RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE STUDIES

Analysis

Improving Cyber Security: NATO and the EU

Piret Pernik

September 2014

Piret Pernik

ISSN 2228-2076

International Centre for Defence Studies
Toom-Rüütli 12-6, 10130 Tallinn, Estonia
info@icds.ee, www.icds.ee
Tel.: +372 6949 340
Fax: +372 6949 342

ICDS Analysis
ISSN 2228-2076

Introduction

The critical infrastructure and essential services on which modern economies depend rely increasingly on information and communication technologies (ICT). Most global, transatlantic and regional international organisations (UN, NATO, the EU, G8, OSCD, OECD, ITU, ICANN, AU, ASEAN, OAS, etc.) have developed policies and instruments to address the growing sophistication of cyber attacks against critical infrastructures and services. This paper presents a comparative analysis of the approaches of NATO and the EU to cyber security.

For both NATO and the EU, cyber security is a strategic issue that impacts the security and defence of member states and of the organisations themselves. They both prioritize the resilience and defence of their own networks, organisations and missions, leaving cyber security of individual members states a national responsibility. The missions of the two organisations are complementary, with NATO focusing on security and defence aspects of cyber security, and the EU dealing with a broader, mainly non-military range of cyber issues (Internet freedom and governance, online rights and data protection), and internal security aspects.

The paper demonstrates how the understandings of cyber threats and challenges have evolved over the last decade in these organisations, and then more closely examines NATO's approach. It also addresses major issues of contention among NATO member states and suggests a way forward for further development of NATO's defence policy, stressing the need for greater cooperation between the two organisations.

Cyber security - a strategic security priority for NATO and the EU

NATO shares common liberal values and strategic interests with the EU. NATO, a political and military alliance and a self-defence organisation, defends not only common security and prosperity of its member states, but it forms a unique community of liberal values including freedom, human rights, individual liberty, democracy and the rule of law. NATO's mission is to ensure security of its member states by executing its core tasks: collective defence and deterrence, crisis management, and cooperative security through partnerships. Its primary tasks also encompass the protection of member states and its own organisations, infrastructures, and operations against cyber attacks.

In the view of NATO, cyber threats have negative implications for transatlantic and national security. In the *Strategic Concept* of 2010 NATO Allies declared that: "Cyber attacks are becoming more frequent, more organised and more costly […]; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability"[1] and committed to "develop further our ability to prevent, detect, defend against and recover from cyber attacks." Two years

[1] „Active Engagement, Modern Defence: Strategic Concept for the Members of the North Atlantic Treaty Organisation". Lisbon: NATO, 19 November 2010. Available at: http://www.nato.int/cps/en/natolive/official_texts_68580.htm

later, at the Chicago Summit, NATO heads of state and government, observing that "cyber attacks continue to increase significantly in number and evolve in sophistication and complexity", reiterated their commitment to develop further NATO's cyber defence capabilities. Most recently, at Wales Summit on 5 September 2014, NATO's Secretary General Anders Fogh Rasmussen restated NATO's commitment to defend Allies against the full range of threats, including cyber threats.[2] Separately, in a recent survey, out of ten largest member states, seven believed that cyber security is among six top national security priorities after attacks on Allies and international terrorism.[3]

As a politico-economic union, EU's main areas of responsibility for cyber security concern primary internal security issues - police and criminal justice cooperation in the fight against cyber-crime, the protection of critical infrastructures - and international cooperation. Compared to NATO, the EU is a latecomer concerning the national security and defence aspects of cyber security. It identified for the first time only in 2008 cyber threats as a key challenge that, in addition to economic and political, also has a military dimension.[4] Until then it dealt primary with network and information security, cyber-crime; and to a lesser degree with cyber-terrorism[5], while its approach was fragmented with overlapping parallel policies.[6]

It was only in 2010 that the European Commission cautioned about the significant increase of cyber attacks[7], and the EU launched a more strategic approach with the Internal Security Strategy of 2010 focusing on cyber-crime, partnership with industry and capability-building.[8] As of today, the Union deals

[2] "NATO leaders take decisions to ensure robust Alliance," 5 Sept 2014. Available at: http://www.nato.int/cps/en/natohq/news_112460.htm. Press Conference by NATO Secretary General Anders Fogh Rasmussen, 5 September 2014. Available at: http://www.nato.int/cps/en/natohq/opinions_112871.htm

[3] Wickett X., McInnis K., „NATO: Charting the Way Foward", Reserach Paper, July 2014, Chatham House, The Royal Institute of International Affairs.

[4] Report on the Implementation of the European Security Strategy - Providing Security in a Changing World – of 2008 brought greater attention than previously to the attacks against critical infrastructure. The document depicted cyber attack as "a potential new economic, political and military weapon". Report on the Implementation of the European Security Strategy, 11 December 2008, S407/08. Available at: http://www.eu-un.europa.eu/documents/en/081211_EU%20Security%20Strategy.pdf

[5] In the European Commission's communication "Network and Information Security: Proposal for A European Policy Approach" (COM(2001)298) (2001) the Commission outlined the increasing importance of network and information security. The Framework Decision on Attacks against Information Systems of 2005 aimed to improve co-operation between judicial authorities in order to fight cyber-crime. In 2006 a Strategy for a Secure Information Society aiming to develop a culture of network and information security in Europe was adopted. The EU Strategy for a Secure Information Society, adopted in 2006, addresses also internet-based crime. Cyber-terrorism was referenced in the Council's "The European Union strategy for combating radicalisation and recruitment to terrorism", 14781/1/05, 2005.

[6] Klimburg A., Tiirmaa-Klaar, H. „Cybersecurity and cyberpower: concepts, conditions, and capabilities for cooperation for action within the EU", European Parliament Study. April 2011, p.29.

