Received: 15. 3. 2019 Accepted: 5. 4. 2019 Published on-line: 15. 6. 2019
Available from: www.obranaastrategie.cz doi: 10.3849/1802-7199.19.2019.01.005-022

LAGGING COLOSSUS OR A MATURE CYBER-ALLIANCE?
20 Years of Cyber Defence in NATO

ZAOSTÁVAJÍCÍ KOLOS ANEBO VYZRÁLÁ KYBERNETICKÁ ALIANCE?
20 let kybernetické obrany v NATO

Tomáš Maďar[a]

Abstrakt

Článek představuje současné NATO jako uvědomělou a sebevědomou organizaci, která postupuje na cestě k zabezpečení kybernetické bezpečnosti celé Aliance. Zdůrazněna je teze, že přestože v první dekádě po válce v Kosovu byla problematika kybernetické obrany v rámci Aliance upozaděna, v návaznosti na útoky na Estonsko v roce 2007 a jejich analýzu *post mortem* dokázala Aliance definovat priority pro tuto oblast a v posledních deseti letech mílovými kroky deficit dohnala. Jako nejdůležitější jsou identifikovány summity z let 2014, 2016 a 2018 a jejich přínos.

Abstract

The article presents NATO as a self-aware and confident organisation that takes measured steps to enhance the cyber security of the Alliance as a whole. I reassert the notion that in spite of cyber defence not featuring on the top of the agenda in the early 2000s due to the effects of 9/11, the subsequent wars in Afghanistan and Iraq, and the 2004 NATO enlargement process, after the 2007 attacks on Estonia and their post-mortem analysis the Alliance has been able to define priorities for this particular area and to significantly decrease the deficit by taking substantial but measured steps to rectify the situation it found itself in. The summits of 2014, 2016 and 2018 are identified as the most important in terms of NATO's development in this area.

Klíčová slova

NATO; kybernetická obrana; kybernetické útoky; schopnosti; kybernetická bezpečnost; aliance; Evropská unie.

Keywords

NATO; Cyber Defence; Cyber-Attacks; Capabilities; Cyber Security; Alliance; European Union.

[a] Department of Political Science, Faculty of Social Studies of the Masaryk University. Brno, Czech Republic. E-mail contact: t.madar@mail.muni.cz. Researcher ID: B-3413-2017.

INTRODUCTION

Feedback loops designed to help solve the air defence problem during the 1940s, the endeavour directed at decrypting the infamous Enigma cipher machines during the very same timeframe, later on the Global Positioning System and packet switching networks, to name a few – much of the development in fields such as cybernetics, cryptography, computer science and information technology had historically been closely rooted in or linked to their potential or real application in warfare.[1] Even the ubiquitous Internet, quite possibly the very symbol of the information revolution for the average citizen, is a direct descendant of ARPANET, a packet switching network originally funded by the Advanced Research Projects Agency (ARPA) of the United States Department of Defense.

The military application of the many innovations based in computer science and information technology had matured throughout the second half of the 20th century. This process culminated in January 1991, as Operation Desert Storm began. The First Gulf War was the first embodiment of information era conflict in which coalition forces led by the United States attained information dominance, significantly outperformed Iraqi forces and quickly forced a surrender whilst sustaining minimal losses themselves.

The coalition forces' efficacy was further bolstered by the U.S. intelligence having exploited Iraqi systems and networks in the run-up to the Desert Storm breaking out via computer network operations. Through computer network exploitation of Iraqi command-and-control systems, the U.S. military gained precise insights into the status of Iraqi forces. As the fighting broke out, by having disabled Saddam Hussein's fibre-optics communication links by bombing the switching systems pinpointed by European companies which installed them, the coalition forces made the adversary reroute communications to a back-up system built on microwave signals which could then be exploited by satellite means.[2]

Though kinetic weapons were favoured over computer network attack capabilities, Operation Desert Storm marks the first campaign where cyber means were utilized effectively as a force multiplier.

In 1994, the Clinton administration contemplated an invasion onto Haiti, after a UN Security Council resolution called for restoration of rule of the democratically elected president, Jean-Bertrand Aristide, who was ousted in a coup d'état. Even though the situation was eventually resolved after the perpetrators fled the island, a U.S. military plan for onslaught involved disabling the Haitian air-defence system that was hooked up to local telephone lines by a denial-of-service type computer network attack.[3]

Seeking lessons to be learned from the conflict and its consequences, U.S. analysts soon realized that the very technology on which Western democracies were becoming more and more reliant would also be used by adversarial forces in future conflicts against the West. NATO, however, only understood this challenge after it was already too late.

[1] Rid, Thomas. 2016. *Rise of the Machines*. New York: W. W. Norton & Company, Inc.
Lycett, Andrew. 2011. *Breaking Germany's Enigma Code*. Available at: https://bbc.in/1OFnntY
[2] Kaplan, Fred. 2016. *Dark Territory: The Secret History of Cyber War*. New York: Simon&Schuster, pp. 21-29.
[3] Ibid., pp. 58-59.

The Kosovo war of 1999, dubbed "*Web War I*" or "*The First Internet War*" first laid bare in full the potential vulnerabilities of NATO networks. While most of the exchange within the conflict consisted of information competition and propaganda, patriotic hackers based in Serbia, Russia, Latvia, Lithuania and even China[4] engaged in cyber attacks, and in some cases managed to degrade networks of NATO and the U.S. military. A successful distributed denial-of-service attack even resulted in bringing down the official NATO website, prompting a public apology by then-NATO spokesman, Jamie Shea.[5]

The experience of Operation Allied Force clearly demonstrated the growing reliance on information technology in both operations and strategic communications and public relations. With the recognition of these vulnerabilities coinciding with the adoption of the revolutionary 1999 NATO Strategic Concept, how quickly did NATO get up to speed to be able to face threats emanating from cyberspace?

AIMS AND METHODOLOGY

Twenty years after the first baby steps were taken by NATO, where exactly does the organization find itself with regard to its cyber preparedness and how does it lay the groundwork and fulfil its role-model part for the Allied nations? Which summits were the most instrumental in that their decisions were key to establishing NATO's current strategic cyber defence posture?

