From 'Armed Attack' to 'Cyber Attack': The Evolution of Collective Self-Defense in NATO

Brooke A. Smith-Windsor

Senior Research Fellow,
RAND Europe

Abstract

In 2014, the world's most powerful political-military alliance in history, the North Atlantic Treaty Organization (NATO), decided to officially associate cyber attacks with its collective self-defense mandate. The development marked a significant milestone in the evolution of the 70 year-old defense alliance with widespread implications for its future military capabilities, doctrine, and partnerships with like-minded states. This paper explains how this landmark decision came about and considers NATO's continued "cyber adaptation" in the perspective of the September 2018 US National Cyber Strategy.

Key Words: *NATO, cyber defense, collective defense, hybrid threat, European Union*

From Armed Attack to Cyber Attack

從「武裝攻擊」到「網路攻擊」
北大西洋公約組織集體自衛的演變

Brooke A. Smith-Windsor

蘭德歐洲智庫 資深研究員

摘　　要

在 2014 年，世界上有史以來最強大的政治與軍事同盟，北大西洋公約組織（北約），正式決定將網路攻擊納入共同防禦之範疇。此發展可謂該防衛同盟 70 年來演進的重大里程碑，廣泛涉及了未來的軍事能力、準則，以及理念相同國家之間的夥伴關係。本文闡釋了此標誌性決議之形成過程，並從 2018 年 9 月美國《國家網路戰略》的案例來思索北約該如何「深化網路防禦」。

關鍵詞：北約、網路防禦、集體防禦、混和威脅、歐盟

Introduction

Founded in 1949, the North Atlantic Treaty Organization (NATO) routinely has been described as the most successful collective defense alliance in history. Today, its 29 (soon 30)[1] member states represent over half of the world's economic and military might collectively pooled to defend the territory and shared liberal democratic values of Europe and North America. NATO's success is a function of its proven ability to adapt to an ever-changing security environment. The Alliance consistently has demonstrated the flexibility to address new threats to transatlantic security whether in terms of actors or capabilities. The shift from preoccupation with a Soviet invasion to concern with global terrorism since 911 is one such adaptation. Its refocus on inter-state warfare and the defense of Europe against a resurgent Russia since 2014 is another. To these can be added recent efforts to bolster defenses against ballistic missiles in view of their proliferation. What is more is NATO's response to threats posed in the cyber domain. As the Alliance's Secretary General, Jens Stoltenberg, remarked in May 2018, "From the moment a rock was first used as a hammer, society has been driven by technology. Today's great leap forward is not physical, but it is digital … But there is a dark side to this technology. In recent years we have seen many large-scale cyber-attacks."[2]

Cyber attacks represent a particularly daunting challenge because they were not envisioned in collective defense terms when the United Nations (UN) Charter was founded in 1945 (Article 51) or when NATO was created four years later. As NATO's founding treaty's collective defense provision (Article 5) states:

> *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*

[1] In July 2018, NATO invited the former Yugoslav Republic of Macedonia to begin accession talks.

[2] Jens Stoltenberg, "Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defense Pledge Conference." Cyber Defense Pledge Conference, May 15, 2018, Paris. Speech. *NATO*, May 15, 2018. https://www.nato.int/cps/en/natohq/opinions_154462.htm.

> *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.*[3]

Nevertheless, at their Wales summit of September 2014, NATO and its member states took the historic step of associating cyber with Article 5. "Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence."[4] This acknowledgment was no small feat considering that all decisions in NATO require consensus. How the Alliance arrived at this point and the policy implications that followed it is the subject of this paper. It begins with a summary of the principal historic events in Europe that helped galvanize NATO's thinking about cyber threats. This is followed by consideration of some of the conceptual foundations that supported official decision-making within the Alliance. The next part examines the components of NATO's formal "cyber adaptation" over the last decade. The paper concludes with observed challenges facing NATO's continued adaptation in the cyber realm.

Real-world Milestones

The 20th century American political journalist, Norman Cousins, observed that "history is a vast early warning system." The words ring no less true when it comes to cyber in more recent times. For NATO, four real-world crises in the European theater were the harbinger of the dark side of the digital age.