[7] http://europa.eu/rapid/press-release_MEMO-10-598_en.htm?locale=en

[8] The Internal Security Strategy of 2010 identified three objectives: building capacities in law enforcement and judiciary, working with industry, and improving capabilities for dealing with cyber-attacks. It acknowledges that cyber-crime is a global phenomenon causing significant

also with security and defence aspects in the framework of the EU's Common Security and Defence Policy (CSDP), but its ambition is not member states' cyber security. Within the CSDP the aim of cyber defence capability building is to ensure resilience of CSDP institutions, operations and missions. For doing so the EDA is developing by the end of 2014 a cyber-defence policy framework and a road map.

The EU does not provide direct technical assistance to its member states under cyber attack, but acts as facilitator by encouraging them to adopt best practices. Through the European Network and Information Security Agency (ENISA) and the European Defence Agency (EDA) it distributes guidelines, arranges pan-European cyber exercises, and supports education and training.

In 2013 the EU brought its diverse lines of actions into a single document constituting a comprehensive approach – its cyber security strategy.[9] The strategy notes the use of "ever more sophisticated methods" by cybercriminals and emphasises the possible disruptions of the "essential services" and critical infrastructure.[10] The document prioritises enhancing public-private partnership, fostering national and international co-operation and information sharing, advancing European ICT industry and research and development (R&D), and developing cyber defence capabilities.[11] In monetary value, the EU invests over €500 million in the area of cyber security under the research and innovation programme "Horizon 2020".[12] Finally, in December 2013 the EU Council urged the Union to further strengthen its cyber defence-capabilities.[13]

Thus even though not all NATO and EU members states prioritize cyber security among the top national security themes, both organisations have collectively acknowledged cyber security as a strategic security priority. Similarly, for both of them cyber defence of their own networks, organisations and missions is a fundamental priority. Their missions are nevertheless complementary: NATO is

damage to the EU internal market and Europe is a key target for cyber-crime. Internal Security Strategy for the European Union: Towards a European Security Model, 5842/2/2010.

[9] „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions. Brussels, 7.2.2013 JOIN (2013) 1 final.

[10] The strategy does allude to national security by making a reference to the "increase of economic espionage and state-sponsored activities" targeting governments and private sector, but does not discuss it any further. Available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[11] The strategy establishes five strategic priorities: (i) achieving cyber resilience; (ii) drastically reducing cyber-crime; (iii) developing cyber defence policy and capabilities related to the CSDP; (iv) developing the industrial and technological resources for cyber security; and (v) establishing a coherent international cyberspace policy for the EU with a view also to promote core values. The strategy establishes five strategic priorities: (i) achieving cyber resilience; (ii) drastically reducing cyber-crime; (iii) developing cyber defence policy and capabilities related to the CSDP; (iv) developing the industrial and technological resources for cyber security; and (v) establishing a coherent international cyberspace policy for the EU with a view also to promote core values.

[12] European Commission, 'Horizon 2020: Work programme 2014-2015. Part 14', Decision C (2013)8631, 10 December 2013. Available online at: http:// www.statewatch.org/news/2013/dec/com-2013-horizon-2020-security-wp.pdf

[13] Council Conclusions (19/20 Dec 2013) calls for working out the cyber security framework in 2014, including a roadmap to improve member state's capabilities, research and technology.

mainly concerned with national security aspects, including the defence of the Allies, while the EU focuses primary to internal cyber security issues such as cyber-crime, resilience of critical infrastructure, and data protection, as well as to cyber diplomacy aspects (internet freedom and governance, online privacy and fundamental rights, etc.). In both organisations member states remain responsible for the issue of cyber security within their national borders.

Development of the approaches of NATO and the EU

The principal focus of NATO's cyber defence approach has always been the protection of its own headquarters, agencies, and operations. The Alliance has been improving its cyber defence capabilities since 1990s. The first well-known cyber incident against NATO took place in 1999 during NATO's operation "Allied Force" in Kosovo when hacker groups from Russia and Serbia disrupted NATO's internal systems.[14] Few years later, at the Prague Summit in 2002, cyber security appeared for the first time on NATO's political agenda with NATO declaring to "strengthen our capabilities to defend against cyber attacks."[15] In the same year, the North Atlantic Council (NAC) approved a Cyber Defence Programme and as part of this, the **NATO Computer Incident Response Capability** (NCIRC) - NATO's emergency team to prevent, detect and respond to cyber incidents - was created.[16]

The cyber attacks against Estonia in 2007 that disabled its governmental, media and financial websites and the Russia-Georgia war in 2008 that included military offence against Georgian military forces and cyber attacks against Georgian webpages[17] helped NATO to realize how it was behind in cyber space. Subsequently, the Alliance's focus broadened from the security of its own networks to that of its member states.[18] In January 2008 NATO approved its first **Policy on Cyber Defence** stressing "the need for NATO and nations to protect key information systems […]; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack."[19] In the same year, it established the **Cyber Defence Management Authority** (CDMA) to coordinate cyber defence, review capabilities and conduct appropriate security risk

[14] Healey, J. (ed.) „A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association, 2013.

[15] Prague Summit Declaration, 21 November 2002. Available at: http://www.nato.int/docu/pr/2002/p02-127e.htm. Cyber security has been in NATO's political agenda in all summits since then (the Riga Summit in 2006, the Bucharest Summit in 2008, the Strasbourg/Kehl Summit in 2009, Lisbon Summit in 2010, the Chicago Summit in May 2012)

[16] The NCIRC was created in response to DDoS attacks by pro-Serbian hacker groups targeting NATO's webpages during its Kosovo campaign (Hegenbart 2014).