Even after the big leaps taken at both the 2014 Wales Summit and 2016 Warsaw Summit, there were voices that still echoed the notion that NATO's build-up in capabilities and development of policies remains limited and slow. Not just NATO, but the Alliance[6] has been seen by some as not wholly living up to its potential in addressing the cyber threats and risks of the 21st century. Some of the oft-stressed areas included the Alliance's supposed indecisiveness, inability or unwillingness to adopt offensive cyber capabilities or undertake offensive computer network operations, lack of doctrine and strategic objectives and vast differences in levels of defence capability and preparedness across respective NATO Member States.[7]

Utilizing the research design of a retrospective longitudinal case study, the article presents an overview and analysis of NATO's development of policies, capabilities and bodies responsible for tackling the issues pertaining to cyber defence from the year of 1999 to the 2018 Brussels Summit. This will be achieved, in part, by tracing the

[4] After the mistaken bombing of Chinese embassy in Sarajevo – see Jason Healey and Klara Tothova Jordan. 2014. *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*. Available at: https://bit.ly/1lLFa5U

[5] Diamond, Jonathan. 2013. Early Patriotic Hacking. In: Healey, Jason (ed.). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington: Cyber Conflict Studies Association, pp. 136-141.
In 2001, a collision of U. S. Navy EP3E ARIES II (a signals intelligence) aircraft and a People's Liberation Army J-8IIM fighter jet led to yet another exchange of computer network attacks between Chinese and American hackers targeting government and military servers (ibid., pp. 141-145).

[6] For the purposes of this article, I adhere to language that differentiates between the NATO bodies and the Alliance as a whole (which consists of both NATO bodies and the Member States).

[7] Smeets, Mark. 2017. *Europe Slowly Starts to Talk Openly About Offensive Cyber Operations*. Available at: https://on.cfr.org/2WEi5F1
Ilves, Toomas Hendrik. 2018. *Ilves at CyCon 2018: 'Cyber NATO' coalition of liberal democracies needed*. Available at: https://bit.ly/2IB3Fk0
McCord, Cameron. 2018. *Russia's Baltic Cyber Campaign Leaves NATO Endangered*. Available at: https://bit.ly/31wW5zz

developments embedded in respective NATO Summit Declarations, which are the highest-level consensual policy documents that the Alliance subsequently acts on. The article identifies the NATO Summits most instrumental to the development of cybersecurity in the Alliance, whose impact will likely be lasting for the decades to come. Last but not least, it attempts to answer the questions of whether NATO has done enough to boost the capabilities of the Allies and to prepare them for the cyber threats of the 21st century or whether it is lagging behind and needs to up the ante in order to prepare for the security environment it currently faces. Other significant issues, namely NATO's cooperation with the European Union as well as the question of developing offensive capabilities, are briefly outlined and discussed.

Wherever possible, references will mostly consist of primary sources, such as summit declarations, strategic concepts, and official communications. Furthermore, based on their relevance, articles and analyses found on the websites of NATO and its affiliated organisations will be utilized. Last but not least, secondary literature focusing on relevant issues will be used.

CYBER DEFENCE DECISION-MAKING IN NATO

The process of cyber defence policy preparation in NATO is mostly referred to the Cyber Defence Committee, which reports directly to the North Atlantic Council, the main body of the North Atlantic Treaty Organization (NATO), whose every decision is understood to be an expression of the collective will of all 29 Allies, as its decisions must be taken by consensus.[8]

At the highest level, the NATO's stated purpose is to safeguard the freedom and security of its members through political and military means. The declared political objectives include promotion of democratic values and encouraging consultation and cooperation on defence issues to build trust and prevent conflicts. On the military side, despite NATO claiming it is being first and foremost committed to the peaceful resolution of disputes, should diplomatic efforts fail the Alliance has continually reaffirmed that it retains the military capacity needed to undertake crisis management operations, which are carried out either under Article 5 of the Washington Treaty or under a UN mandate.

Even though the overall stability and security within the Euro-Atlantic area and in the rest of the world is desired, one of the Alliance's three core tasks (and arguably the most important one) is its essential collective defence framework, which since 2014 per the Enhanced NATO Cyber Defence Policy also comprises cyber defence.

The organisational structure within NATO is hierarchical with precisely defined responsibilities. The existing structure pertinent to cyber defence was streamlined by the aforementioned 2014 Policy.

As with any important decision, the ultimate oversight and political responsibility lie with the North Atlantic Council (NAC). NAC provides the International Staff (IS) and International Military Staff (IMS) with high-level oversight on the implementation of the

[8] NATO. Undated. *What is NATO*. Available at: http://www.nato.int/nato-welcome/index.html.
NATO. 2018. *Cyber Defence*. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm.

policy, exercises authority in cyber-defence related crisis management and receives information and provides political guidance on any major cyber incident or attack.

The key political body subordinate to the NAC is the Cyber Defence Committee (CDC), which consists of representatives from the Allied countries and IS and IMS staff. CDC provides NAC with proposals and recommendations and develops political guidance and cyber defence policy.

The Cyber Defence Management Board (CDMB), which meets on several occasions annually, is responsible for the coordination of cyber defence efforts across the Alliance. Its scope permeates all relevant NATO bodies, regardless of their nature, be it political, technical or military. Stakeholders from the International Staff, International Military Staff and respective relevant bodies all get a seat at the table.

The Consultation, Command and Control (C3) Board provides technical and implementation guidance. Similar specific responsibilities lie with the NATO Military Authorities (NMAs) and the NATO Communications and Information Agency (NCIA). The Allied Command Transformation (ACT) based in Norfolk, Virginia, is responsible for the continuous adaptation of the Alliance to new challenges. In the cyber defence field, ACT is also responsible for the organisation of the annual Cyber Coalition exercise.

Last but certainly not least, NCIA's NCIRC centres are at the forefront of securing NATO's cyber defence technically as well as of coordinating efforts both within NATO and with other international organizations. A key Cyber Operations Centre is presently being set up after being established in August 2018.[9]

This robust setup has evolved for almost 20 years along with NATO's cyber policies, which provided the respective bodies with the mandate to conduct their duties. At the very beginning of the process, however, NATO had been awfully unprepared for the initial set of challenges it was about to face, and – as the following paragraphs will illustrate – most of the progress in the area in fact resulted from decisions taken in the past dozen years or so.