---

[3] "The North Atlantic Treaty," *NATO*, 1949, https://www.nato.int/cps/ua/natohq/official_texts_17120.htm.

[4] "Wales Summit Declaration," *NATO*, 2014, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

Kosovo

In 1999, NATO embarked on a 78-day aerial bombardment of the Federal Republic of Yugoslavia to halt mass atrocity crimes in Kosovo. Operation Allied Force succeeded. However, the experience also brought to light in unprecedented terms the vulnerabilities of NATO information systems and networks to cyber assaults during a military campaign. A notable occurrence was the temporary disruption of the NATO public affairs website by pro-Serbian hackers.[5] Not surprisingly, at their first wide-ranging summit since the Kosovo operation, NATO and its member states affirmed the need to "Strengthen our capabilities to defend against cyber attacks."[6]

Estonia

If Kosovo for the first time highlighted the risks to NATO's own information technology (IT) infrastructure, an event taking place eight years later would firmly elevate the Alliance's awareness about the dangers of cyber attacks from the tactical-operational level to the strategic one: where an entire society could be adversely affected. In 2007, three years since becoming a NATO member state, Estonia suffered a distributed denial of service attack (DDoS) on both the public and private (economic) sector networks. While in this instance, the attacks did not result in casualties and physical destruction, their comprehensive nature and the suspicion of state (Russian) sponsorship had not been seen before. NATO's subsequent Strategic Concept (2010) acknowledged the new reality: "Cyber attacks are becoming more frequent, more organised and costlier in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure …"[7]

---

[5] Christine Hegenbart, "Semantic Matters: NATO, Cyberspace and Future Threats." *NATO Defense College Research Paper*, No. 103, 2014, p.3.

[6] "Prague Summit Declaration," *NATO*, 2002, https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

[7] "Strategic Concept – Active Engagement, Modern Defence," *NATO*, 2010, https://www.nato.int/strategic-*concept*/pdf/Strat_Concept_web_en.pdf.

Georgia and Ukraine

Conflict in Georgia and Ukraine in 2008 and 2014 respectively saw the first European case of the coordination of state-sponsored cyber attacks as part of a military campaign with societal-wide disruption. When Russian forces moved into the breakaway republics of Abkhazia and South Ossetia, Georgia's internal communications were effectively shut down. Six years later, a similar yet reportedly 32 times larger DDOS attack, targeted Ukraine as pro-Russian forces seized control of Crimea and fomented separatism in eastern Ukraine.[8] Although Georgia and Ukraine are NATO partners, not members, the lessons from the experience were not lost on the Alliance. As the NATO website acknowledges to this day, "the conflict between Russia and Georgia demonstrated that cyber attacks have the potential to become a major component of conventional warfare,"[9] it also is no coincidence that the association of cyber with Article 5 cited earlier came within months of Russia's illegal annexation of Crimea from Ukraine. Cyber defenses to guard against a similar fate for a NATO member state are now as important as conventional and nuclear ones.

Conceptual Foundations

In tandem with the real-world experiences of cyber attacks in Europe—and informed by them— analysts on both sides of the Atlantic began in earnest to debate the political, legal and military underpinnings of collective defense in the cyber realm. The best-known example is the so-called Tallinn Manual facilitated by the NATO-accredited Cooperative Cyber Defense Center of Excellence, initiated in 2009, first published in 2013 and now in its second edition.[10] It is beyond the scope of this paper to delve into every aspect of the (ongoing) debate. However, highlighting a

[8] Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nation s." *NBC News*, December 18, 2016, https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.

[9] "Cyber Defense." *NATO*, July 16, 2018. https://www.nato.int/cps/en/natohq/topics_78170.htm.

[10] Information on the Tallinn Manual's development is available at: https://ccdcoe.org/tallinn-manual.html.

few elements sheds light on the conversation that has helped shape official policy-making in NATO.

