) attacks against government websites. Government, banking and media websites were hit by DDoS attacks carried out by the Kremlin-sponsored cyber hacktivist groups such as *The Dukes*.[8]

Moreover, there was a rise of malware callbacks in cyberspace. According to the FireEye report, approximately 30 million of callback messages were sent back from intercepted computers, allowing hackers to control them remotely. Interestingly, the culmination of malware callbacks could be observed when visa bans were imposed on Russian officials, prior to the annexation of Crimea. Allowing unknown parties to remotely control computers may result in weakened defensive capabilities of the Alliance.

The most recognized cyber tool, *Snake,* was used in Ukraine for a large-scale espionage. According to BAE Systems' report, *Snake* malware[9] had Russian origins and was found under the name of *Uroburos* which relates to Greek mythology.[10] *Snake* penetrated the Ukrainian government web systems collecting data and forwarding it to Moscow. This prelude to the subsequent kinetic operation leaves no doubt that Russia had adopted similar, if not the same strategy, during the war in Georgia, blocking government websites and the Internet in the country, just like in Ukraine.

6 Wirtz, J., *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*, [in:] Geers, K., Cyber War in Perspective: Russian Aggression against Ukraine, Tallinn 2015, CCDCOE, p.31.

7 Geers, K., *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn, CCDCOE, p.31.

8 F-secure Labs Threat Intelligence, (2015), The Dukes. 7 years of Russian cyberespionage TLP: Whitepaper, https://www.fsecure.com/documents/996508/1030745/dukes_whitepaper.pdf (access: 24.01.2016), pp.26-27.

9 BAE Systems (2015) Snake Campaign-Cyber Espionage Toolkit, London, p.5.

10 Paganini, P., (2014) Crimea – The Russian Cyber Strategy to Hit Ukraine, http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/ (access: 17.12.2015).

On 23 December 2015, electric power grids were subject to cyberattacks in the western region of Ivan-Frankivsk in Ukraine, leaving thousands of people without electricity. Local media informed that the power grid centres were hacked causing blackouts.[11] *BlackEnergy* Trojan was used as a cyber weapon against the electric substations.

The BlackEnergy malware overwrote and deleted system files in the power station.[12] It turned out that the malware was "dormant" within the system for a decade, but it could be traced to a Moscow-based hacker group *Sandworm*, associated with the Russian government.[13] Hackers used a highly destructive variant of the *BlackEnergy* malware to compromise the systems at three regional power grids in Ukraine. The *BlackEnergy* malware was confirmed by the Security Service of Ukraine. According to SBU's report, the cyberattack was accompanied by a number of phone calls to technical support, suggesting a diversified action resulting in a denial-of-service attack.[14] The *BlackEnergy* included *KillDisk* with a capability of destroying over 3,500 different types of files and rendering machines unbootable.[15]

Released in 2014, ESET report[16] clearly states that the malware targeted around 100 organisations in public and private sectors in Poland and Ukraine, while the F-Secure company claims that there were also attacks using *BlackEnergy* against targets in Brussels such as the European Parliament and the European Commission.[17] The evidence gathered by the F-Systems experts corroborates the fact that this cyber espionage was attributed to *ComsicDuke* which has links with *MindDuke* and *OnionDuke Advanced Persistent Threat* campaigns.[18] All these campaigns are products of state-sponsored Russian cyber groups which develop their capabilities under the sponsorship of the Russian government.

NATO's response to the increasing number of cyberattacks

Since 2008, NATO has undertaken several actions in order to adapt to cybersecurity challenges by approving and implementing a cyber defence policy. At the 2014 Wales Summit, NATO members endorsed a new enhanced policy and action plan to adapt to new challenges to maintain a robust cyberdefence.

11 Paganini, P., (2016), Black Energy Used as a Cyber Weapon Against Ukrainian Critical Infrastructure, http://resources.infosecinstitute.com/blackenergy-used-as-a-cyber-weapon-against-ukrainian-critical-infrastructure/ (access: 13.01.2016).

12 Burgess, M., (2016) Hackers cause electricity 'blackout' in Ukraine, http://www.wired.co.uk/news/archive/2016-01/05/cyberattack-power-electricity-ukraine (access: 10.01.2016).

13 Bumgarner J., (2014) A Cyber History of the Ukraine Conflict, http://www.darkreading.com/attacks-breaches/a-cyber-history-of-the-ukraine-conflict/d/d-id/1127892 (access: 15.05.2014).

14 Tomkiw, L., (2016) Did Russia Kill Ukraine's Electricity? Cyberattack Linked to Power Outage Has Global Implications, http://www.ibtimes.com/did-russia-kill-ukraines-electricity-cyberattack-linked-power-outage-has-global-2249900 (access: 10.01.2016).

15 Tomkiw, L., (2016) Did Russia Kill Ukraine's Electricity? Cyberattack Linked to Power Outage Has Global Implications, http://www.ibtimes.com/did-russia-kill-ukraines-electricity-cyberattack-linked-power-outage-has-global-2249900 (access: 10.01.2016).

16 Paganini, P., (2016), Black Energy Used as a Cyber Weapon Against Ukrainian Critical Infrastructure, http://resources.infosecinstitute.com/blackenergy-used-as-a-cyber-weapon-against-ukrainian-critical-infrastructure/ (access: 13.01.2016).

17 Healey, J., and Jordan, T.,K., (2014) NATO Cyber Capabilities: Yesterday, Today, and Tomorrow, http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf (access: 10.12.2015).

18 Zetter, K., (2014), Russian 'Sandworm' Hack Has Been Spying on Foreign Governments for Years, http://www.wired.com/2014/10/russian-sandworm-hack-isight/ (access: 01.02.2016).

Furthermore, one of the most important actions taken by the Alliance was the signing of a Technical Arrangement, aimed at increasing its inter-institutional cooperation with the European Union to protect their networks. NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU) concluded the agreement on cyber defence cooperation.[19] The aim of the Technical Arrangement is to share information and good practices between the two teams in order to enhance the cyber defences of both organisations.

It is important to stress again that NATO's role is to protect its communications and information systems (CIS); therefore, defence and offensive defence capabilities fall within the scope of responsibility of the member states. For this reason, NATO should only support its Allies by providing comprehensive training and information that strengthen cyber capabilities of its members.