TRACKING THE EVOLUTION OF NATO'S POLICY APPROACH TO CYBER DEFENCE

The 1999 Strategic Concept as a Prelude to a Cyber-Aware NATO

In spite of the fact that the threat of cyber-attacks is for the first time mentioned verbatim in the 2002 Prague Summit Declaration, one could argue that it was in fact the year of 1999 that one could view as the key milestone in the first recognition and jumpstart of NATO's approach to cyber defence. Two notable events, which took place in April 1999, support this argument.

The first of these were the cyber-attacks orchestrated by Serbian and Russian hackers against NATO systems and networks during the Kosovo War. Later, after the mistaken bombing of the Chinese embassy in Belgrade, they were joined by hackers hailing from China. These cyber attacks, an oft-forgotten component of the 1999 Kosovo campaign, mostly took shape of denial of service type intrusions and website defacements, and on

[9] NATO. 2018. *Cyber Defence*. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm.

several occasions succeeded in taking down servers and websites operated by NATO and the U.S. military.[10]

The second, and in this context arguably even more important, development was the adoption of the new Strategic Concept first released on 24th April 1999, which notably resulted in the Alliance broadening its approach to security threats. Apart from traditional military threats, NATO took note of the evolving strategic environment, and redesigned its purpose to be able to also respond to new emerging threats and other "*non-military risks which are multi-directional and often difficult to predict.*"[11]

These threats included "*serious economic, social and political difficulties. Ethnic and religious rivalries, territorial disputes, inadequate or failed efforts at reform, the abuse of human rights, and the dissolution of states can lead to local and even regional instability. The resulting tensions could lead to crises affecting Euro-Atlantic stability, to human suffering, and to armed conflicts. Such conflicts could affect the security of the Alliance by spilling over into neighbouring countries, including NATO countries, or in other ways, and could also affect the security of other states.*" Other explicitly mentioned issues included proliferation of nuclear, biological and chemical weapons, acts of terrorism, sabotage, organized crime, disruption of the flow of vital resources, migration – particularly as consequence of armed conflicts – or the global spread of technology that can be of use in the production of weapons.

The very groundwork for subsequent expansion of NATO's cyber defence policies and capabilities is then laid forward in paragraph 23: "*In addition, state and non-state adversaries may try to exploit the Alliance's growing reliance on information systems through information operations designed to disrupt such systems. They may attempt to use strategies of this kind to counter NATO's superiority in traditional weaponry.*"[12]

It is unclear whether this statement was prepared well in advance or put together hastily in the light of transpiring events. However, prior to the adoption of the 2010 Strategic Concept, it served as the very framework and basis for the development of capabilities required to tackle these threats on which the respective Summit Declarations of the 2000s have since built upon.

The need to be able to address emerging threats was cemented by the 9/11 terrorist attacks in the United States, which have further demonstrated that at a time when an interstate armed conflict in the trans-Atlantic area seemed rather unlikely in the foreseeable future, the so-called emerging threats were to play a key role in security matters in the early 21st century.

The first cyber defence capabilities of NATO countries (such as the U.S. or the United Kingdom) were thus developed as a response to cyber-attacks being considered a likely component of any future crisis as well as a new requirement to securing the systems, networks and services of NATO missions deployed all over the world, including missions

[10] Healey, Jason (ed.). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington: Cyber Conflict Studies Association, pp. 50-51.
[11] NATO. 1999. *The Alliance's Strategic Concept*. Available at: https://bit.ly/2MMVGpB
[12] Ibid.

aiming to curb the threat of world-wide terrorism.[13] The strategic thinking reflected the lessons learned from conflicts of the 1990s.

Baby Steps: Recognition of Cyber Threats, Establishing the NCIRC

NATO first recognized both the existence of cyber threats and the need to protect its networks during the 2002 Prague Summit. One of the decisions made there also included establishing the NATO Computer Incident Response Capability, or NCIRC, which is the body that provides technical and legislative support services to respond to computer security incidents within NATO computer systems and networks.[14] Currently based at SHAPE,[15] Mons, Belgium, NCIRC "*protects NATO's own networks by providing centralised and round-the-clock cyber defence support to the various NATO sites.*"[16]

The impact of the recognition should not be overestimated, as the 2002 Prague Summit Declaration mentioned cyber defence only briefly in article 4f, where the decision to "*[s]trengthen our capabilities to defend against cyber-attacks*" was explicitly expressed.[17]

From today's perspective, the recognition is to be understood as a reactive decision in light of the increasing attacks on Allied networks. As previously mentioned, the first major attacks targeting NATO's networks occurred during the Operation Allied Force in the Kosovo war of 1999, when Serbian and Russian hackers reportedly conducted Distributed Denial of Service (DDoS) attacks in response to the Alliance's involvement in the conflict. Chinese hackers later joined in on the fray, after the Chinese embassy in Belgrade was accidentally bombed.[18] However, the first cyber espionage case targeting networks of U.S. universities and military bases took place in 1986[19] and computer systems and networks in Allied countries were hit by politically motivated hackers as far back as 1989, with several more incidents occurring in the 1990s.[20] Given the timeframe, NATO was significantly lagging behind some of its respective member states in terms of identifying new threats.