Typology of Cyber Threats

A 2013 study published by the NATO Defense College Research Division offered a succinct catalogue of cyber threats ranging from: (i) hacktivism and cyber vandalism; (ii) cyber crime; (iii) cyber espionage; (iv) cyber sabotage; (v) cyber terrorism; (vi) cyber war.[11] The categorization avowedly was important to determining the extent of NATO's involvement in the cyber domain. Beyond the routine protection of NATO's own networks through the Computer Incident Response Capability for instance, the first two contingencies were situated as primarily the subject of civil law enforcement within individual nations. Only the latter four categories were considered to have significant national security implications. And the ones viewed as exhibiting the greatest potential for the infliction of a significant degree of harm on NATO and its member states were cyber sabotage, cyber terrorism and cyber war. In such a scenario Article 4 of the NATO's founding treaty conceivably could be involved—high level consultations if the territorial integrity, political independence or security of any of the member states is threatened—but also possibly Article 5. In the context of NATO's collective defense, the Tallinn Manual's definition of a cyber attack was considered informative: "'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.' The definition is shaped by the result: if a cyber operation is followed by significant destructive consequences, it qualifies both as a cyber attack and as use of force."[12] During the same period, others also argued that cyber attacks that threaten human beings' integrity and cause significant disruption and destruction, within or outside cyberspace, would qualify as the use of force under the UN Charter.[13] In sum, a recurring theme was that when it comes to collective self defense, the severity of negative

[11] Hegenbart, pp.6-10.
[12] Ibid., pp.8-9.
[13] Iulian F. Popa, "NATO's Cyber Security and Defense: Before and After 2014 Wales Summit." *Annals of the "Constantin Brancusi" University of Targu Jiu, Letterand Social Sciences Series*, No. 3, 2014, p.127.

consequences for a society resulting from a cyber attack matters.

The Attribution Challenge

Even if real and considerable harm were to be inflicted on a NATO member through cyber sabotage, terrorism or warfare thus warranting a collective response, analysts have long recognized that cyberspace presents a challenge when it comes to attribution. Whether it be an online terrorist cell, a state's intelligence service or a country's use of "cyber proxies" to do its bidding, a plethora of actors with the conceivable intent and means to disrupt and destroy are active in cyberspace. Moreover, in this domain none need be geographically proximate to the targeted area and encryption shields identities. Yet, without reasonably assured identification of the perpetrators of an attack, determination of the proportionate response including potential retaliation becomes exceedingly difficult. This predicament is perhaps best summed up in a phrase coined by NATO's Secretary General that "Nowhere is the 'Fog of War' thicker than in cyberspace."[14] To break through the cyber fog, writing in 2015, two analysts suggested a multi-layer approach to the question of culpability. As summarized a year later in the paper entitled, "Cyber Operations and Gray Zones: Challenges for NATO," the model is about understanding: (i) how the attack was perpetrated in technical terms (tactical level); (ii) what non-technical factors—determined through signals intelligence and human intelligence for example—combined with the former to realize the attack (operational level); and finally, who masterminded the attack and why (strategic level).[15] Combined, such factors can serve to propel decision-makers closer to the "proof beyond reasonable doubt" threshold when it comes to apportioning responsibility for the large scale disruption and destruction of societies enacted through cyberspace.

Deterrence

As with nuclear and conventional war, states of course wish to prevent cyber attacks before they happen. Here, the question of deterrence comes

[14] Stoltenberg.
[15] Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections*, Vol. 15, No. 2, 2016, pp.114-115.

into play. In cyberspace, an element of self restraint on the part of actors operating within it is "built in." Sometimes this is referred to as "deterrence through interdependence." In other words, some attackers will be wary of going too far to degrade or destroy the IT infrastructure on which they also rely. [16] However, analysts steadily recognized that this type of self-regulation was an unreliable defense. More and more sophisticated attacks as in Estonia, Georgia and Ukraine revealed how widespread disruption to targeted populations and economies could be achieved by a state sponsor without adversely affecting its own. Pro-active deterrence measures, therefore, also would be required. Not surprisingly, advocacy for a retaliatory cyber defense capability on the part of NATO and its member states multiplied. It would have to be credible—able to impose costs on an adversary greater than the gains to be achieved from an attack. And it would have to be deliberately ambiguous—to instill in an adversary uncertainty as to the threshold for NATO retaliation.[17]