Conclusions and recommendations

The Russian-Ukrainian crisis clearly demonstrated the effectiveness of well-deployed *hybrid warfare* tactics by the Russian Federation. It also showed that cyberspace becomes a significant dimension of warfare which can be efficiently used in a military campaign.

The successful use of modern technologies has allowed Russia to exploit the cyber and informational dimension of the civil war in Ukraine. Russia has put strong emphasis on cyberspace as part of its grand military strategy. Cyberattacks, whether aimed at espionage or destruction, are increasing in number and becoming a serious threat to NATO's security. The Ukrainian crisis is a perfect example of that and should inspire the Alliance's leaders to continue their efforts to further strengthen the NATO Enhanced Cyber Defence Policy, and call for the member states to develop their own cyber capabilities.

In light of the above, NATO **should take the following actions**:

1. Foster more intense **cyber defence cooperation** among NATO members, international organisations like the European Union, and the private sector. It is important to maintain appropriate levels of preparedness by strengthening both national and cross-border networks and systems. The EU's broader approach to cyber security and NATO's narrowly focused activity in cyber defence are complementary.

2. Establish a ***NATO-EU Counter Hybrid Warfare Group***. The Group would consist of NATO and EU experts working closely with intelligence agencies from the EU and NATO member states to produce analyses and prepare counter measures to cyber threats. Enhanced information exchange would facilitate better detection of incidents and more immediate response to them.

19 NATO, (2016), NATO and the European Union enhance cyber defence cooperation, http://www.nato.int/cps/en/natohq/news_127836.htm (access: 30.04.2016).

3. Increase the number of cyber **training programs and exercises** in order to practise and evaluate collective training of staff, units and forces to enable them to work together effectively.

4. Improve strategic **communication**. NATO does not carry out information campaigns (*propaganda)*; however, it should establish mechanisms for immediate response to adversarial propaganda (e.g., Russia's disinformation activities). The Alliance should be capable of countering disinformation with accurate facts and figures.

Information Warfare in Cyber Sphere and NATO's Prevention Capabilities

Michał Matyasik, Ph.D.
Jagiellonian University

Designed to influence political or military decision makers and information-dependent processes, information operations (INFO OPS) have been utilized by countries since the very beginning of their engagement in international relations. Composed of such psychological warfare techniques as black propaganda, false narration, denial, misguidance, and deception, these types of information operations constituted the core of all military psychological operations (PSYOPS) and, to some extent, political activities as well. In various times and different conflicts, they had to evolve and adapt to altering circumstances, but one crucial aspect remained unchanged – the growing importance of such operations and activities. In contemporary conflicts, victory will not be evaluated by the number of eliminated enemies, but by the population affected, whose perception will determine who the winner is and who has lost the war.[1]

We should also be aware that the capability of information operations to affect targeted audiences has increased dramatically in the past few decades. It is beyond any discussion that a major platform to distribute such messages is still the traditional media such as TV, radio, and newspapers. However, with a rapid development of the Internet and social media in particular, information warfare capability has been elevated to another level. A rapid spread of information through the Internet, together with a considerable low cost of such operations and easiness to reach a specific target audience (e.g. young people, minorities, and other groups vulnerable to radicalization) demand a different and more flexible approach to information warfare and cyber security. A combination of traditional media and the Internet as a new channel of communication has set contemporary conflicts and international security in a categorically different environment. Therefore, it is of utmost importance that NATO and other countries create capabilities (including proper procedures and institutions) that could be utilized to guide and accurately execute information operations in support of military activities as well as to counter hostile undertakings in the Internet.

In the past few years NATO has acknowledged the importance of strategic communication and the need for further development of its capabilities in terms of information operations. For

1 See: *ISAF Commander's Counterinsurgency Guidance* (2009) issued by General Stanley McChrystal, http://www.nato.int/isaf/docu/official_texts/counterinsurgency_guidance.pdf (access: 06.01.2016).

instance, in 2011, NATO accepted the Allied Joint Doctrine for Communication and Information Systems (AJP-6) and Defence Ministers approved the second NATO Policy on Cyber Defence. This conceptual development had been accompanied by the creation of specialized institutions and agencies, namely the NATO Cooperative Cyber Defence Centre of Excellence (2008), followed by the NATO Communication and Information Agency (2012) and the NATO Strategic Communication Centre of Excellence (2014).

Even though NATO has developed several appropriate concepts and institutions, considering a more comprehensive perspective, there is still room for improvement in regard to the mechanisms of cooperation and coordination of strategic communication, information warfare and cyber security. The following text will provide a set of recommendations for NATO bodies supported by selected examples of the utilization of the Internet and information activities conducted by the Israeli Defence Forces (Operation Pillar of Defence) and the Russian Armed Forces after the invasion and occupation of Crimea.

Operation Pillar of Defence

In between 14-21 November 2012, the Israeli Defence Forces (IDF) launched another military operation against Hamas. The operation, at its core, was not very different from the previous ones. The manifestation of power, the destruction of crucial infrastructure, and the elimination of high value targets were intended to send a clear message that any hostile activity against Israeli society will not remain without punishment. During eight days of the operation, IDF managed to target around 1500 terrorist sites, including 30 senior Hamas leaders and Islamic Jihadist terrorists, 980 underground rocket launchers, 140 smuggling tunnels and 26 weapons manufacturing and storage facilities.[2]

As mentioned earlier, the operation and its objectives did not differ from other operations undertaken in previous years, but one aspect was elevated to a brand new level of military operations. For the first time ever, IDF decided to utilize social media to a maximum possible extent, launching a comprehensive cyber psychological operation combined with an information campaign. First and foremost, the operation was announced through official IDF channel on Twitter. Second, IDF utilized the most popular social media such as YouTube, Flickr, or Facebook. Simultaneously, similar messages (e.g. "Hamas leaders should surrender themselves" or "What would you do if your society would live under constant terrorist threat?") were broadcast in different social media. Interestingly, while some of the messages were directed against Hamas supporters, others were targeting societies in Western Europe where support for Israeli activities in Palestinian territories decreased in the past few years. Third, selected actions during the operation were broadcast almost live through IDF's YouTube channel. For instance, barely 45 minutes after the elimination of one of the Hamas's leaders – Ahmed Jabari – anyone around the world who had access to the Internet could watch a missile striking a car in which A. Jabari was travelling. Finally, IDF facilitated its own information campaign by encouraging ordinary Internet users to spread IDF's messages (e.g. through a social media game on Facebook "IDF Ranks" where the most active players could acquire higher "military" ranks for resending messages). Acting this way, IDF decided to exploit a great number of Internet users and supporters of IDF operations.