The decision to establish the NCIRC would thus seem to be in accordance with the 1999 Strategic Concept, which for the first time affirmed the Alliance's commitment to a broad approach to security, and probably in response to the attacks on NATO's networks first

[13] Healey, Jason (ed.). 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington: Cyber Conflict Studies Association, pp. 251-264.
Rid, Thomas. 2016. *Rise of the Machines. A Cybernetic History*. New York: W. W. Norton & Company Inc., pp. 294-339.
Stiennon, Richard. 2015. *There Will Be Cyberwar: How the Move to Network-Centric War Fighting Has Set the Stage for Cyberwar*. Birmingham: IT-Harvest Press.
[14] NATO. 2002. *Prague Summit Declaration*, para. 4f. Available at: https://bit.ly/2XaxMZ3
[15] Supreme Headquarters Allied Powers Europe.
[16] NATO. 2018. *Cyber Defence*. Available at: https://bit.ly/2BuWGFf
[17] Ibid.
[18] Supra note 4.
[19] Stoll, Cliff. 2015. "*The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*." New York: Pocket Books.
[20] Further high-profile attacks include the 1989 NASA hack through the WANK worm, activities by the Electronic Disturbance Theater throughout the 1990s, the Strano Network and its virtual sit-in on websites of French government agencies, etc. See Tim Jordan, 'Hacktivism: Direct Action on the Electronic Flows of Information Societies' in: Keith Dowding, Jim Hughes and Helen Margetts (eds.), 'Challenges to Democracy: Ideas, Involvement and Institutions' Palgrave Macmillan (8 August 2001), pp. 118-131.

manifested the threat posed by its growing reliance on information systems that could be exploited or degraded. A presentation given by Suleyman Anil, then Head of the NCIRC Coordination Centre within the NATO Office of Security, on 15th January 2004 in Madrid during the 11th TF-CSIRT Meeting however states that in part the development of the NCIRC was made possible by the momentum of 9/11.[21] This seems to be supported by the 2002 Prague Summit Declaration, where cyber defence measures could be construed as being undertaken in order to ensure the proper functioning of computer networks and systems on missions where NATO forces are deployed.[22]

Explicit mentions of areas pertaining to the field of cyber defence are present in neither of the declarations from the Istanbul Summit of 2004[23] nor the Heads of State and Government meeting in Brussels in 2005.[24] These summits mostly revolved around issues such as terrorism and proliferation of weapons of mass destruction, the situation in Afghanistan, Iraq and/or the Balkans, etc. In light of the aforementioned issues as well as the landmark 2004 NATO enlargement, which again highlighted the capability gaps between the Allies (not just amongst the newcomers, but also the longstanding members of the Alliance), it is understandable that the already recognized, but not yet fully understood field of cyber defence did not receive much attention at all.

The 2006 Riga Summit's final communiqué however fleshes out how NATO's forces must continue to adapt, with 'work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber-attack' being one of the included initiatives.[25] Even though Riga put the cyber agenda back on the map after a brief lull, cyber defence would likely not take off as much had it not been for a game-changing attack on one of the member states.[26]

Estonia, Bucharest and Beyond: Ramping Up

The 2007 cyber attacks on Estonia that accompanied protests against the decision to move the statue of the Bronze soldier from the city centre of Tallinn to its outskirts mark a drastic shift of development in regards to NATO's approach to cyber defence.[27] While the actual effects of the cyber campaign, which mostly consisted of DDoS attacks, in

[21] Suleyman Anil. 2004. *NCIRC (NATO Computer Incident Response Capability*. Available at: https://bit.ly/2ZmEBUP
[22] Supra note 12.
[23] NATO. 2004. *Istanbul Summit Communiqué*. Available at: https://bit.ly/2MPlgdD
[24] NATO. 2005. *Statement issued by the Heads of State and Government participating in a meeting of the North Atlantic Council in Brussels*. Available at: http://www.nato.int/docu/pr/2005/p05-022e.htm
[25] NATO. 2006. *Riga Summit Declaration*, para. 24. Available at: https://bit.ly/2MXrV5g
[26] This sentiment is not universal. Goździewicz argues the first instance of Cyber Defence Policy was developed as a result of the Riga Summit. See Goździewicz, Wiesław. 2016. From Riga to Wales. NATO's Road to Collective Cyberdefence. In: Świątkowska, Joanna (ed.). *NATO Road to Cybersecurity*. Kraków: The Kosciuszko Institute.
[27] Andreas Schmidt. 2012. The Estonian Cyberattacks. In: Jason Healey (ed.): *A fierce domain: conflict in cyberspace 1986-2012*. Arlington: Cyber Conflict Studies Association, pp. 174-193.
Kaplan, Fred. 2016. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, pp. 145-170.

hindsight did not prove to be as sinister as the initial reaction might have suggested,[28] the events did play a key role in shaping the discourse for years to come.

In the aftermath of the events in Estonia during the spring of 2007, the first NATO Policy on Cyber Defence was defined and approved in January 2008.[29] It was this very iteration of the Policy, along with the subsequent Bucharest Summit, that laid the actual foundation of NATO's policy approach toward cyber defence, almost ten years after the Alliance first bore the brunt of cyber attacks. In spite of the Summit bringing the attention to emerging threats in general (including cyber defence), these were only mentioned at the end of the Summit Declaration, once again suggesting that the topic was still not considered the top Allied priority at the time.[30]

The established framework however included first key principles, such as that NATO and the Allies should protect their key information systems in accordance with their respective responsibilities, share best practices and provide a capability to assist Allied nations, upon request, to counter a cyber-attack (in line with the Article IV of the Washington treaty).[31]

The Alliance also pledged to continue the development of cyber defence capabilities and to strengthen the linkages between NATO and national authorities. Requirements for NATO systems and recommendation for the Allies were also fleshed out and the Cyber Defence Management Authority (later replaced by the Cyber Defence Management Board, or CDMB) was created.

If there was any room left for doubt vis-à-vis the necessity of these measures, the notion was quickly dispelled in summer of 2008, as armed forces of the Russian Federation invaded Georgia. The footsteps of Russian soldiers onto Georgian soil were accompanied by a well-orchestrated campaign of attacks in cyberspace,[32] further providing credence to the idea that, at the very least, cyber-attacks will be used as a tactical force multiplier in virtually every military campaign to come, and that they pose a clear threat to the mission and interests of the Alliance.

There were numerous reasons as to why the Russian leadership opted for the military campaign, but one notably stands out – just months prior, in the Bucharest Summit Declaration, NATO welcomed Ukraine's and Georgia's aspirations for membership in NATO with the premise that they could eventually become Allies by making it clear the Alliance supports both countries' application for a Membership Action Plan.