Comprehensive Approach

Following the 911 terrorist attacks on the US and NATO's intervention in the place of their origin, Afghanistan, the Alliance realized early-on that it could not act in isolation. Counter-terrorism and stabilization missions required a whole-of-government, inter-agency effort with states working alongside non-state actors each according to its respective mandates and strengths. As a political-military actor, NATO had a role to play but so did others who might at times be in the lead. To recall the common refrain, "Lessons learned from NATO operations show that addressing crisis situations calls for a comprehensive approach combining political, civilian and military instruments. Building on its unique capabilities and operational experience, including expertise in civilian-military interaction, NATO can contribute to the efforts of the international community for maintaining peace, security and stability, in full coordination with other actors. Military means, although essential, are not enough on their own to meet the many

[16] Jamie Shea, "NATO Dealing with Emerging Security Challenges?" *Georgetown Journal of International Affairs*, Vol. 14, No. 2, 2013, p.194.
[17] Fitton, p.117.

complex challenges to our security."[18] Informed by this experience, it was not difficult for analysts to purse similar logic in conceptualizing the Alliance's approach to cyber defense. A 2009 commentary entitled "NATO in Cyberspace" is indicative: "As NATO commanders have learned, defending cyber-based assets is a duty which requires constant, twenty-four hour communication and coordination, mainly with non-military organizations which control more than ninety percent of global cyber infrastructure."[19] For NATO, this would mean moving beyond traditional linkages with foreign and defense ministries, and strengthening ties with interior ministries, intelligence and police services, and national security councils. It also would mean working with the same in partner countries. And to an extent not contemplated in Afghanistan, a comprehensive approach to cyber defense would mean interacting with industry and the private sector as the principal developers and users of information technologies.[20]

NATO's Cyber Adaptation

In 2013, one year prior to NATO associating cyber with collective self defense, its Deputy Assistant Secretary General for Emerging Security Challenges, Jamie Shea, outlined what he saw as the three essential components of the way forward for the Alliance and cyber.[21] Using that blueprint as a guide, this final part explains what has formally transpired in each area over the last decade: *(i) Mandate; (ii) Policy; (iii) Institutionalization and capability development.* Combined, these developments explain how NATO has consensually adapted in official terms to meet the cyber challenge.

---

[18] "A 'comprehensive approach' to crises." *NATO*, June 26, 2018, https://www.nato.int/cps/su/natohq/topics_51633.htm.
[19] Rex Hughes, "NATO in Cyberspace: Digital Defenses." *The World Today*, Vol. 65, No. 4, 2009, p.20.
[20] Shea, p.196.
[21] Ibid., pp.197-198.

Mandate

Delineating a mandate for NATO in cyberspace has necessarily been grounded in its founding treaty. While, as mentioned previously, cyber is not mentioned in the North Atlantic Treaty given the period of its compilation, this fact has not prevented the member states from adapting their interpretation of its principles to fit the digital age. Principally, Articles 3 (capabilities), 4 (consultation) and 5 (collective defense) have been formally implicated drawing on the lessons of the real-world experiences and advice cited earlier. Reference to a selection of official texts is illustrative.

Where Articles 3 and 4 are concerned, the 2010 Strategic Concept is noteworthy. Article 3 of the North Atlantic Treaty commits NATO members to "separately and jointly, by means of continuous and effective self-help and mutual aid, [to] maintain and develop their individual and collective capacity to resist armed attack."[22] The Strategic Concept carried forward the spirit of this article into the cyber domain with a collective member state commitment to "develop further our ability to prevent, detect, defend against and recover from cyber attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations."[23] Building on this earlier interpretation, six years later, the Cyber Defense Pledge (discussed further below) would specifically associate Article 3 with cyber defense capability development.[24] Where Article 4 is concerned, the advocacy for high-level consultations in the event of a member state feeling threatened by a cyber attack has been mentioned. As early as 2010, its translation into official policy may be observed in the Strategic Concept's assertion that "Any security issue of interest to any Ally can be brought to the NATO table."[25]

While the Strategic Concept spoke of deterring and defending against

[22] The North Atlantic Treaty.
[23] Strategic Concept – Active Engagement, Modern Defence.
[24] "Cyber Defense Pledge", *NATO,* July 8, 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.
[25] Strategic Concept – Active Engagement, Modern Defence.