It is not an easy task to evaluate the overall efficiency and effectiveness of the operation since it was conducted in the information domain. Nevertheless, the analysis of the operation and its scientific evaluation provides a basis for several important conclusions. First of all, the operation in the cyber domain was of a multidimensional character, and was organized and coordinated by the military forces. Second, such operationalization and utilization of social media is beneficial as it helps to reduce financial costs of PSYOPS operations and decrease the unnecessary risk (no need for boots on the ground to spread the message). Third, it is much easier, with carefully drafted messages, to reach a specific audience (e.g. local inhabitants, young people, or belligerents). Last, the utilization of social media in CYBERPSYOPS poses a significant risk that the opponent can exploit the same capabilities in order to counter information operations. In fact, it was exactly what Hamas did by exploiting social media to mirror IDF activities.

Russia's information war

It is beyond any doubt that Russia and its information warfare concept constitutes the greatest challenge to NATO. The origins of Russia's information warfare doctrine dates back to the First Chechen War of 1994-1996. Back then, Russian decision makers were astonished by the amount and scale of criticism expressed by the Russian and international media. Almost on a daily basis, people around the world could watch war videos and images as well as listen to stories of atrocities that happened during the violent conflict in Chechnya. An uncontrolled flow of information produced a narrative of civilian suffering, Chechens fighting against oppressive forces and Russians bearing the blame for the disastrous situation. That experience helped Russian politicians and military representatives understand the importance of framing messages according to desired political objectives and highlighted the specific role of both traditional and social media in military operations.

In 2011, the Russian government launched a landmark document entitled *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*. The document stated that one of objectives of information warfare should be to undermine the political, economic and social system of the targeted state. It could be achieved through massive brainwashing of the population, aimed at destabilizing the society and the state, and forcing the state to make decisions in the interest of the confronting party. Moreover, the document highlighted that the defensive potential of the Russian Federation significantly depended on the efficient activities of the Armed Forces in the information domain.

However, the first time when the information warfare was employed by the Russian government to an incomparable extent and in a comprehensive manner was during the occupation of Crimea. The information operation had been initiated a year before the first Russian soldier set foot in Crimea. Having a multidimensional character, the campaign made use of Russian TV stations (Russia Today, Russia 1 and others) as well as the Internet, unfolding both deceptive

2 More about Operation Pillar of Defence see: https://www.idfblog.com/about-the-idf/history-of-the-idf/2012-operation-pillar-of-defense/.

and misleading narrative.[3] The conflict between Ukraine and Russia was presented as a struggle between the Orthodox Church conservative ethics and "spoiled" Western European values. Although Russians and Ukrainians were described as one nation, the former were supposed to be treated in a privileged manner. On several occasions Ukraine was also described as an artificial state, which was the argument behind Russia claiming its full right to Crimea. Moreover, according to Russian propaganda, the real reason behind the conflict was the covert activity of the U.S. and the EU states which aimed to exploit the grievances and differences between the two Slavic nations. While the effectiveness of traditional media was limited to Russian-speaking communities, the Internet allowed messages to be spread beyond any borders and with no limitations, thus constituting the biggest challenge for counter-information operations. Typically, a single message, no matter how false and irrational, was immediately multiplied in several social media.

Conclusions and recommendations

1. Information campaigns should constitute a core objective for every NATO operation. They should definitely be more oriented towards cyber sphere since it provides the most effective and the fastest means of communication.

2. Both military and civilian structures of NATO should engage in such campaigns as the political and military cohesion of messages is crucial for their effectiveness. According to a doctrine of Comprehensive Approach, it would be advisable to involve non-governmental actors in the designing process as well (NGOs, mass media, those who have capabilities to influence audiences through cyber activities).

3. Due to a rapidly changing environment in information sphere, NATO should develop a dynamic 24/7 coordination procedure for information campaigns, especially in the cyber domain.

4. Optionally, such a procedure could be founded on the Military Staff Committee Operation Division supported by the analytic capabilities of the scientific community and the NATO Cooperation Cyber Defence Centre of Excellence or the NATO Strategic Communication Centre of Excellence.

5. Finally, based on recent observations of Russia's information campaigns in relation to Crimea and the Eastern Ukraine conflict, it is beyond any doubt that such information campaigns preceded kinetic operations by at least one year. It would be advisable for NATO to consider a possibility for launching mass information campaigns in a similar timeframe manner in the future.

3 More about Russia's information warfare can be found here: *„Analysis of Russia's information campaign against Ukraine. Executive summary"* prepared by NATO Strategic Communication Centre of Excellence in 2015.

Mechanisms for Strengthening Cooperation between NATO & its Private Sector Partners (NATO Industry Cyber Partnership)

Tomasz Romanowski

Cyberattacks are really cheap. Regardless of whether the goal is to disrupt the enemy nuclear facility or commit espionage, using conventional means such as jet fighters and spies will almost always be more expensive. By contrast, a team of talented coders with the knowledge of Python, C++, Assembler, and SCADA can do just as good, and does not require an army of informants or a manufacturing assembly line. Hence the equation is simple: since cyberattacks are cheaper, the number of them will only rise. In light of this fact, NATO will not be able to fully secure its cyberspace and infrastructure by itself – it will need partners to do that.

The need for cooperation with private actors arises from economical and utilitarian reasons. Despite its military origins (the predecessor of today's Internet was ARPANET), the main drive behind the Internet success and its exponential growth nowadays is private industry and companies. True, nation states create regulations that allow service providers and companies to operate their services, but at the end of the day it is people behind such enterprises as Cisco, Microsoft and Google who shape the face of the Internet beyond borders and national limitations (mostly). The necessity for cooperation is, therefore, born out of the realization that only by working with companies that create cyberspace and its environment one can fully understand how to protect their network and provide complex cybersecurity. It is especially important for large-scale organisations like the Alliance. For NATO, such cooperation should come more naturally than for an average country given its international character and the fact that both enterprises and the Alliance work with many, often the same, institutions and people.