The Russian response was thus likely premeditated and probably aimed at preventing Georgia from joining the Alliance. As the official NATO policy includes the precondition that international, ethnic or external territorial disputes are settled by peaceful means

[28] The Estonian defence minister reportedly considered asking for the invocation of the Article V of the Washington Treaty. The attacks are still sometimes being referred to as "the first cyberwar".
[29] NATO. 2018. *Cyber Defence*. Available at: http://www.nato.int/cps/en/natohq/topics_78170.htm
[30] NATO. 2008. *Bucharest Summit Declaration.* Available at: https://bit.ly/1km1TEJ
[31] Ibid.
[32] Hagen, Andreas. 2013. The Russo-Georgian War 2008. In: Healey, Jason (ed.). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington: Cyber Conflict Studies Association, pp. 194-204.
Kaplan, Fred. 2016. Dark *Territory: The Secret History of Cyber War*. New York: Simon & Schuster, pp. 164-166.

prior to a country joining the Alliance,[33] Georgia is de facto prevented from gaining membership due to the frozen conflicts with Abkhazia and South Ossetia as well as the fact that both of the territories declared independence from Georgia in the aftermath of the war, despite these claims being largely internationally non-recognized.

In 2009, the Strasbourg-Kehl Summit Declaration stressed the commitment to strengthening communication and information systems that are of critical importance to the Alliance against cyber attacks. Apart from detailing numerous successes (such as NATO having adopted the policy, improved the NCIRC, and established the CDMA), the Declaration stated that cyber defence was to be made an integral part of NATO exercises, the development of cyber defence capabilities was to be further accelerated, and the cooperation between NATO and Partner countries and even with international organizations (albeit with the caveat of 'as appropriate')[34] was to be improved. Last, but not least, the Declaration celebrated the successful establishment of the NATO Cooperative Cyber Defence Centre of Excellence, a think-tank created in Tallinn in the wake of the 2007 attacks on Estonia and accredited by NATO.

The Declaration on Alliance Security, another document that was adopted at the Summit in April 2009, inter alia called for a new Strategic Concept for the Alliance.

From Lisbon to Wales: New Concept and Policy

The 2010 Strategic Concept was developed in the run-up to the 2010 Lisbon Summit, where it was adopted along with the Lisbon Summit Declaration. Apart from the general realization that cyber defence will likely remain a key security topic for the foreseeable future and that future conflicts taking place all around the world are highly likely to include a cyber dimension, the two documents clearly reflect on the lessons learned from computer network operations observed in Estonia in 2007 and in Georgia in 2008 and push for integration and coordination of cyber defence throughout the Alliance.

The Strategic Concept lists cyber threats as well as potential threat actors – foreign militaries and intelligence services, organized criminals, terrorist and extremist groups. Cyber defences and resilience – the ability to quickly recover from a cyber-attack – are pointed out as priorities. Moreover, the NATO Defence Planning Process (NDPP) is to be used to enhance and coordinate the Allied cyber-defence capabilities. All NATO bodies are to be brought under a centralized cyber protection and NATO cyber awareness, warning and response with Allied nations to be better integrated.[35]

The Lisbon Summit Declaration first mentions the rapid increase in cyber threats and their sophistication. It states that NATO's permanent and unfettered access to cyber space and the integrity of its critical systems need be ensured, and the cyber dimension of modern conflicts needs to be taken into account by NATO. Furthermore, the resilience of the systems and the capabilities of the NCIRC were to be boosted.[36]

[33] Schweickert, Rainer, Melnykovska, Inna and Hanno Heitmann. 2010. *NATO Accession Conditionality for Post-Socialist Institutional Change – From Cross-Country Evidence to the Case of Macedonia*. Available at: https://bit.ly/31zbKyD

[34] The paragraph was likely watered down due to positions of Turkey and/or the other non-EU Member States.

[35] NATO. 2010. *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Available at: https://bit.ly/1uFACMD

[36] NATO. 2010. *Lisbon Summit Declaration*. Available at: https://bit.ly/1hWSlhP

The North Atlantic Council was subsequently tasked to develop a new, revised and in-depth iteration of NATO Cyber Defence Policy by June 2011 and to prepare an action plan for its subsequent implementation. The Policy included several important goals: the NCIRC was to achieve Full Operational Capability (or FOC) by the end of 2012 and all NATO bodies were to be brought under its wings. As part of this measure, the Alliance was to set up cyber Rapid Reaction Teams (RRTs) consisting of national or NATO experts that could be quickly deployed should a severe attack befall an Ally.[37] In turn, the NCIRC became part of the NATO Communications and Information Agency (NCIA), which overtook the responsibility for NATO's centralised cyber protection.[38]

For further development of the Allies' cyber defence capabilities, to assist the Allies upon their request in accordance with the Article IV of the Washington treaty and to optimise information sharing and interoperability, in accordance with the Strategic Concept, NATO's defence planning processes were to be followed. NATO also committed itself to work closely with other international organizations, such as the United Nations, the Council of Europe, Organization for Security and Co-operation in Europe, and the European Union, again with a caveat of 'as agreed'.[39] In this regard, in hindsight, the second iteration of the Cyber Defence Policy along with the Cyber Defence Concept and Cyber Defence Plan should be seen as aspirational, with limited outcomes at this point in time.

The Chicago Summit held in May 2012 and its Declaration subsequently echoed the aforementioned goals that were embedded in the policy and its implementing documents.[40]

The Wales Summit and the Enhanced Cyber Defence Policy

In February 2014, Allied defence ministers tasked NATO to develop a new iteration of the cyber defence policy. The Enhanced NATO Policy on Cyber Defence was successfully adopted in June 2014. Its implementation is supported by the Cyber Defence Action Plan, which contains specific objectives and timelines. Just prior to the implementation, in May 2014, the NCIRC achieved its slightly delayed full operational capability.[41]

By far the most important aspect of the 2014 policy is that the cyber defence has for the first time been officially established as part of NATO's core task of collective defence. NATO is held responsible for the protection of its own networks, while the respective Allies are responsible for their own communication and information systems and networks. The applicability of international law to cyberspace has also been confirmed by the Heads of State and Government.