[17] Russian attacks included various distributed denial of service attacks to deny/disrupt communications and information exfiltration activities conducted to accumulate military and political intelligence from Georgian networks. These attacks also included web site defacement for Russian propaganda purposes. For further discussion see David M. Hollis, „Cyberwar Case Study: Georgia 2008", Small Wars Journal. Available at: http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

[18] Robinson, N. et. al., "Cyber-security threat characterisation. A rapid comparative analysis", Rand 2013.

[19] Bucharest Summit Declaration, 2 April 2008. http://www.nato.int/cps/en/natolive/official_texts_8443.htm

management across the Alliance. It also accredited the **Cooperative Cyber Defence Centre for Excellence** (CCD COE) with the main objectives to improve the interoperability of NATO and enhance cyber awareness, education, and training efforts.

In 2009 cyber defence was rendered an integral part of NATO exercises. In 2010 the Lisbon Summit addressed cyber defence capabilities gaps including improvements to the NCIRC, and in the same year the **Emerging Security Challenges Division** was created within NATO International Staff with a mandate to analyse among other asymmetrical threats cyber threats. The **Defence Policy and Planning Committee/Cyber Defence** (from 2014 titled the Cyber Defence Committee) was also established to provide political-level guidance and oversight.

In 2011 the **Cyber Defence Management Board** (CDMB, supplanted CDMA), which consists of NATO cyber experts at the political, military, operational, and technical levels was set up. Its purpose is to coordinate cyber defence activities throughout NATO and associated agencies, and to facilitate implementation of NATO's cyber defence policies and capabilities.[20] In June 2011 a revised **Cyber Defence Policy** was approved, confirming the resolve to protect NATO's networks and assist member states in the event of cyber attack. It also commanded the establishment of two cyber Rapid Response Teams (RRTs) by the end of 2012 with a core of six professionals that can be deployed within 24 hours to a member state.[21] Any NATO nation under cyber attack could request the team's assistance through the CDMB[22], the deployment must be approved by the North Atlantic Council (which may be politically challenging). The policy also defined minimum requirements to national networks critical to NATO's core tasks and assistance to the Allies to achieve the minimum levels of security. Additionally, the **Defence Policy and Planning Committee** in Reinforced format (DPPC(R)) was set up to oversee the work of CDMB and manage the overall planning process, including cyber capabilities.[23] In 2012 the **NATO Communications and Information Agency** (NCIA) was established.[24]

[20] To date, NATO has signed MoUs with Bulgaria, Estonia, Poland, Slovakia, Turkey, the UK, and the US. Hunker 2010, cited in Rand 2013.

[21] Benitez 2012, cited in Robinson, N. et. al., "Cyber-security threat characterisation. A rapid comparative analysis", Rand 2013. Prerequisite for the deployment of RRT is a request by the member state and approval by the North Atlantic Council.

[22] Seffers 2012, cited in Robinson, N. et. al., "Cyber-security threat characterisation. A rapid comparative analysis", Rand 2013.

[23] Healey, J., and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", Atlantic Council issue brief, February 2012. http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf

[24] NCIA is responsible for identifying and promoting the development of capabilities in ensuring cyber security. NATO capabilities to identify, prevent, detect and respond to external threats to NATO networks is primarily performed by the NCIRC Technical Centre (NCIRC TC). NCIS implements also a Cyber Information Sharing Programme which will allow industry working with NATO and NATO to share cyber security Information. https://www.ncia.nato.int/Documents/Legal%20Office/NATO-Industry%20cooperation%20on%20cyber%20information%20sharing%20March%202014.pdf

Until the end of the decade, NATO's progress in bolstering its cyber capabilities was slow - it took over ten years until NCIRC with a ten-month delay attained full operational capability in November 2013.[25] In the last two years NATO has advanced nimbly: developed RRT capability, augmented the around the clock protection of its networks in more than 50 locations in 31 countries,[26] launched a solid cyber exercise and training programme,[27] and in 2013 included cyber to its defence planning.[28] Until then, NATO did not deal with deterrence and the use of force in cyberspace.[29]

In June 2014 NATO defence ministers approved Alliance's third enhanced **Cyber Defence Policy.** The new policy, endorsed at NATO Summit in Wales on 4-5 September this year establishes clearly that cyber defence is part of the Alliance's core task of collective defence - NATO nations are able to invoke the collective defence clause of the North Atlantic Treaty (Article 5) in case of a cyber attack with effects comparable to those of an armed attack. Priority areas for NATO are streamlining its cyber defence structures, defining capability targets for allies through **NATO's Defence Planning Process** (NDPP), improving information sharing, and setting up procedures for assistance to the member states.[30] The policy further commits the Alliance to developing principles, criteria and mechanisms to ensure minimum level of security among Allies, and to continue identifying NATO's dependencies on national networks to make sure that all follow the same standards.[31]

In terms of enhancing education and training, an important signal about the NATO's seriousness is the decision to create a **NATO Cyber Range** in Tallinn that will be used as the Alliance's main cyber defence training field.[32] The field enables Allies to test and exercise their cyber capabilities under a NATO structure, to feed lessons learned and new concepts into the Alliance, and to ensure the same levels of expertise across the Alliance.[33]

According to Jamie Shea, Deputy Assistant Secretary General for Emerging Security Challenges at NATO, NATO nations have also agreed to invest into

[25] Illési, Z., et al. "DAV4 II Report: Region's quest for inclusive cyber protection", Central European Policy Institute, 16. December 2013. Available at: http://www.cepolicy.org/publications/dav4-ii-report-regions-quest-inclusive-cyber-protection

[26] Shea, J. „NATO's new Cyber Defence Policy", 3 July 2014. International Conference on Cyber Conflict, 3-6 July 2014, Tallinn.

[27] https://www.chathamhouse.org/media/comment/view/197236

[28] Tigner, B. „NATO looks t ostand up collective cyber defence", Janes Defence Weekly, 20 September 2013.