A chance to increase NATO Cybersecurity capabilities in cooperation with outside partners is the Framework For Collaborative Interaction (FFCI). Developed by NATO Allied Command Transformation (ACT), the programme aims to foster partnerships with the representatives of Academia and Industry. By initiating the programme, the Alliance has acknowledged that it lacks requisite knowledge required to provide full security to its members and that it tries to leverage the experience of its industrial and academic partners for mutual benefit of all parties involved.[1]

1 http://www.act.nato.int/ffci.

Under FFCI, NATO invites potential partners to collaborate in order to increase the overall efficiency of the Alliance as well as to study and challenge contemporary problems and create solutions to them. In this way, the Alliance gains access to up-to-date knowledge and technologies while companies have a chance to sell products and data as well as influence the development of cyber partnerships with the world's largest military alliance.

To that end, however, NATO must know what it actually needs from its potential partners. During the last edition of the annual Chiefs of Transformation Conference hosted by Supreme Allied Commander Transformation in Norfolk, Virginia, the attendants recognised that, when it comes to cybersecurity, NATO must highlight "the importance of building relationships with industry to explore the Cyber challenges, and leverage the potential technological breakthroughs in this domain. This will include developing Response Capability, Defence Capability, Information Assurance & Sharing, and Training."[2]

By partnering with industry, the Alliance may especially benefit from:

1. Threat Intelligence Solutions – although national agencies are quite proficient in mapping incoming threats, they may lack knowledge on the creation of very large networks, so-called honeypots, required for constant monitoring of attack methods.
   NATO may strongly benefit from cooperation with threat intelligence and antivirus software companies that possess one of the most complex and extensive threat intelligence as well as real time attacks mapping solutions.
   Creating a NATO-wide network of interconnected honeypots enables NATO CERT teams to receive accurate information and data regarding possible DDOS attacks or attempts of systems foot printing (services enumeration, ports scanning, ping sweeps). And as the representatives of NATO itself have noted, sophisticated attacks must be countered with even more sophisticated defence and means to stop any intruders from penetrating NATO systems.[3]
   Companies specialising in threat intelligence and antivirus software are natural partners for big military organizations, and all parties can reap mutual gains from sharing both experience and threat intelligence software. Such cooperation can take place as a part of the NATO Cyber Industry Partnership (NCIP) Smart Defence project – Cyber Information and Incident Coordination System (CIICS) which aims to detect incidents in real time and share information about them.[4]

2. Open Source Intelligence – Social Media cooperation
   Some may ask: What does a military organization have in common with social media companies when it comes to security? The answer is quite simple – there was a reason why Facebook, among other internet companies, was part of the NSA PRISM program.[5]
   Cooperation and information exchange with social media giants does not correspond directly to cybersecurity; however, it does apply to security itself. Facebook and Twitter process tremendous amounts of data, especially the unseen one (private correspondence, acquaintances, contacts), which may have great intelligence value to NATO members and its partners. Creating a platform for cooperation between NATO, national intelligence agencies, and social media companies, may drastically improve the process of gathering intelligence about potential suspects who may pose a direct threat to the security of NATO members or deliver important information about incoming dangers. Since threat actors do not always avoid social media of any kind, a fast and coordinated exchange of social media data about suspects may prove invaluable for maintaining NATO's security. Even information such as the EXIF data (metadata embedded within pictures, such as GPS coordinates, date and time when a picture was taken, the camera model etc.) can be a useful source of intelligence.[6]
   In such a case, NATO may further encourage cooperation between national intelligence agencies and social media companies, working on the acquisition of important social media data and its immediate distribution among the agencies. By doing this, the Alliance can kill two birds with one stone: obtain access to social media intelligence and solve the problem of intelligence agencies being reluctant to share information, which led in part to the unfortunate November 2015 terrorist attacks in Paris.[7]
   It is hoped that the Alliance Ground Surveillance system, which NATO is acquiring, may greatly help in this task.

3. If necessary, Industry can provide NATO members with access to both defensive and offensive capabilities in cyberspace. The case of Hacking Team, an IT company, reveals that governmental bodies are interested in acquiring means to successfully infiltrate suspected systems and provide cyber surveillance on targets.[8] In the future, NATO may also wish to possess software capable of effective taking down Command and Control Botnet Servers, thus enabling the Alliance to successfully stop them from launching further attacks on NATO's infrastructure. Very few companies can provide such solutions; nonetheless, they do exist and their services may be of use to the Alliance. Contemporary NATO policies such as the Cyber Defence Policy and the Wales Summit Declaration show that, at least for now, the Alliance is reluctant to resort to such means, but it is always good to have a deep knowledge of offensive security in case a sudden change within the current political environment should occur.

Still, there is one key question that remains unanswered: is NATO actually capable of a successful implementation of necessary mechanisms to commence effective cooperation with industry?

As the 2014 NATO Industry Forum has shown, there are several challenges that impede the Alliance's progress in this area.[9]

2 Langeland H., *Chiefs of Transformation Conference 2015 focussed on Strategic Innovation and Sustained Transformation*, 2015, http://www.act.nato.int/chiefs-of-transformation-conference-2015-focussed-on-strategic-innovation-and-sustained-transformation (access: 13.01.2016).

3 *Changing the game: The art of deceiving sophisticated attackers*, Nikos Virvilis, Oscar Serrano Serrano, Bart Vanautgaerden, 2014, https://ccdcoe.org/cycon/2014/proceedings/d2r2s6_serrano.pdf (access: January 2016).

4 http://www.nicp.nato.int/nato-tests-cyber-alerting-tool/index.html NATO tests cyber alerting tool.

5 *The NSA paid Silicon Valley millions to spy on taxpayers*, Brian Fung, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/23/the-nsa-paid-google-and-facebook-millions-to-spy-on-taxpayers/ (access: January 2016).

6 *US Air Force Targets and Destroys ISIS HQ Building Using Social Media*, Mike Hsoffman, 2015, http://defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media/ (access: January 2016).

7 *France, Belgium to push intelligence sharing after Paris attacks*, AFP, 2015, http://www.timesofisrael.com/france-belgium-to-push-intelligence-sharing-after-paris-attacks/ (access: January 2016).