Other key aspects include streamlined cyber defence governance, establishing of procedures for assistance to Allied countries, the integration of cyber defence into operational and contingency planning, and improvements to awareness, education,

[37] NATO. 2012. *NATO Rapid Reaction Team to fight cyber attack*. Available at: https://bit.ly/2WJzUHN
[38] Goździewicz, Wiesław. 2016. From Riga to Wales. NATO's Road to Collective Cyberdefence. In: Świątkowska, Joanna (ed.). *NATO Road to Cybersecurity*. Kraków: The Kosciuszko Institute.
[39] Supra note 7.
[40] NATO. 2012. *Chicago Summit Declaration*. Available at: https://bit.ly/2Ri0MZx
[41] NATO. 2018. *Cyber Defence*. Available at: https://bit.ly/1xoc3bM

training and exercises activities. The Allies further committed themselves to enhance mutual information sharing and assistance.

The development of capabilities will be facilitated by an Alliance-wide approach via the NATO Defence Planning Process (NDPP). Cyber defence capabilities and their development were also integrated into NATO's Smart Defence initiative. Specific projects included the Malware Information Sharing Platform (MISP) project, the Smart Defence Multinational Cyber Defence Capability Development (MN CD2) project, and the Multinational Cyber Defence Education and Training (MN E&T) project.

Moreover, an initiative to boost cooperation with industry and academia on cyber threats and challenges was launched in accordance with the new policy in September 2014. The NATO Industry Cyber Partnership (NICP) framework was endorsed at the Wales Summit and later presented at an industry conference held in Mons, Belgium.[42]

The Wales Summit Declaration from September 2014 built upon the Enhanced NATO Cyber Defence Policy, reaffirming the need for the Allies to strengthen the cyber security of their national networks upon which NATO depends for its core tasks and for the entire Alliance to further develop both bilateral and multilateral cooperation. Relevant partner nations as well as other international organisations are to be engaged on a case-by-case basis, with the European Union explicitly named as an example, again with the caveat of 'as agreed'. The development of a NATO cyber range, which was to be built on the existing Estonian cyber range capability, was another notable decision of the Wales Summit.[43]

A two-day May 2015 meeting in Antalya, Turkey marked an official NATO-EU agreement on the cooperation in countering hybrid warfare, which also includes cyber threats. This was an important step, since until then the NATO-EU cooperation in cyber security mostly consisted of high-level staff-to-staff consultations that took place annually since 2010. Prior to that, initial cooperation in the field was only facilitated by informal ad hoc staff-to-staff talks, in which relevant bodies from each organisation participated.[44]

The Way Forward: The Warsaw Summit and the Adoption of Offensive Capabilities in Brussels

As the Alliance moved toward the Warsaw Summit, it had to cope with a new set of challenges that put cyber defence at the forefront. The two greatest were the resurgence of aggressive Russia in Ukraine as well as the spread of the so-called Islamic State in Syria and Iraq, including its various cells and offshoots in Europe and elsewhere.

Warsaw was thus expected to further build on the foundation laid by the 2014 Enhanced NATO Cyber Defence Policy and the Cyber Defence Action Plan, which were at that point still being implemented. However, the end-result that manifested in two important declarations exceeded expectations.

While the Allies reaffirmed NATO's defensive mandate and the intent to continue to follow the principle of restraint, steering clear of expanding the mandate to include offensive operations, the Warsaw Summit Declaration recognises "*cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on*

[42] Ibid.
[43] NATO. 2014. *Wales Summit Declaration*. Available at: https://bit.ly/1AeY2eg
[44] EEAS. 2016. *EU and NATO cyber defence cooperation*. Available at: https://bit.ly/1RpvwDz

land and at sea." With the rationale being that as most crises and conflicts have and will continue to have a cyber dimension or element, the intent of treating cyberspace as a domain should result in enabling NATO to better protect and conduct its missions and operations.[45]

In its essence, the decision has raised the priority of cyber defence by equalizing it with the other three domains, enabled NATO to tackle the challenges at an operational level and broadened the range of potential responses to cyber attacks.

The second important outcome produced at the Warsaw Summit was the Cyber Defence Pledge, a declaration made at the highest political level of Heads of State and Government that recognizes new realities of the trans-Atlantic security environment and pledges that the Allies will enhance their cyber security by developing "*the fullest range of capabilities*" as a matter of priority, reinforce resilience and defences in the Euro-Atlantic region and continue working on improving international cooperation and facilitating cooperation through multinational projects. In terms of enhancing national cyber defence capabilities, the Pledge ranks among the most important agreed documents to date, as it required attention and decision-making at the highest levels.

To ensure that the Cyber Defence Pledge does not end up a mere empty declaration, the Allies stressed that progress would be tracked by an annual assessment based on agreed metrics and reviewed at the next summit.[46] The metrics probably would have been developed by 2017, their setup and manner of reporting will in all likelihood be instrumental to either the success or the downfall of the Pledge.

The Cyber Defence Pledge reasserts NATO's ongoing adaptation to the threat environment, a realization that, in cyber defence, the Alliance is only as strong as its weakest member, and a long-term shift to building resilience. Apart from other benefits including a more stable infrastructure and less downtime in case of an event or incident taking place, in a field where traditional deterrence models in many cases are no longer adequate, resilience can also "*work as a form of post-even deterrence-by-denial, which, if successful, may reduce adversaries' cost-benefit analyses.*" Such a framework accepts "*that cyberattacks will happen, recognizing that this is not necessarily a 'deterrence failure' but may represent an opportunity to learn and adapt.*"[47]

Furthermore, in February 2017, Allied defence ministers approved an updated Cyber Defence Action Plan along with a roadmap to implement cyberspace as a domain of operations, and, in June of the same year, they also agreed to a new set of cyber defence capability targets.[48]

The years 2016 and 2017 also set new milestones in terms of NATO-EU cyber defence cooperation. Even prior to the Warsaw Summit, in February 2016, NATO and the EU agreed on a Technical Arrangement on Cyber Defence, which set up a framework that allows the NCIRC and the Computer Emergency Response Team of the EU (CERT-EU) to exchange information and share best practices to prevent and respond to cyber attacks.[49]

[45] NATO. 2016. *Warsaw Summit Communiqué*. Available at: https://bit.ly/2hI5l96
[46] NATO. 2016. *Cyber Defence Pledge*. Available at: https://bit.ly/2WGyttH
[47] Pijnenburg, Lilly and Tim Stevens. *Upholding the NATO cyber pledge. Cyber Deterrence and Resilience: Dilemmas in NATO defence and security politics*. Oslo: Norwegian Institute of International Affairs. Available at: https://bit.ly/2wl3fXt
[48] NATO. 2018. *Cyber Defence*. Available at: https://bit.ly/2BuWGFf
[49] Ref. 48