[29] Kamp K-H., "NATO's 2014 Summit Agenda" Research Paper n 97, NATO Defense College, September 2013.

[30] Allied Command Transformation (ACT) delivers a comprehensive Cyber Defence Education, Training, and Exercise programme.

[31] http://www.nato.int/cps/en/natolive/topics_78170.htm?selectedLocale=en

[32] Ibid. Estonia offered its national cyber range for the use of all NATO nations, NATO approved it in June 2014. In 2013 the range hosted NATO's largest cyber defence exercise Cyber Coalition 2013 and the NATO Cyber Defence Centre of Excellence (CCD COE) exercise Locked Shields.

[33] http://www.atlanticcouncil.org/images/publications/NATO_in_an_Era_of_Global_Competition.pdf

common cyber capabilities.[34] In respect to fostering capability building, Smart Defence initiatives are going to be pursued that enable smaller groups of countries to acquire joint capabilities. Out of 143 Smart Defence projects three involve presently cyber defence:[35]

1. **Multinational Cyber Defence Capability Development Project** (MNCD2) aims to facilitate sharing sensitive information, improve situational awareness and the ability to detect malicious activity. A Cyber Information and Incident Coordination System developed by the participating nations (Canada, Denmark, Norway, Romania, and the Netherlands) will advantage NATO's Cyber Coalition exercise in 2014.[36]
2. **Malware Information Sharing Platform** facilitates technical information sharing within a trusted community without having to share details of an attack.[37]
3. **Transatlantic Defence Technological and Industrial Cooperation** is a partnership with industry.

Other actions the Allies are going to pursue include developing early-warning systems and contingency operational plans, enhancing information and intelligence sharing. The engagement with industries and international partners is also prioritised,[38] not least because NATO plans to use commercial clouds for less sensitive data.[39]

Concerning the partnership with the EU, working level regular informal staff-to-staff meetings on cyber security have taken place since 2010, and further cooperation is planned in the areas of awareness raising, joint trainings and capability-building, but due to the Cyprus issue bilateral relationship is weak.

Similarities and difference between the EU and NATO

Both NATO and the EU stress that cyber security of its member states is a national responsibility. In the EU there is no central authority responsible for common cyber security, while in NATO the top political decision-making body NAC exercises principal decision-making authority and overseas the development on NATO's cyber defence posture. Both organisations prioritise cyber security of its own institutions and infrastructure, operations and missions. Both aim at the development of comprehensive cyber security policies and are setting minimum

[34] Shea J., „NATO's new Cyber Defence Policy", 3 July 2014. International Conference on Cyber Conflict, 3-6 July 2014, Tallinn.

[35] Shea, J. „NATO's new Cyber Defence Policy", 3 July 2014. International Conference on Cyber Conflict, 3-6 July 2014, Tallinn.

[36] https://mncd2.ncia.nato.int/news/Pages/MN-CD2-Board-Meeting-04.aspx

[37] This project was launched in November 2013. http://www.nato.int/cps/en/natolive/news_105485.htm?selectedLocale=en. For more information on MISP see: http://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20(MISP).pdf.

[38] Ibid.

[39] Tigner, B. „NATO looks to stand up collective cyber defence", Janes Defence Weekly, 20 September 2013.

security standards for shared infrastructure. They both prioritise enhancing cooperation with industry and academy, and strengthening international cooperation. Both are identifying cross-sectoral and cross-border interdependencies of critical infrastructure, and attempt to secure ICT supply chain. Hence, there are many common non-military activities and interests, but in contrast to the EU, NATO does not have a mandate to exercise authority or give guidance over civilian and private sector infrastructure.

Where NATO and the EU differ is the area of assisting the member states: NATO nations can request assistance through RRTs, while the EU lacks the capability to provide technical expertise and services to its member states, rather, it functions as a forum for exchanging information and best practices.

Another difference lies in the ownership of the networks: NATO "owns" its command, control, communications, computers, and information systems while the EU does not own ICT infrastructure depending on the member states networks for CSDP missions (Robinson 2013).[40]

Over the last decade, the EU has been lagging behind NATO in developing comprehensive policy, with a more strategic approach mandated as late as in 2008 with the Internal Security Strategy, and lastly, a comprehensive approach in 2013 with cyber security strategy. However, European cyber security efforts are still at an embryonic stage[41] and the member states have gaps in their capabilities with many lagging behind North-America or NATO’s strategic partners in Asia. The future work for the EU should include defining minimum standards and obliging the reporting of significant cyber incidents across all critical infrastructure sectors (to date only telecoms are obliged to report), further advance and harmonise the legal framework, as well as continue to develop cyber defence capabilities within CSDP.

In comparison, while in the beginning of the last decade NATO’s action was also tardy, as of today NATO has been able to develop remarkable strengths in many areas constituting a comprehensive approach, in particular through integrating cyber defence into NDPP, setting up instruments for assistance to the member states, and extensive training and exercises efforts.

Discussion issues between NATO member states

The primary discussion issue for NATO has been establishing the level of ambition regarding the cyber defence. First, whether the organisation should confine itself to defending its own assets before setting more ambitious goal of assisting member states in the case of a cyber attack. Opinions of the NATO nations diverge in this question, and the ambiguous wording of the Wales Summit declaration („assistance to Allies should be dressed in accordance with

[40] Robinson, N. “Cybersecurity Strategies Raise Hopes of International Cooperation”. Available at: http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cybersecurity-strategies-raise-hopes-of-international-cooperation.html. The EU CS strategy (2013) states that “it is predominantly the task of MS to deal with security challenges in cyberspace”.