8 Hacking Team clients by country http://www.engadget.com/gallery/hacking-team-clients-by-country/# (access: January 2016).

9 https://www.act.nato.int (access: January 2015).

1. When it comes to Industry, some politicians and decision makers tend to get very suspicious, which does not help NATO's cause. Rather than perceive them as a group of lobbyist with pockets filled with bribe money for billion dollar military contracts, business and industry representatives should be seen as potential partners. It is especially important considering the fact that cybersecurity projects expenses within NATO are unlikely to be on the same tier as, let's say, ammunition or aircraft contracts, and will necessitate cooperation with external partners to, for example, share costs of new technologies.

2. The NATO Communications and Information Systems Agency must consider the interoperability of cyber projects in the future. As a guardian of IT Security solution implementation within the Alliance, the Agency should make sure that innovations are meeting NATO-wide standards in order to make them easier to apply. The issue was brought up during the NATO Wales Summit in 2014 and should be considered for future projects.[10]

3. Transition from concept to reality – since 2011, Smart Defence has been widely discussed, apparently well thought out, given very intense focus at almost every NATO Summit, and yet not very successful when it comes to its implementation. As of June 2015, NATO was working on 26 international Smart Defence projects. Six of them have already been finished, and although money was saved, it is debatable whether Smart Defence indeed contributed significantly to the speed with which projects were executed. In its current form, Smart Defence may contribute to smaller cybersecurity initiatives undertaken in partnership with Industry, but bigger schemes may take a very long time to implement, making some solutions outdated since advancements in cybersecurity can be quite rapid due to the increasing number of dangers and threat actors emerging in cyberspace.

Conclusions and recommendations

1. As far as cooperation with industry is concerned, for NATO's Smart Defence to bring fast results it should focus on small-scale projects, producing immediate effects required to increase cybersecurity capabilities, with the exception of the NATO Computer Incident Response Capability and Rapid Response Teams. Preferably, the choice of projects should involve investment into Research and Development of new capabilities and technologies which not only respond to already existing threats, but foresee new ones and create solutions to them before they actually emerge. With NATO's recent **Cyber Security Incubator project showing promising results,**[11] it is hoped that the NATO Industry Cyber Partnership can help deliver these capabilities in the near future.

10 https://www.act.nato.int/images/stories/events/2015/nif/nif2015_readahead.pdf NATO – Industry Forum Industry in support of the Alliance Ambitions 2015, https://www.ncia.nato.int/NewsRoom/Pages/150918-Cyber-incubator.aspx NATO boosts cyber cooperation with Industry.

11 https://www.ncia.nato.int/NewsRoom/Pages/150918-Cyber-incubator.aspx NATO boosts cyber cooperation with Industry.

2. With R&D in place, NATO should invest time and effort to determine the exact scope of issues and solutions it requires in order to solve them. The Alliance should develop cybersecurity capabilities in the same way as it enhances its defensive and offensive military capabilities in response to specific external challenges. Once NATO has identified its needs, it should be much easier for Industry to adjust their solutions to the requirements of the Alliance. The cooperation with industry and academia may in fact bring faster and more accurate results.

3. The efforts to foster closer cooperation between NATO and industry have been limited so far to either inviting business and private sector representatives to exercises (Trident Juncture), or to awaiting collaboration proposals from potential partners (Framework for Collaborative Interaction by Allied Command Transformation). However, once NATO has identified specific technical issues or challenges, it should proactively search for and invite partners to tackle them, taking into account its own resources and limitations as well as the capabilities of potential partners to solve these problems. Although widely recognised and respected, NATO is not the only partner for security companies. What NATO needs to consider when confronting challenges in cybersecurity is ICT market growth, driven primarily by the private sector, and estimated to reach a value of USD 170 billion by 2020.

4. In a never ending cyber arm race, NATO must specify its cybersecurity needs, so that its industry partners can meet the Organisation's technical requirements to prepare it for threats of today and tomorrow.

5. Further cybersecurity solutions standardization should follow to increase their interoperability among NATO members.

6. In addition, the Alliance's structures responsible for enhancing industry cooperation should run campaigns addressed to NATO decision makers and aimed at changing their perception of industry from a suspicious client to a partner. Such initiatives can deepen the understanding of benefits this dialogue yields on both sides.

7. NATO should focus its attention not only on responding to today's challenges, but also on working on R&D projects with Industry to predict and face problems that the near future may bring. In order to become again a harbinger of new military and civilian technologies, NATO must step outside its technological comfort. Smart Defence and NATO Industry Cyber Partnership may help to achieve this goal, considering the promising results both initiatives have brought so far.

8. Depending on identified needs, the Alliance should start actively searching for partners in order to significantly increase its operation capabilities in terms of cybersecurity.

Looking Ahead – a Multi-Disciplinary Approach to Cybersecurity Education

Magdalena Szwiec
The Kosciuszko Institute

The emerging hyperconnected world gives an impression that the global community has opened the Pandora's Box of cybersecurity. Public and private sectors alike have to face challenges brought about by an increasingly complex cybersecurity landscape. In order to achieve relative cyberspace safety, the Alliance will have to come up with a new arrangement of responsibilities and authority as well as establish more standardized relations with government institutions, academia, industry, and third parties.

Nevertheless, the current debate about NATO's cybersecurity is missing a bigger picture, namely it fails to address the problem of unfilled positions of cybersecurity specialists. In this context, all parts of the equation share the same interest in educating and training cybersecurity professionals, which requires a consistent framework and a long-term strategy. With this in mind, NATO and its member states should approach this challenge in a more complex manner, mainly by improving cooperation with institutions of higher education, both civil and military, but also by recognising a multidimensional nature of cybersecurity education.

According to the report conducted by one of the leading cybersecurity companies, the facts are straight: a global figure of demand is at one million now and will rise to 6 million by 2019.[1] However, it is important to note that the report focuses chiefly on IT positions. In these circumstances, NATO has to put emphasis on its cooperation with academia to address the problem of shortages in cybersecurity specialist roles.

Naturally, technical programs and courses receive most attention, which indisputably allows for some of the cyberthreats to be addressed. However, IT experts are only capable of finding solutions to technical problems, which does not fulfil the requirements for sufficient management of NATO's safety in cyberspace. Therefore, the focus on "cybersecurity courses" should also be reflected in traditional majors such as law, international relations, economics, management, psychology etc.