In summer, the agreed Warsaw Summit Declaration further reasserted the intent to cooperate with the EU (albeit again with the caveat of "*as agreed*"). Apart from cooperation at the technical and tactical levels, the key form of cooperation consists of information sharing. For instance, during the 2017 WannaCry and NotPetya campaigns, NATO shared information about the threats with the EU, nations and private companies in real time.[50] While threat intelligence and information sharing are both vital in coordinating responses and tackling cyber threats, this information exchange was not always feasible, as the confidential nature and limited releasability of intelligence in both organizations that consist of different member states often prevents full disclosure. Moreover, in December 2016, NATO and EU agreed on a package of over 40 measures aimed at managing hybrid threats, which again included cyber defence.

These decisions would further build upon the outcomes of the Warsaw Summit. However, for the time being the cooperation is likely to remain limited to the tactical or in rare cases operational levels. Firstly, it is because the two organizations focus on different agendas, with NATO focusing predominantly on capacity building and preparedness in cyber defence while the EU zooms in on regulation and cyber security best practices (through mechanisms such as the NIS Directive). Secondly, in terms of institutional, policy and organisational preparedness, NATO is ahead of the EU, which only adopted its first cyber defence policy framework in late 2014[51] and which cannot compare to NATO in terms of institutional and organisational build-up, where NATO had a notable head start. Finally, while both organisations can each step in to help the other out, the Allies (and especially the non-EU Member States among them) will be wary of any potential duplication taking place.

The 2018 Brussels Summit and the Future: On the Offensive?

Despite not making for the most visible highlights, cyber defence was featured very prominently on the agenda during the Brussels Summit.

The 2018 Brussels Summit Declaration has references to cyber defence littered throughout the document. In an output in which every last comma is carefully weighed, discussed and argued over, it highlights both the importance the Alliance currently ascribes to cyber defence as well as the development the agenda has undergone in the past twenty years.

By far the most impactful decision that the Allies agreed on and had embedded in the Declaration are the continued efforts to implement cyberspace as a domain of NATO operations and missions. For the first time ever, the Alliance took the decision to employ the full range of cyber capabilities, including "*sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, in the framework of strong political oversight.*"[52] This is in stark contrast to the previous assertions, in which NATO continually reaffirmed its strictly defensive posture for cyber operations.

Moreover, the 20th paragraph of the Declaration stressed the need for bolstering intelligence-led situational awareness for decision-making, encouraged the respective

[50] Stoltenberg, Jens. 2018. *Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris)*. Available at: https://bit.ly/2KIfnJ1
[51] The EU Cyber Defence Framework was subsequently upgraded in a 2018 update. See Council of the European Union. 2018. *EU Cyber Defence Policy Framework (2018 update)*. Available at: https://bit.ly/2DJZtO9
[52] NATO. 2018. *Brussels Summit Declaration*. Available at: https://bit.ly/2mb5ZUo

Allies to attribute cyber attacks when appropriate, and reasserted NATO's previous commitments of Cyber Defence Pledge and the applicability of international humanitarian law and human rights law (with a caveat) to cyberspace. NATO, furthermore, committed to supporting peace, promoting stability and working with the industry and academia.[53]

The decision to potentially go on the cyber offensive taken at the summit is a major development in the overall picture of the Alliance. Despite being somewhat overshadowed by the antics of the U.S. president Trump as well as his demands for the Allies to ramp up their defence spending to at least 2% of their national GDP,[54] in essence the Alliance has redefined its strategic cyber defence posture to also include an offensive component.

NATO has thus clearly re-evaluated its previous position, and the Alliance has embarked on a gradual shift towards a more proactive and offensive posture, which will allow it to utilize a wider range of potential responses to being targeted.

In order for the decision to be implemented, in August 2017 NATO established, and is currently in the process of setting up, a Cyber Operations Center, or CyOC, in Mons, Belgium. The command centre is to be fully staffed and operational by 2023. Even though ground rules are still being pondered over and the current policy may yet change, currently the likely vision of the centre is to serve as a conduit for the coordination of national contributions to NATO operations and missions, as the Allies have decided to only provide voluntary effects, not capabilities per se. These could be likened to hacking-as-a-service. At full strength, the centre aims to staff a 70-strong team of experts. The CyOC will also closely cooperate with existing bodies that protect NATO, namely the NATO Communications & Information Agency and the NATO Cyber Incident Response Capability technical centre.[55]

The utilization of the offensive element and the setting up of the CyOC also suggest the likely cyber agenda for NATO for the years ahead. Apart from efforts to strengthen national defences through continued implementation of the Cyber Defence Pledge, challenges that the Allies will have to face together in the near- and medium-term will probably include fleshing out mechanisms to attribute attacks and coordinate national contributions to operations and missions. While a push by some European Allies for greater cooperation with the European Union and possibly other international organisations is considered possible, greater progress is probably unlikely, as the immediate concerns and priorities of the respective organisations are somewhat disparate, with the notable exception of the NATO-EU threat environment, which may provide potential for greater information-sharing and cooperation at the tactical and operational levels.

[53] Ibid.
[54] MacAskill, Ewen. 2018. *How Trump's Nato summit meltdown unfolded*. Available at: https://bit.ly/2F5ZnAb
Diamond, Jeremy. 2018. *Trump drama overshadows NATO summit*. Available at: https://cnn.it/2WBXdhW
Herszenhorn, David M. and Lili Bayer. 2018. *Trump's whiplash NATO summit*. Available at: https://politi.co/2KOW1Xr
[55] Emmott, Robin. 2018. *NATO command to be fully operational in 2023*. Available at: https://reut.rs/2MP5Jud
Freedberg, Sydney J. Jr. 2018. *NATO To 'Integrate' Offensive Cyber By Members*. Available at: https://bit.ly/2zen4DO
Brzozowski, Alexandra. 2018. *NATO sees new cyber command centre by 2023 as Europe readies for cyber threats*. Available at: https://bit.ly/2JddfcM

CONCLUSION

The cyber defence approach of the North Atlantic Treaty Organization stems from the organisation's aims and overall needs rooted in its three core tasks of collective defence, crisis management and cooperative security. After all, NATO's main purpose is to ensure security and stability in the Euro-Atlantic region. The successes and limits alike are largely based on the fact that NATO is an intergovernmental organization with a consensus-based decision-making. As per its 2014 Enhanced NATO Cyber Defence Policy, cyber defence is understood as part of NATO's core task of collective defence.