[41] http://www.europeanglobalstrategy.eu/nyheter/opinions/eu-and-cyber-security-whats-next

the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks") indicates that with the fundamental responsibility for cyber security lying with the members states, the collective assistance for a member state under attack is not an automatic process, but will decided at political level on a case-by-case basis.[42]

A second issue concerns the question what aspects of cyber security should be left to the EU in order to avoid duplicating efforts.[43] Despite regular NATO-EU working level meetings regarding cyber security the tangible results have been modest. This has to do with a political obstacle resulting from the Cyprus-Turkey conflict that blocks the overall security cooperation between the EU and NATO[44]; and unfortunately this stalemate is not likely to be solved any time soon.

A third issue is about equal burden sharing for developing cyber capabilities. The larger member states contributing greater shares to NATO's common military budget (in 2012 the top contributors were the US, UK, Germany and France),[45] worry about who would pay for new capabilities.[46] Meanwhile, more advanced member states, having heavily invested into national cyber capabilities, hesitate sharing these with others for financial and security reasons.[47] So far there seems to be little will for the development of NATO's own defensive or offensive capabilities, primary because they would further strain members' shrinking defence budgets.[48] Besides, the European members are reluctant to further strain their defence budgets (only three of NATO's European members fulfil the requirement to spend on overall defence 2% of gross domestic product: UK, Greece and Estonia). Concerning the civilian capabilities, the uneven and insufficient level of preparedness and capability of the EU member states undermines security of European countries with overlapping memberships. Smaller EU member states tend to have particular difficulties, even staffing their Computer Emergency Response Teams is challenging.

A forth issue concerns the core task of the Alliance - which cyber attacks call for collective response? Article 4[49] and 5[50] of the North Atlantic Treaty provide for

[42] Wales Summit Declaration, 5. November 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en
[43] Ibid.
[44] Turkey does not allow Cyprus to attend EU-NATO meetings; as a result, the EU does not want to discuss any points outside of the 'Berlin Plus' Agreement. See full source information on article: http://www.atlantic-community.org/index.php/Open_Think_Tank_Article/Cyprus_Conflict_Prevents_EU-NATO_Strategic_Partnership
[45] The NATO Military Budget, the NATO Civil Budget, and the NATO Security Investment Program (NSIP) are maintained by direct contributions from NATO's member states. The US share in NATO military budget is approximately 25% of the total budget and in the NSIP 22%. See full source information on report: http://fas.org/sgp/crs/row/RL30150.pdf
[46] Ibid.
[47] http://www.atlantic-community.org/index.php/Open_Think_Tank_Article/Cyprus_Conflict_Prevents_EU-NATO_Strategic_Partnership
[48] https://www.chathamhouse.org/media/comment/view/197236
[49] The North Atlantic Treaty, Article 4, "The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened."

political consultations if an Ally feels its security is threatened and for a collective response in case of an armed attack against an Ally. It has been convincingly argued elsewhere that the existing ambiguity for the threshold for the cyber attack that is considered an armed attack or defining concrete circumstances entailing collective response actually increases NATO's cyber deterrence.[51] Likewise, it is undesirable for NATO to draw a clear red line that obliges collective response when it is crossed, and it is indeed questionable if a clearly articulated threshold would deter non-state actors from crossing it.

A way forward for NATO's cyber defence posture

Collective defence

As confirmed in Wales, the Allies are able to invoke Article 5 in case of a cyber attack with effects comparable to those of an armed attack. It is less equivocal how Article 5 commitment will be implemented in practice. NATO nations need to think about what the criteria are when a cyber attack qualifies as equivalent to an armed attack, what the strategic implications of such an attack are, what circumstances obligate a collective response (for example does damage to or disruption of private critical networks resulting in serious effects?), and how the problem of attribution can be solved[52], among other questions.

The invoking of Article 5 will always be a political decision taken consensually on a case-by-case basis after consultations among the Allies. It entails lengthy consultations to build political consensus and approve operational plans. Even though in 2001 - the only time when Article 5 has been activated - it took only 24 hours to do so after the 9/11 terrorist attacks against the US, many European countries would consult their sovereign decision-making bodies in the capitals (governments and parliaments). They must agree a cyber attack is considered serious enough to constitute an armed attack, and what kind of response would be appropriate. In case of a cyber attack, timely response must be rapid to avoid major damage.

Given the existing capability, policy and doctrinal divide between the Allies and the absence of criteria what constitutes an armed attack, deliberations would be thorny. NATO's decision-making process might be delayed also by the scarce understanding of operational and technical aspects of cyber defence, as well as the lack of general consensus on key cyber security terms at the strategic level.

[50] The North Atlantic Treaty, Article 5, "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."

[51] Hunker J. „NATO and cyber security", in Graeme P. Herd, John Kriendler (ed.). "Understanding NATO in the 21st Century: Alliance Strategies, Security and Global Governance". Routledge, 2013. Jamie Shea shares the same view, see Jordan, S. 'NATO updates cyber defence policy as digital attacks become a standard part of conflict', ZDNet, 30 June 2014, http://www.zdnet.com/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict-7000031064/

[52] According to the North Atlantic Treaty, for a collective response the attack should originate outside NATO territory, but the technical attribution of an attack may be impossible.

To speed up the decision-making process and craft effective responses, the pre-existing consensus including a set of possible response options for strategic level decision-makers to choose from, as well as a list of Allies' operational cyber capabilities must be made available.[53] Pre-existing consensus should include criteria of a cyber attack as an armed attack, if and when pre-emptive cyber strike or kinetic response would be allowed (the response might be limited to entirely non-kinetic measures)[54], which kind of response would be proportional, etc.[55] It has been suggested to institute a high level advisory body, a Senior Cyber Committee (similar to a NATO's nuclear planning group) consisting of technical experts, policy personnel, and military representatives to discuss regularly cyber security in the Allied context.[56] This would help to reduce the lack of understanding between technical and strategic levels, keep senior decision-makers attention on cyber security and facilitate timely decision making.