1 Morgan S., *"One million Cybersecurity job opening in 2016"* http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#58ea3287d274 (access: 09.05.2016).

In her report *One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat,* Francesca Spidalieri from Pell Center for International Relations and Public Policy evaluates current efforts made by leading educational institutions in the United States to prepare non-technical workforce in both public and private sectors. The report focuses predominantly on several postgraduate courses: Master of Business Administration (MBA), Master of Public Administration (MPA), Master of Public Policy (MPP), Master of International Relations (IR), Master of Laws (LLM), Criminal Justice, and Healthcare Management. The study shows that the interest of distinguished American universities in developing new content for multi-disciplinary cybersecurity programs has increased. However, there is a strong imbalance between the need to educate future generations of leaders about the intricacies of cyberspace and the insignificant role cybersecurity plays in most graduate programs.[2]

Unfortunately, a similar situation occurs within European education systems, where the awareness of the need for developing a multi-disciplinary approach to cybersecurity education remains relatively low. In the recently published report by ENISA *Cybersecurity Education snapshot for workforce development in the EU Network and Information Security (NIS) Platform,* the authors state that *"*(...) there is a lack of differentiation between traditional programmes offering fundamental security related curricula and more versatile cybersecurity programs with multi-disciplinary coverage and multi-faceted training materials". Moreover, when presented with the opportunity to participate in multi-disciplinary programs, students tend to choose social or technical studies.[3]

These findings show that there is an urgent need for changing the culture of cybersecurity education. Developing and improving multi-disciplinary programs is crucial for several reasons. To start with, cyberthreats pose a serious challenge to all elements of states, societies, and economies. The lack of fundamental knowledge about cybersecurity among future decision makers, politicians, lawyers, or managers, will make the Organisation and its allies vulnerable. In comparison to most current leaders, the new generation of stakeholders has to be fully prepared for future challenges. Hence, NATO must evaluate current approaches to education that are essential from the point of view of the Organisation's needs and use its own and national resources to catalyse research and development of good practices and curriculum recommendations.

Within its structures, NATO has launched initiatives and platforms which aim to strengthen cooperation between the Alliance, academia, and industry to address future threats:

- **Framework For Collaborative Interaction (FFCI)**

  Launched by Allied Command Transformation (ACT), NATO's military command responsible for identifying and promoting the development of essential capabilities for future operational needs of the Alliance, FFCI considers countering cyberthreats as one of its priorities. The idea behind the project is to recognize potential risks as early as possible and increase the cost-effectiveness of capability development efforts.[4]

2 Spidalieri F.,*"One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat".*

3 https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/cybersecurity-education-snapshot-for-workforce-development-in-the-eu/view page 4 (access: 22.06.2016).

4 http://www.act.nato.int/ffci (access: 10.05.2016).

In addition to new areas of possible collaboration, this initiative introduces appropriate instruments and tools on several levels (e.g. joint solution development, joint studies, white papers, international discussions etc.). However, it should still be taken as a kind of signpost for future investments in cybersecurity education.

- **Innovation Hub**

  Designed as a platform for expert collaboration, the Innovation Hub brings together students, scholars and cybersecurity professional in order to share their perspectives and generate a better understanding of future challenges.[5]

  Given the fact that the Innovation Hub has not been established with a view to developing specific programs or courses, it should still be used as a source of information and knowledge to meet educational needs of future generations. The Hub could potentially fill the gap in the process of curriculum design at a university level.

- **The Science for Peace and Security Programme (SPS)**

  As a policy tool intended to enhance cooperation and dialogue with various partners (e.g. international organizations, industry, academia, and third parties), the SPS Programme draws on scientific research, innovation, and knowledge exchange to provide funding, expert advice, and support to security-related activities jointly developed by NATO member states and partner countries.[6]

  In 2015, a total of 8 SPS projects were related to cyber: cyberdefence strategies, cyberdefence capabilities in security related to government sectors and cyberdefence cooperation at a regional level.[7] Yet they have failed to remodel the multi-disciplinary approach to cybersecurity education. Similarly to FFCI, the SPS Programme could become NATO's most effective platform, serving as a springboard for developing new study programs and courses.

- **NATO NCI Agency, Europol, and The Hague Security Delta**

  As hosts of the annual International Cyber Security Summer School, they offer students and young professionals a five-day course covering various aspects of cybersecurity. In addition to lectures delivered by the hosts, students have an opportunity to receive lectures from other Dutch and international organizations: Eurojust, the Cooperative Cyber Defence Centre of Excellence, the National Cyber Security Centre, and the European Telecommunications Standards Institute.[8]

5 http://www.act.nato.int/innovationhub (access: 10.05.2016).

6 http://www.nato.int/cps/en/natohq/topics_85373.html (access: 22.05.2016).

7 http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/20160511_SPS-Annual-Report-2015.pdf (access: 23.05.2016).

8 http://www.summerschoolcybersecurity.org/ (access: 26.05.2016).

Although the Summer School does not offer comprehensive cybersecurity courses, it gathers high-level institutions together with the aim to create a more holistic approach to cybersecurity education. The initiative has great potential for establishing suitable study programs and courses within the organizational structures of the hosts.

Non-NATO Platforms For Collaboration and Promotion of The Multi-disciplinary Approach to Cybersecurity

There are several platforms that can serve as examples of initiatives to address the lack of a multi-disciplinary approach to cybersecurity education:

- A Rhode Island Academic Collaboration on Cybersecurity Technology and Policy – the platform spans four recognized American Universities: the University of Rhode Island, Brown University, the U.S. Naval War College, and Bryant University. Launched in 2012, the initiative aims to promote academic collaboration on cybersecurity issues, focusing in particular on cyber threats at the intersection of technology, policy, law, and national strategies. The founders commit themselves to inform each other of courses and degree programs they offer, funded research projects, publications, seminars, and conferences.[9]

  With NATO's support, these types of initiatives could become more effective and correlate with new recommendations developed by top academic institutions, which, in turn, would bring substantial benefits to the Alliance itself.

- The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (USA), is a platform created to catalyse and promote a partnership between government, academia, and the private sector, focused on cybersecurity education, training, and workforce development. The founders want to achieve their mission by facilitating change and innovation, supporting already existing successful programs and bringing leadership and ideas to increase the number of cybersecurity professionals.[10]

  Drawing upon already existing support from the U.S. government, NATO could encourage other member states to develop similar national initiatives, which would most definitely strengthen the market of cybersecurity specialists.