"emerging security challenges" in the perspective of Article 5, as highlighted at the outset of this paper, it was not until 2014 at the NATO Wales summit when cyber was formally associated with the article. Cyber was further linked to Article 5 at the NATO Brussels summit of July 2018 in the context of so-called hybrid warfare: "We face hybrid challenges, including disinformation campaigns and malicious cyber activities … While the primary responsibility for responding to hybrid threats rests with the targeted nation, NATO is ready, upon [North Atlantic] Council decision, to assist an Ally at any stage of a hybrid campaign. In cases of hybrid warfare, the Council could decide to invoke Article 5 of the Washington Treaty, as in the case of armed attack."[26]

Similar to the 2018 NATO Brussels Summit Declaration, the earlier Wales declaration affirmed the applicability to cyberspace (and, therefore, NATO activities therein) of the UN Charter (presumably Article 51 in particular) as well as international and humanitarian law. Reflective of the policy advice heard years before about deterrence, the 2014 pronouncement also was deliberately ambiguous about the threshold for retaliation whether against cyber sabotage, terrorism or war: "A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."[27] As suggested above, however, the magnitude of harm inflicted would likely be a key factor. Using history as a guide, the direction of the attack also would likely figure in the deliberations. In reflecting on the criteria used to invoke Article 5 in response to 911, Edgar Buckley, Assistant Secretary General for Defence Planning and Operations from 1999 to 2003, recalled that alongside the scale of an attack, "External direction was important because it was clear that the Allies did not regard attacks by internal terrorist organisations—such as in Belfast or Oklahoma City—as falling under the Treaty."[28] For reasons discussed previously, determining the external direction of a cyber attack might prove more difficult than unearthing a

[26] "Brussels Summit Declaration," *NATO*, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

[27] *Wales Summit Declaration*. The North Atlantic Council is NATO's highest decision-making body.

[28] Edgar Buckley, "Invoking Article 5." *NATO Review*, No. 2, 2006. https://www.nato.int/docu/review/2006/Invokation-Article-5/Invoking_Article_5/EN/index.htm.

plot to hijack airliners hatched in Afghanistan, but confirming foreign culpability would still be significant. At least one model for helping to do so has been presented.

In recent years, the strategic ambiguity that has deliberately surrounded a NATO response to a cyber attack also has included the possibility of action short of collective defense. As NATO's Secretary General explains, "The level of cyber-attack that would provoke a response must remain purposefully vague. As will the nature of our response. But it could include diplomatic and economic sanctions, cyber-responses, or even conventional forces … We need a full spectrum response. So we can respond to serious cyber-attacks even if they don't cross the Article 5 threshold."[29] Since the 1990s, NATO's mandate has evolved to comprise crisis management alongside collective defense (and cooperative security) as a core task; so the Secretary General's remarks may be viewed in this context.

Finally, it is worth noting that 2016 was another watershed year for NATO's mandate in cyberspace. Cyberspace was for the first time officially identified as a domain of Alliance operations joining the traditional ones of land, sea and air.[30]

Policy

With a defensive mandate in cyberspace established, policies to realize it in practice have continued apace. Published in 2014, the third iteration of a NATO Cyber Defense Policy identified the protection of NATO's own communications and IT systems as the chief priority, but also instituted several governance and educational measures to enable individual member states to draw on NATO support in response to cyber attacks and to build national capacity. The policy also integrated cyber defense into operational and civil-emergency planning. Reflective of previously referenced calls for a comprehensive approach, the policy went on to advocate for cooperation