In considering options for possible responses, NATO's dependency on civilian and private sector infrastructures needs to be taken into account. For example, what kind of response follows a cyber attack that damages or disrupts NATO's mission-critical private infrastructure, especially if the perpetrator is a non-state actor, collateral damage cannot be avoided, or attribution is impossible? Further questions include a collective response to a non-Article 5 crisis - when the effect of a cyber attack is not severe enough to be classified as an "armed attack" should NATO take some counter-action through civil emergency capabilities?

A solution to the attribution problem would be adoption of "a comprehensive attribution approach" that in addition to technical parameters considers wider political situation, geopolitical indicators and warnings. For improving attribution capabilities the Alliance should invest more in forensics research.[57]

Operational planning and capabilities development

A report by the defence committee of the UK parliament finds that NATO is poorly prepared to respond to the Russia's use of asymmetric warfare, including cyber attacks, information and psychological operations. The committee urges the Alliance to develop its own asymmetrical warfare capabilities, discuss how to deal with these attacks and operations, and mount its own offensive operations.[58]. It also calls NATO to re-examine the legal and military doctrines, criteria, and responses for the declaration and use of both Article 4 and Article

[53] Hunker, J. "NATO and cyber security," in Graeme P. Herd, John Kriendler (ed.). "Understanding NATO in the 21st Century: Alliance Strategies, Security and Global Governance". Routledge, 2013.

[54] Jordan, K. T. "Would NATO Go to War Over a Cyberattack?" The National Interest. 4 September 2014. Available at: http://nationalinterest.org/feature/would-nato-go-war-over-cyberattack-11199

[55] According to Jamie Shea decision if a cyber attack equals to an armed attack must be made based on the effect of the attack (Jane's Defence, 25 September 2013).

[56] "NATO in an Era of Global Competition", The Atlantic Council, June 2014. Available at: http://www.atlanticcouncil.org/images/publications/NATO_in_an_Era_of_Global_Competition.pdf

[57] Jordan K., T. "Re-examining Article 5: NATO's Collective Defence in Times of Cyber Threats. " Available at: http://www.huffingtonpost.com/klara-tothova-jordan/reexamining-article-5-nat_b_5491577.html

[58] "Towards the next Defence and Security Review: Part Two—NATO", 22 July 2014. Available at: http://www.publications.parliament.uk/pa/cm201415/cmselect/cmdfence/358/358.pdf

5.[59] Likewise, James Stavridis, retired NATO's Supreme Allied Commander (SACEUR) believes NATO should stand up a cyber defence operations force under the SACEUR, as well as explore the utility of offensive cyber weapons.[60] The need to integrate cyber into NATO's military operations and operational planning has been acknowledged also by Jamie Shea.[61] Operational planning both for Article 5 and non-Article 5 events along with capability development must be adjusted to the reality of asymmetrical or hybrid warfare that employs a range of tools, including information operations and cyber attacks.

In addition to the need to integrate cyber into both military and civil emergency operational planning, NATO must improve the interoperability of cyber capabilities of the Allies and this process can be facilitated by the means that will be provided by the newly established NATO's cyber range.

Furthermore, realistic cyber threat scenarios, as well as clear and tested response procedures and mechanisms should be in place. Operational contingency plans must clarify which capabilities NATO nations are prepared to make available to the Alliance, and the mechanisms for collective assistance by the individual Allies. A full range of response options (including kinetic means) accompanied by appropriate plans and capabilities need to be worked out. Since a simultaneous strike against NATO's own and the member state's infrastructure is likely, it would be prudent to ensure enough common capabilities to respond to both tasks. The existing two small RRTS consisting of a permanent core of six experts may be inadequate for simultaneous tasks.

In order to enable military operational planning NATO should consider the development of cyber warfare doctrine. It should establish a joint cyber command or headquarters (not unlike the Special Operations Headquarters), aligning joint strategy with political ends, at Supreme Headquarters Allied Powers Europe (SHAPE). Concerns about the legality of an offensive action in cyberspace aside, while NATO does not have an offensive cyber capability, member states' capabilities could be used under Article 5 circumstances. NATO needs to ponder also what could be done to help an Ally experiencing a cyber attack causing serious damage to its private critical infrastructure.

It goes without saying that intelligence and information sharing, joint situational awareness, early-warning, analysis of vulnerabilities and malware, as well as appropriate forensic capabilities should be fostered. In order to facilitate sensitive information sharing among Allies and with industry, secured

[59] Asymmetric warfare conventionally includes cyber attacks, information and psychological operations., economic and proxy attacks. Hybrid warfare „combines conventional military forces with information operations, provocateurs, cyber and economic measures". "NATO in an era of Global Competition", June 2014, Atlantic Council. Available at: http://www.atlanticcouncil.org/images/publications/NATO_in_an_Era_of_Global_Competition.pdf

[60] Stavridis, J. "NATO's New Brave World", Foreign Policy, 21 August 2014. Available at: http://www.foreignpolicy.com/articles/2014/08/21/natos_brave_new_world_syria_iraq_putin_russia

[61] Shea J. „NATO's new Cyber Defence Policy", 3 July 2014. International Conference on Cyber Conflict, 3-6 July 2014, Tallinn.

anonymised/aggregated (in contrast to certain and detailed) information exchange portals with standardised information-sharing formats could be developed. In addition to sharing technical data among all members, limited trusted information sharing could be worked out involving some of the members. General awareness and knowledge raising through education, training and exercises also increases trust between participants.

Finally, due to the rapid evolvement of cyber environment and threats, continuous attention to cyber security at the NATO's top decision-making level is essential. To enhance common understanding of decision-makers and treat cyber security as strategic and not merely as a technical issue regular discussions are needed.[62]The upcoming NATO Defence Minister's meeting in February 2015 should endorse the practical measures that have been worked out in order to fulfil the obligations taken this summer in Wales by the NATO heads of state and government.