- The Cyber Security Oxford network supports all of the researchers and experts working on cybersecurity at the University of Oxford. The network creates a community to help foster cybersecurity education and research activities across the University. In addition, the CSO network partners with other academic institutions as well as public and private organizations.

  NATO should initiate the development of these types of networks at leading universities in the member states to facilitate the education of leaders, which would considerably increase national cyber capabilities and, as a consequence, also the Alliance's.

9 http://cs.brown.edu/people/jes/Cybersecurity/RI%20Collaboration%20for%20CCTP%20Sept%2013%20FINAL.pdf (access: 09.05.2016).
10 http://csrc.nist.gov/nice/about/strategicplan.html (access: 09.05.2016).

Practical recommendations

- Encourage stronger inter-university collaboration supported by the Alliance and its member states (for example with academic centres for cybersecurity such as the Cyber Security Oxford network) in order to integrate best practices, university curricula and innovative approaches to create dedicated multi-disciplinary studies programs for future cybersecurity experts and, as a consequence, considerably improve qualifications of future cybersecurity specialist at national and NATO's levels alike.

- Build a network of internship opportunities available at NATO, other international organizations, industry, and academia, providing mentoring programs to talented students and graduates, and at the same time making the internships more accessible.

- Engage "cyber veterans" in training and academic work to promote knowledge sharing of systems and solutions to aid the understanding of NATO's needs, standards, and regulations.

- Strengthen cooperation with the EU to avoid duplication of effort (for example with the already well-established educational and alumni programs such as Erasmus, Erasmus Mundus, Erasmus +).[11]

Conclusions

Providing cyber-strategic leaders with high quality cybersecurity education will enable them to gain essential knowledge to govern and manage future challenges. Moreover, it will improve the quality of actions undertaken by international organizations, both governmental and non-governmental, transnational corporations, national governments, societies etc. Equipped with practical and theoretical skills, the alumni of multi-disciplinary studies would become genuine game changers with great potential to deliver safe cyberspace. NATO's future security depends on its ability to train and educate next generations of cybersecurity professionals. With the ongoing geopolitical tensions, evolving hybrid threats and omnipresent digitalization, no room exists for shortcuts or compromises. NATO and its member states have to take concrete action, carefully planned and scheduled, with cautiously designed framework. Although it will require time and funding, there is no other way to deliver safety in the future. The so-called New Normal has to become Just Normal.

11 http://ec.europa.eu/programmes/erasmus-plus/node_en (access: 13.05.2016).

Authors

Wiesław Goździewicz, CDR

(Polish Navy), graduated from the Faculty of Law and Administration of the University of Gdańsk in 2002. Subsequently, he joined the Armed Forces and started his military career as a junior legal officer at 43rd Naval Airbase in Gdynia. He also served in the Public International Law Division of the Legal Department of the Ministry of National Defence. In October 2009, he was appointed Legal Advisor to the Joint Force Training Centre in Bydgoszcz. Apart from giving legal advice related to the daily functioning of the Centre, his role involves providing training on the practicalities of the application of International Humanitarian Law (IHL)and legal aspects of military operations, from conventional warfare to space and cyber operations. CDR Goździewicz has given lectures as a guest speaker at the National Defence Academy in Warsaw, Naval Academy in Gdynia, Kazimierz Wielki University in Bydgoszcz and NATO School, Oberammergau. He is the author of several articles and other publications on the application of IHL in contemporary military operations.

Joanna Kulesza, Ph.D.

is Assistant Professor of international public law at the University of Lodz, Poland. She is the author of five monographs and over fifty other peer-reviewed publications on various aspects of international law and new technologies, including "International Internet Law" (Routledge 2012) and "Due Diligence in International Law" (BRILL 2016, forthcoming). She is an expert on human rights online for the Council of Europe and the European Commission. Dr. Kulesza is also the Membership Committee Chair of the Global Internet Governance Academic Network (GigaNet). She has been a visiting professor with the Oxford Internet Institute, Norwegian Research Center for Computers and Law, Westfälische Wilhelms Universität Münster and Justus-Liebig-Universität Gießen. She was a post-doctoral researcher at the University of Cambridge and Ludwig-Maximilians-Universität München, a scholar of the Robert Bosch Stiftung, Polish Ministry of Foreign Affairs and the Foundation for Polish Science. She worked for the European Parliament and for the Polish Ministry of Foreign Affairs. Her main research interests cover human rights, cybersecurity, and Internet governance.

Mateusz Krupczyński

holds a Master's degree in International Relations and Politics from the University of Dundee, and a Master's degree in Global Security from Keele University. Mr. Krupczyński is also a graduate of the Academy of Young Diplomats at the European Academy of Diplomacy and Visegrad School of Political Studies. He was awarded 2016 Future NATO Fellowship at the Atlantic Council as well as received Alumnus of the Year 2015 award from the European Academy of Diplomacy and New Security Leader award from the Warsaw Security Forum. Currently, Mr. Krupczyński is

a Specialist at the National Centre for Strategic Studies. Previously, he worked at the Ministry of Economy, NATO Investment Management Office, and the Chancellery of the Polish Prime Minister. His main areas of interests span a wide range of topics including transatlantic security, cyber warfare, Polish foreign and security policy.

Miron Lakomy Ph.D.

is Assistant Professor at the Department of International Relations, University of Silesia (Katowice, Poland) and Coordinator of National and International Security studies at the Faculty of Social Sciences, University of Silesia. Holds a MA, Ph.D. and Post-Doctoral Degree in Political Sciences (specialization: International Relations, International Security) from the University of Silesia. A former scholarship holder from the University of Cambridge (Corbridge Trust program, 2011), Dr. Lakomy completed research grant on the role of cyberspace in the Canadian security policy under the Faculty Research Program from the International Council for Canadian Studies. He participated in the Erasmus LLP Program giving lectures in France and Italy. His current research interests focus on cybersecurity problems (cyberwarfare, cyberterrorism, and cyberjihadism), military conflicts and the security of France and Poland.