[29] Stoltenberg.
[30] "*Warsaw Summit Communiqué*," *NATO*, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

with partner countries and relevant international organizations.[31] Two years later, the Cyber Defense Pledge further compelled each member state to step up the "cyber hygiene" and defense of national infrastructures as well as static and deployable networks including those on which NATO relies. Improved information sharing and collaboration among Allies likewise was pledged.[32] Other policy milestones have included a concerted effort to engage industry. At the behest of Estonia, the Netherlands and United Kingdom, the NATO Industry Cyber Partnership was launched in 2014. Among its objectives is to improve sharing of best practices and expertise on preparedness and recovery including technology trends and malware information. In May 2018, for example, the Alliance signed bilateral agreements with industry leaders CY4GATE, Thales and Vodafone. The agreements are designed to facilitate rapid early bilateral exchange of non-classified technical information related to cyber threats and vulnerabilities to be integrated into NATO's 24/7 detection and prevention system.[33] The comprehensive approach to cyber defense, moreover, has not ended with industry. In July 2016, the European Union and NATO also signed a bilateral Joint Declaration. Cybersecurity was one of seven areas highlighted for concerted collaboration. The EU's External Action Service recently emphasized the (ongoing) exchange that has ensued on cyber concepts and doctrine, training and education, and threat indicators.[34]

Institutionalization and capability development

When Jamie Shea wrote about the essential components of NATO's cyber defense portfolio, "creating a firm bureaucratic foothold in the NATO organization" was one of them.[35] The point was that policy statements do not create defense capabilities by inertia. Dedicated organizations and processes do. Thus, it should come as no surprise that NATO's "cyber

---

[31] "Cyber Defense," *NATO*, July 16, 2018, https://www.nato.int/cps/en/natohq/topics_78170.htm.

[32] Cyber Defense Pledge.

[33] "New NATO-industry cyber partnerships signed at NITEC18." *NCI Agency*, May 23, 2018, https://www.ncia.nato.int/NewsRoom/Pages/180523-IPAs_signature_NITEC.aspx.

[34] "EU-NATO Cooperation – Factsheet." *EEAS*, July 10, 2018. https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en

[35] Shea, p.197.

bureaucracy" steadily has expanded. The following constitute some of the key organs.

The Cyber Defense Committee provides high-level political oversight of NATO cyber defense initiatives. Working-level support is provided to it by the NATO Cyber Defense Management Board. Technical advice resides in the NATO Consultation, Control and Command Board. The NATO Communications and Information Agency supports NATO operations and connects as well as defends NATO networks. The Agency is a core function of its NATO Computer Incident Response Capability Technical Center of 200 experts. Recognizing the importance of nurturing the next generation of such experts, the Agency is also establishing a 20 million-euro NATO Communications and Information Academy to be opened in 2019.[36] Furthermore, at the 2018 NATO Brussels summit, the creation of a dedicated Cyberspace Operations Center was a central plank of the first expansion of the NATO Command Structure in several years.[37] It is intended to provide situational awareness and coordination of NATO operational activity within cyberspace. The same Brussels meeting also announced the establishment of NATO Counter-Hybrid Support Teams, adding to the Alliance's cyber-defense portfolio that already includes the precursor NATO Cyber Rapid Reaction Teams. These teams are designed to provide tailored, targeted assistance to individual member states upon their request. It also is worth recalling that alongside the constitution of these official cyber organs within the NATO bureaucracy, new processes have been added. Significantly, since 2012, cyber defense has been integrated into the NATO Defense Planning Process through which the Alliance and national capability targets are harmonized. Successive Cyber Defense Policy statements have, in turn, been accompanied by a Cyber Defense Action Plan to guide their implementation.[38]

Finally, outside the formal Alliance structures, the previously mentioned NATO-accredited Cooperative Cyber Defense Center of

[36] "NATO breaks ground on IT academy." *NCI Agency*, May 23, 2017. https://www.ncia.nato.int/NewsRoom/Pages/170523-NCI-Academy_groundbreaking_ceremony.aspx

[37] Brussels Summit Declaration.

[38] "Cyber Defense," *NATO*, July 16, 2018. https://www.nato.int/cps/en/natohq/topics_78170.htm.