Smart Defence; pooling and sharing

Thus, NATO should consider how to encourage European Allies to invest into and how to ensure interoperability of their cyber capabilities. In order to assist other Allies or NATO under cyber attack it is necessary to pool resources.

Due to the budgetary and security concerns it will be difficult to attain agreement of all 28 Allies regarding common funding beyond NATO's own networks and nodes for the development of joint capabilities and the acquisition of common assets (e.g. hardware and software). However, pooling and sharing is feasible among "coalitions of the committed" that jointly fund development of multinational capabilities. With a Framework Nation concept, participating countries agree on which will provide which kinds of capabilities. The larger, "framework" nation provides the basic infrastructure, while smaller nations contribute niche capabilities. In that way a smaller group of nations can pool their resources, thereby making the resulting capabilities available to others. A good example is a Smart Defence initiative, the **Multinational Cyber Defence Capability Development Project**[63] (MNCD2), which aims to enhance joint tactical and operational situational awareness of participating nations. In the spirit of solidarity, this capability, developed by five countries, will be made available for the use of all Allies - the project will provide a Cyber Information and Incident Coordination System for NATO's Cyber Coalition 2014 exercise.[64] Likewise, for greater solidarity, all advanced NATO nations could make their national capabilities available for NATO's use. Estonia's offer to use its Defence Forces cyber range for training and exercises for all NATO nations is an excellent example that paves the way for the greater common use of national assets.

[62] The first ever meeting of defence ministers on cyber defence took place as late as in June 2013. While there is little information on the agenda of the North Atlantic Council sessions, it has discussed cyber defence at least once, on 9 May 2014.

[63] The MNCD2 participating countries are Canada, Denmark, Norway, Romania, and the Netherlands. The project aims to facilitate sharing sensitive information, improve situational awareness and the ability to detect malicious activity.

[64] https://mncd2.ncia.nato.int/news/Pages/MN-CD2-Board-Meeting-04.aspx

Education, training and exercises

A cyber force is only as good as its members. NATO needs a robust and creative training and exercise programme, and NATO nations should take greater advantages from education, training, and R&D opportunities provided by the CCD COE. It is alarming that, according to Jamie Shea, NATO currently has only about one-third of the cyber capabilities it needs, relying instead to a certain degree on benevolent "white hat" hackers.[65] In addition to the overall lack of highly skilled cyber professionals in military that all countries suffer, too many European Allies still lack basic cyber threat information, and have not developed cyber security strategies (as of 2013 only 17 EU member states have strategies), not to speak about military cyber security doctrines and rules of engagements.

Cyber environment is highly integrated into other security and defence domains. This means that decision-making structures, including the strategic, operational, and tactical levels, must be supported with uncomplicated cyber expertise. A gap in the understanding of cyber issues at the technical side of cyber and the strategic decision makers has been long identified. In addition to improving the awareness through training where modelling and simulation can be utilized, employing visualisation and other tools that help to convey technical information to a non-specialist audience would be helpful.

In this respect, the institution of the NATO's cyber range based on the Estonian Defence Forces facilities enables greater interoperability of the national capabilities. The range enables Allies to test and exercise their cyber capabilities within a NATO structure, to feed lessons learned and new concepts into the Alliance; and to ensure that cyber experts across the Alliance share the same levels of expertise.[66] Last year the cyber range hosted NATO's largest cyber defence exercise Cyber Coalition 2013 and an exercise Locked Shields of the NATO Cyber Defence Centre of Excellence (CCD COE). The setting up of NATO's cyber range sends a clear signal that NATO takes seriously its role in defending against cyber attacks. Interestingly, as NATO's CCD COE is also located in Estonia, this tiny, but in terms of cyber security, innovative and advanced NATO member state would be a convenient hub for the NATO's education, training and interoperability improvement efforts.

Partnerships with the EU and industry

Capability building is founded on strategy, doctrine and legal framework. In partnership with the EU, the Alliance should encourage NATO nations to develop solid strategic and doctrinal principles for cyber security. Efficient dialogue with the Union is needed also to advance mutual information sharing and incident reporting, avoid duplication of efforts, consolidate civilian emergency and crisis management procedures, and conduct joint training and exercises.

[65] Tigner, B. "NATO officials warn of personnel gap in their cyber defences".*Jane's Defence Weekly*, 18 November 2013.

[66] "NATO in an era of Global Competition", June 2014, Atlantic Council. Available at: http://www.atlanticcouncil.org/images/publications/NATO_in_an_Era_of_Global_Competition.pdf

Military capabilities depend greatly on networks and infrastructures that are in most countries largely privately owned. Both NATO and the EU are working on mapping those dependencies. The partnership with industry should furthermore include getting greater access to competencies of industries who possess a majority of state-of-art and response capabilities in cyber environment. As identified by NATO and the EU, securing supply chain management and procurement processes are equally crucial.

The EU has expertise in ensuring resilience of critical infrastructure and in establishing public-private partnerships for doing so. Exchanges with the EU would in this respect be beneficial for NATO because it also needs to think about how to encourage the Allies to improve the security of their critical infrastructure on which NATO missions depend. NATO could agree on common security standards that ensure the uniform level of cyber security across the Alliance.

Out of the 28 EU member states 21 are in NATO. Most of the 28 NATO Allies belong to the EU. Countries with overlapping memberships have only one set of budgets and capabilities to ensure cyber security. Therefore more efficient cooperation between NATO and the EU is essential. The existing ad-hoc NATO-EU working level meetings on cyber issues should be instituted into a permanent joint working group which task is to review areas where greater exchanges would bring synergy. For example, to beef up education and training capabilities, exchanges of best practices and lessons learned between the cyber ranges project of the EDA and NATO's cyber range should be supported.