Michał Matyasik Ph.D.

is Assistant Professor at the Institute of Political Science and International Relations of the Jagiellonian University in Cracow, Poland. He was awarded a Ph.D. degree in Political Science in 2006 and a Master's degree in Law in 2003. He specialises in international relations and military science. Having participated in a number of military-oriented training programs, Dr. Matyasik was deployed to Afghanistan as a CIMIC functional specialist with a POL-ISAF contingent in 2012/13. His area of expertise is associated with non-kinetic military operations and counter-insurgency.

Kate Miller

is a research and project assistant with the Cyber Security Project at the Harvard Kennedy School's Belfer Center for Science and International Affairs. Previously, she was a student associate with the Center's Project on Managing the Atom and interned with the U.S. State Department, contributing to reporting on European affairs. Kate Miller received her Master's degree in International Security and her Bachelor's degree in International Relations and French. In her research, she focuses on transatlantic security.

Tomasz Romanowski

is an IT Security Consultant at Comarch, expert of the Kościuszko Institute, former security journalist and analyst. Mr. Romanowski graduated in Political Science from the Jagiellonian University in Cracow. He also completed Information Security Postgraduate Studies in University of Technology in Cracow and was an attendant of the Erasmus program in Sciences Po in Paris. Mr. Romanowski is a member of the board of the Polish Transhumanist Association. He enjoys penetration testing, good food and watching astrophysics videos on YouTube.

Professor Ryszard Szpyra

is professor of Social Sciences and the head of doctoral studies at the Polish National Defence University. He has held numerous teaching and academic positions at the NDU. He has been a member of the Executive Academic Board of the EU European Security and Defence College since 2010 and a member of the International Council of the International Society of Military Sciences since 2012. His experience, spanning three decades, includes working on military and security issues, which has given him a deep understanding of problems related to military security, intelligence, information warfare and cybersecurity.

Magdalena Szwiec

is a CYBERSEC Project Manager at the Kosciuszko Institute. She graduated with a Bachelor's degree in National Security and a Master's degree in International Relations with a special focus on Israel's domestic and foreign policy. She was a scholarship holder from Tel Aviv University, Oslo University and the Peace Research Institute in Oslo. Ms Szwiec studied European Studies at Siena University and worked as an intern at the Embassy of Republic of Poland in Dublin.

Joanna Świątkowska Ph.D.

is the Programme Director of the European Cybersecurity Forum, the Chief Editor of the European Cybersecurity Journal and Senior Research Fellow of the Kosciuszko Institute. She is a member of the Advisory Group for Cybersecurity of the Republic of Poland working within the Polish Presidential National Bureau of Security (NBS). She has been involved in numerous high-profile national and international cybersecurity initiatives, including the Sino-European Cyber Dialogue held in Geneva and Beijing in 2014. She cooperates with Polish public institutions such as NBS on a regular basis. In the framework of the National Forum of Security organized by NBS, she made a significant contribution to the cyber doctrine of Poland. She also advised the Supreme Audit Office in terms of cybersecurity control in Poland. Joanna Świątkowska is the author of numerous articles, reports and analyses concerning cybersecurity. She often speaks at national and international conferences and seminars on a wide range of cybersecurity topics. In 2016, she took part in the U.S. Department of State's International Visitor Leadership Programme (IVLP) on Cybersecurity and Government Interoperability. Joanna Świątkowska holds a Ph.D. in Political Science.

PUBLISHER

The Kosciuszko Institute is an independent, non-governmental research institute that was founded in 2000 as a non-profit organisation. The institute drafts expert reports and policy recommendations for European and Polish decision makers. The Kosciuszko Institute strives to be a leader of positive change, to create and to promote the best solutions, not only for Poland, but also for Europe and neighboring states which are in the process of building states based on the rule of law, civil society, and a free market economy. Studies prepared by the institute have not only served as the basis for significant legislative reforms but also as a factual support for the ongoing activities of strategic decision makers.

Since 2011, the Kosciuszko Institute is a leading research in the framework of the project "Target: Cybersecurity", which was a response to the growing need for actions towards assuring the safe functioning of states, commercial entities and citizens in cyberspace. The Kosciuszko Institute cooperates in cyber security issues with the institutions and government in Poland: the National Security Office (BBN), the Government Security Centre (RCB), the Supreme Audit Office (NIK) and the Ministry of Digital Affairs. KI experts are daily guests in national media outlets providing insights and opinions related to cybersecurity.

PARTNER

Polish Armaments Group is the leader of the defence industry

Polish Armaments Group is the leader of the Polish industry and one of the largest defence groups in Europe. It concentrates more than 60 companies (of defence, shipyard, new technologies sectors), achieving annual revenue of circa PLN 5 billion. By making use of the technology Polonisation potential, close cooperation with the Polish scientists and focus on the research & development process, PGZ offers innovative products which enhance Poland's security.

PGZ's priority is broad participation of the Polish defence industry in the programmes of the Technical Modernization Plan of the Polish Armed Forces in order to enhance Poland's defensive potential. The recently signed contract on modernization of LEOPARD tanks can serve as an example here.

PGZ offers, among others: very short range air defence system including POPRAD system and SOŁA radar; GROM mobile anti-aircraft missile set; E-310 unmanned aircraft system; ROSOMAK armoured personnel carrier; artillery system with KRAB self-propelled howitzer; and individual soldier equipment with BERYL rifles.

Furthermore, PGZhas expertise to design, construct and equip vessels. In addition, PGZ modernizes and maintains vehicles, airplanes, helicopters, vessels,including post-Soviet equipment. In the coming years, Polish Armaments Group will develop aerospace and satellite technologies as well as cyber technologies. Moreover, PGZ expands its expertise by cooperating with numerous scientific centres and research & development units. The company also intends to develop production for civil purposes.

When it comes to cyber defence policy the North Atlantic Alliance has come a long way. But NATO's journey towards cybersecurity has not come to an end yet; on the contrary, it will take a lot of effort and further bold decisions to move closer towards achieving the goal. In this report, the Kosciuszko Institute invited authors to take up the most pressing cybersecurity challenges facing the Alliance. We believe that our recommendations will prove useful for shaping future decisions considering NATO's engagement in cybersecurity.

Partner

PGZ
POLISH ARMAMENTS GROUP

ISBN: 978-83-63712-29-7

THE KOSCIUSZKO INSTITUTE