The evolution of NATO's approach to cyber defence dates at least as far back as 2002, however, the importance of the field seems not to have been fully grasped until Estonia became victim to a series of cyber attacks in 2007.

The first iteration of NATO's cyber defence policy along with the Bucharest Summit Declaration have subsequently laid the foundation to tackle the emerging cyber threats. As the evolution continued further, more improvements were made possible by the Lisbon Summit Declaration, the 2010 Strategic Concept and most importantly the revised 2011 Enhanced NATO Cyber Policy, which was later reaffirmed by the 2012 Chicago Summit. In hindsight, at this point, the policies and measures taken could still be seen as aspirational and limited, i.e. cybersecurity still lingered in a state of void in terms of technologies, institutional and policy preparedness, as well as legal background.

15 years of Allied efforts culminated in 2014, when the new Enhanced NATO Cyber Defence Policy broadened NATO's mandate and the Heads of State and Government publicly recognized at the Wales Summit that cyber defence is part of NATO's core task of collective defence. Together with the recognition of applicability of international law to cyberspace, these two Wales Summit decisions might very well be the most important of all those taken within the agenda in terms of their impact, as they could directly result in the invocation of Article V in a severe cyber-enabled crisis. These decisions and the realization of their implications will continue to bolster the Alliance's resilience and preparedness in light of the contemporary cyber threat landscape. Furthermore, the establishment of NATO Industry Cyber Partnership has increased NATO's potential to cooperate with the private sector and obtain innovative technologies.

The recognition of cyberspace as a domain that was agreed at the Warsaw Summit in summer of 2016 provided the Alliance with more manoeuvrability required to conduct defensive cyber operations. On the national level, the Cyber Defence Pledge also adopted in Warsaw by the top decision-makers – the Heads of State and Government – could provide a remarkable instrument, provided that the Allies have come up with granular, verifiable metrics that will serve to establish a baseline and track progress, and that they will consciously decide for and uphold an allocation of substantial funds for necessary investments over a long-term period.

In terms of NATO's cyber defence posture, the 2018 Brussels Summit was then nothing short of revolutionary, as the Alliance took the decisive step that would allow it to conduct offensive cyber operations based on voluntary cyber effects supplied by the respective Allies. The CyOC that is being established will take years to achieve full operational capability, and prior to that it is likely that the Allies will continue their efforts to specifically flesh out the mechanisms as to how exactly national contributions and Allied efforts will be coordinated and how operations are to be undertaken. The

Alliance will also need to tackle the difficult task of fleshing out and agreeing on the attribution process.

Indeed, the three summits of 2014, 2016 and 2018 will in hindsight probably be considered as instrumental in cementing both the Alliance's cyber defence policy and posture as well as forging a mechanism for the Allies to further invest in developing national capabilities.

Despite continually reaffirming its adherence to the principle of restraint and norms of responsible state behaviour in cyberspace, throughout its declarations NATO stresses that it only observes the process of establishing these norms. The apparent reluctance likely stems from a self-awareness that it would not bode well for a political-military alliance to be the vehicle of Western interests in the process, and that the United Nations and OSCE are a more suitable arena for shaping the discussion.

In terms of capabilities and capacity building, NATO's key decisions and successes were the establishment of NATO Computer Incident Response Capability in 2002 and its further development to full operational capability achieved in May 2014, the establishment of NATO Communications and Information Agency, the decision to establish the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, in the wake of the 2007 cyber attacks on the country, the development of Rapid Reaction Teams for the field of cyber defence or the recent decision to establish a cyber defence range based on the existing Estonian capability. The most important decision going forward has been to set up the proposed Cyberspace Operations Centre (CyOC) in Belgium by 2023.

In terms of actionability, NATO has undertaken significant endeavour in terms of trying to approach the issue of cyber defence in a more proactive fashion, despite being somewhat constrained by the need to reach consensus on every decision taken. This is in stark contrast with the slow and reactive beginnings twenty years ago.

From an outside view, the first steps in the aftermath of the Operation Allied Force yielded no tangible results. Likely due to NATO's inability to prioritize the security of Allied computer systems and networks and to make them a point of focus prior to the 9/11 terrorist attacks, the agenda was overshadowed by more pressing matters of the early 2000s, such as the war against terror or the massive NATO enlargement of 2004.

However, even though the Alliance first adopted proper policies only in the wake of the 2007 attacks on Estonia, it has since come a long way in laying the necessary groundwork to face its looming challenges. In the past 10 years, much progress has been made on both the policy and institutional preparedness fronts.

It no longer holds true that NATO is inadequately prepared for cyber crises of today. The compounding effect of the 2014-2018 summits may well translate to a significant rise in Allied levels of preparedness. NATO currently seems well positioned to provide guidance and lead its Member States in developing the capabilities required to tackle the threats that are bound to come. However, the Alliance must now focus on the actual implementation of all the agreed-upon policies, frameworks and procedures the Allies have developed together.

In terms of NATO doing enough to boost the capabilities of the Allies and prepare them for threats emerging from the cyberspace, one could argue that it has successfully promoted best practices and pushed the respective member states to increase their awareness, spending and capacity-building in the area. Given that the Alliance retains a consensus-based decision-making, its progress in the cybersecurity agenda has been

substantial in the past five years. The future outcome will, however, be decided by actions on part of each Ally, under the guiding principle of the Allied chain being as strong as its weakest link.

Notable challenges will continue to lie in the safety and resilience of interconnected systems, vastly different levels of preparedness of the respective Allies as well as disparate commitments to adhering to the Cyber Defence Pledge and spending on the national level, and the eventual implementation of full-scale computer network operations into the ever-broadening portfolio of tools at the disposal of Allied Command Operations.