Conclusion

This paper has shown that over the past decade NATO and the EU have come to regard cyber security as a strategic security and defence issue. For NATO cyber defence is part of NATO's core task of collective defence. NATO has clearly been more successful than the EU in refining mature and comprehensive approach to cyber security. The fact that the Alliance can launch a military response to respond to a cyber threat constitutes a major breakthrough in the development of NATO's approach to cyber security.

For a stronger cyber defence posture NATO should establish a joint cyber command or headquarters at SHAPE as a focal point of development, coordination and direction for its cyber activities; as well as consider developing cyber defence doctrine. NATO also needs to think about how to put the collective defence commitment into practise, reduce the gap between technical and strategic levels and enable a more agile decision-making process. It should design and test operational response plans, procedures and mechanisms, ensure capabilities and their interoperability, and test them regularly and frequently. It should also encourage the greater investment into and the greater common use of national capabilities. Partnership with industry has become imperative due to dependency on private infrastructure.

The EU is also becoming a major global player in regards to cyber security, impacting a wider range of domains than NATO's more security-centred essence prescribes, from cyber diplomacy to economic and internal security aspects. It has also engaged capacity building through CSDP into its recent comprehensive approach.

The paper likewise identified that the two organisations could benefit more from each other competencies: the EU has solid expertise on resilience of critical infrastructure, public-private partnerships, and strategy and policy development; while NATO is successfully integrating cyber defence into operational and contingency planning and exercises, as well as establishing methods and tools to ensure interoperability of cyber capabilities. We further argued that NATO and the EU should coordinate their activities in respect to cyber security more effectively, in order to attain a joint comprehensive approach that would help to improve cyber resilience of the Euro-Atlantic community and beyond. The first step for doing so would be to set up a permanent NATO-EU joint cyber security working group.

Appendix

Institutional set up of NATO cyber defence

Responsibility for implementing the NATO policy on cyber-defence lies with NATO's political, military and technical authorities and individual allies. The **North Atlantic Council** (NAC), oversees the political aspects of implementation and exercises principal decision-making authority regarding cyber crisis management.

At the political level of defence counsellors from national delegations the **Cyber Defence Committee** (until 2014 the Defence Policy and Planning Committee/Cyber Defence) appraises cyber defence planning and capabilities development processes through NDPP, and provides oversight and advice to NAC on NATO's cyber defence efforts.

At the working level, the **NATO Cyber Defence Management Board** (CDMB) coordinates technical, political and information-sharing activities, and directs and manages cyber defence throughout NATO civilian and military bodies. It constitutes the main consultation body for the NAC and provides advice to member states on all main aspects of cyber defence. The majority of member states have signed memoranda of understanding with CDMB defining information exchange and early warning arrangements, and mechanisms for receiving assistance.

At the technical level, the **NATO Communications and Information Agency** (NCIA) is responsible for implementing and operating NATO's cyber defence capabilities along with the **NATO Military Authorities** (NMA). NATO's cyber emergency response team, the **NCIRC** division of the agency, monitors NATO networks, handles and reports incidents and disseminates incident-related information. It is composed of two sub-units: the Coordination Centre, located in NATO headquarters in Brussels, which coordinates across the Alliance, prepares threat assessments and planning exercises;[67] and the Technical Centre in Mons which pays a key role in case of cyber attacks against NATO networks, providing expertise and technical service. Additionally, the **NATO Consultation, Control and Command** (NC3) deals with technical and implementation aspects of cyber defence. Finally, the **Allied Command Transformation** plans and conducts NATO cyber exercises.

Institutional set up of the EU cyber security

The most important actors in this field are the **European Network and Information Security Agency** (ENISA), the **European Police Office** (Europol) including **the European Cyber Crime Centre** (E/C3), and the **European Defence Agency** (EDA).

European Commission, the executive body of the EU, is involved in formulating the Union's cyber security policy, priorities and objectives through the

[67] Illési, Z., et al. "DAV4 II Report: Region's quest for inclusive cyber protection", Central European Policy Institute, 16. December 2013. Available at: http://www.cepolicy.org/publications/dav4-ii-report-regions-quest-inclusive-cyber-protection

Directorate-General Home Affairs (DG Home) that is responsible for police and criminal justice cooperation and overviews Europol activities; and DG Connect that is in charge of the protection of critical infrastructure and overviews ENISA's activities. An important instrument is also the EU's Council's Friends of the Presidency Group on Cyber Issues.

ENISA provides expertise, advice and assessment of cyber-practices to the EU institutions and member states, and facilitates dialogue among the various actors involved in cyber-security at the European level. It is a key facilitator of cyber exercises, including organising the multi-level pan-European cyber exercise Cyber Europe.

Europol, cooperating with law enforcement and intelligence agencies, focuses on cyber-crime and supports member states in their investigations. The E/C3 established in 2013 within Europol is the Union's focal point in fighting cyber-crime. Europol also assesses the risk of cyber-attacks by terrorist groups.[68]
EDA is in charge of further developing the EU's cyber capabilities together with the **EU Military Staff** (EUMS). Other relevant agencies include the **Judicial Cooperation Unit** (Eurojust), which plays a role in the fight against cyber-criminality by facilitating cooperation among prosecutors, and the CERT-EU established in 2011.

European External Action Service (EEAS) together with EDA deals with Common Foreign and Security Policy (CFSP) and CSDP issues.

[68] Renard, T. "The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security". European Strategic Partnerships Observatory (ESPO)/FRIDE /Egmont working paper 7. June 2014. Available at: h ttp://www.fride.org/descarga/WP7_The_rise_of_cyber_diplomacy.pdf