Excellence (CCDCOE) also has been a longstanding hub of interdisciplinary research, training and education on cyber issues. In addition to the development of the unofficial Tallinn Manual, this contribution has included the annual conduct of the world's largest live-fire exercise Locked Shields on the so-called NATO Cyber Range. In February 2017, a contract to update the Range was granted. As the winning bidder, Guardtime, affirmed at the time, "For NATO we will provide a state of the art flexible, operationally relevant and representative environment design that enables integrated simulation and training and collaboration for a wide variety of blue and red team cyber mission exercise areas …"[39] What is more, since 2017, the work of the CCDCOE has been complemented by the establishment of the NATO-EU sponsored European Center for Countering Hybrid Threats based in Helsinki, Finland (a NATO partner nation). As its mandate states: "Due to increased opportunities for hybrid influencing during the present information age, the hybrid challenge will grow. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) is to serve as a hub of expertise supporting the participating countries' individual and collective efforts to enhance their civil-military capabilities, resilience, and preparedness to counter hybrid threats with a special focus on European security." [40]

Future Challenges

Preceding pages have illustrated NATO's considerable effort to adapt to meeting cyber threats. Yet, a mantra of defense policy planners is that "transformation is a journey, not a destination." NATO's cyber adaptation is no different. So what challenges lie ahead? This paper concludes by briefly discussing one notable policy development: the advent of the new US National Cyber Strategy.

---

[39] Meelis Vill, "Guardtime Awarded Contract for Next-Generation NATO Cyber Range." *Guardtime*, February 1, 2017. https://guardtime.com/blog/guardtime-awarded-contract-for-nato-cyber-range.

[40] Information on the Hybrid COE is available at: https://www.hybridcoe.fi/.

US National Cyber Strategy

In September 2018, the US Administration published the National Cyber Strategy[41]—the first in fifteen years. In the Trump era of "America First," allies as well as adversaries will be obliged to take note. NATO is no exception. While, as mentioned previously, consensus is a core operating principle of the Alliance, US leadership matters to agenda-setting. Its pre-eminence in defense spending is why the United States is understandably referred to as the "indispensable Ally" in NATO circles. Washington will expect NATO and its Canadian and European members to take note of this latest US policy pronouncement and reflect on the implications for the Alliance. Reference to the US National Cyber Strategy of the United States of America released last year should leave no doubt in this regard. It affirmed the US commitment to Article 5 and referred to NATO as one of America's great strategic advantages over competitors, but went on to frankly state that "The NATO alliance will become stronger when all members assume greater responsibility for and pay their fair share to protect our mutual interests, sovereignty, and values."[42] So what are some of the possible repercussions for NATO's cyber deterrence and defense?

The American strategy for one profile increased concern about the growing cyber-related threats to space assets and supporting infrastructure related to: "positioning, navigation, and timing (PNT); intelligence, surveillance, and reconnaissance (ISR); satellite communication and weather monitoring."[43] It goes without saying that each is critical to military operations, including NATO-led ones. While for a country like the US that has long recognized outer-space as an operating domain, redoubling efforts to link it to the cyber one may seem logical. The US also avowedly wants to work with industry and international partners to improve

---

41 *National Cyber Strategy of the United States of America.* United States of America, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

42 "National Security Strategy of the United States of America," *The White House*, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

43 "National Cyber Strategy of the United States of America," *The White House*, September 2018, p.10, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

"space cybersecurity" including the cyber resilience of existing and future space systems. However, for the Alliance that does not yet recognize space as an operating domain alongside cyber, land, sea and air, following the American lead may prove somewhat more challenging. Nevertheless, there are signs that things may evolve in space as rapidly as they have for NATO in the hybrid sphere. In another landmark decision taken at their 2018 NATO Brussels summit, the member states declared: "Recognising that space is a highly dynamic and rapidly evolving area, which is essential to a coherent Alliance deterrence and defence posture, we have agreed to develop an overarching NATO Space Policy."[44]

The Brussels summit was also notable for its commitment to reinvigorate NATO's maritime deterrence and defence posture including maritime warfighting skills to protect critical sea lines of communications. While on this occasion the Alliance did not specifically mention cyberspace in a maritime context, it may soon be urged by the US to do so. The National Cyber Strategy singles out the criticality of maritime transport to the US and global community and, consequently, the need to "accelerate the next-generation cyber-resilient maritime infrastructure."[45] Should calls for an updated Alliance Maritime Strategy be heeded, maritime cybersecurity (which the 2011 version does not mention) surely will receive attention.

Lastly, in September 2018 the US also launched the International Cyber Deterrence Initiative. The aim is to build an international coalition of like-minded states to address malicious cyber behavior including better information and intelligence sharing, reinforcing attribution claims, coordinated public statements of support for responses, as well as the joint imposition of consequences for disruptive and destructive behavior in the so-called "technical ecosystem."[46] Whether in a space or maritime context or elsewhere, NATO's future mandate, policy and capability development in the cyber and related domains will most certainly be influenced by this latest American endeavor.

---

[44] Brussels Summit Declaration.
[45] "National Cyber Strategy of the United States of America," *The White House*, September 2018, pp.9-10.
[46] Ibid., p.21.

Bibliography

"A 'comprehensive approach' to crises," *NATO*, June 26, 2018, https://www.nato.int/cps/su/natohq/topics_51633.htm

"Brussels Summit Declaration," *NATO*, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm

Buckley, Edgar, "Invoking Article 5," *NATO Review*, No. 2, 2006, https://www.nato.int/docu/review/2006/Invokation-Article-5/Invoking_Article_5/EN/index.htm.

"Cyber Defense Pledge", *NATO*, July 8, 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

"Cyber Defense," *NATO*, July 16, 2018, https://www.nato.int/cps/en/natohq/topics_78170.htm.

"EU-NATO Cooperation – Factsheet," *EEAS*, July 10, 2018, https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en.

Fitton, Oliver, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections*, Vol. 15, No. 2, 2016.

Hegenbart, Christine, "Semantic Matters: NATO, Cyberspace and Future Threats," *NATO Defense College Research Paper*, No. 103, 2014.

Hughes, Rex, "NATO in Cyberspace: Digital Defenses," *The World Today*, Vol. 65, No. 4, 2009.

Meelis, Vill, "Guardtime Awarded Contract for Next-Generation NATO Cyber Range," *Guardtime*, February 1, 2017, https://guardtime.com/blog/guardtime-awarded-contract-for-nato-cyber-range.

"National Cyber Strategy of the United States of America," United States of America, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

"National Security Strategy of the United States of America," United States of America, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

"NATO breaks ground on IT academy," *NCI Agency*, May 23, 2017, https://www.ncia.nato.int/NewsRoom/Pages/170523-NCI-Academy_groundbreaking_ceremony.aspx.

"New NATO-industry cyber partnerships signed at NITEC18," *NCI Agency*, May 23, 2018, https://www.ncia.nato.int/NewsRoom/Pages/ 180523-IPAs_signature_NITEC.aspx.

Popa, Iulian F., "NATO's Cybersecurity and Defense: Before and After 2014 Wales Summit," *Annals of the "Constantin Brancusi" University of Targu Jiu, Letter*

and Social Sciences Series, No. 3, 2014.

"Prague Summit Declaration", *NATO*, 2002, https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

Shea, Jamie, "NATO Dealing with Emerging Security Challenges?" *Georgetown Journal of International Affairs*, Vol. 14, No. 2, 2013.

Stoltenberg, Jens, "Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defense Pledge Conference," *NATO*, May 15, 2018, https://www.nato.int/cps/en/natohq/opinions_154462.htm.

"Strategic Concept – Active Engagement, Modern Defence", *NATO*, 2010, https://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

"The North Atlantic Treaty", *NATO*, 1949, https://www.nato.int/cps/ua/natohq/official_texts_17120.htm.

"Wales Summit Declaration", *NATO*, 2014, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

"Warsaw Summit Communiqué", *NATO*, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

Windrem, Robert, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," *NBC News*, December 18, 2016, https://www.nbcnews. com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111.