NATO PARLIAMENTARY ASSEMBLY

SCIENCE AND TECHNOLOGY COMMITTEE (STC)

NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE

General Report

by Susan DAVIS (United States)
General Rapporteur

148 STC 19 E rev. 1 fin | Original: English | October 2019

TABLE OF CONTENTS

I. INTRODUCTION

1. As every sphere of human society is becoming increasingly more connected, cyber threats are skyrocketing. Everyone – from individuals to the international community – must consider how to tackle these threats which grow increasingly serious by the day. The Transatlantic Alliance is no different. NATO registers suspicious cyber events every day on networks it owns and operates (Stoltenberg, 2019), and intrusions into government and critical infrastructure networks in Allied and partner nations are rising dramatically.

2. Unsurprisingly, cyber security, defence, and deterrence have become a matter of urgency for NATO and the NATO Parliamentary Assembly (NATO PA). For the Science and Technology Committee (STC), the matter remains high on the agenda during its biannual meetings and its regular fact-finding visits – for example, its 2019 visits to Singapore and the United Kingdom. In recent years, the Committee has also examined specific cyber issues in depth (see Box 1).

3. This general report cannot possibly deal with all types of cyber threats facing Allied nations. Instead, it focuses on the cyber threats going to the core of NATO's *raison d'être*: cyber attacks threatening an Ally's territorial integrity, political independence, or national security and could lead Allies to invoke NATO's collective defence clause under Article 5 of the Washington Treaty. Countering such threats is at the heart of NATO's mission.

4. The Alliance first publicly recognised the need to strengthen cyber security and defence at the 2002 Prague Summit. In 2008, NATO adopted its first cyber defence policy. However, the crucial turning point came in 2014 at the Wales Summit, when the Alliance adopted an Enhanced NATO Cyber Defence Policy. Among other key decisions, NATO leaders explicitly stated a cyber attack could lead to the invocation of Article 5. For the first time, Allied leaders made clear that "[c]yber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability" (NATO, 2014).

BOX 1: RECENT RELATED STC REPORTS

- *Cyber Space and Euro-Atlantic Security*
- *The Internet of Things: Promises and Perils of a Disruptive Technology*
- *Russian Meddling in Elections and Referenda in the Alliance*
- *Dark Dealings: How Terrorists Use Encrypted Messaging, the Dark Web and Cryptocurrencies*

5. Since the Wales Summit, NATO and the Allies have made cyber security, defence, and deterrence an unambiguous part of NATO's core tasks and implemented the steps to make this a reality. By now, any potential opponent should have realised that a sufficiently harmful cyber attack against one Ally will be considered an armed attack against all and that Allies will invoke Article 5 to collectively defend themselves. At the 2018 NATO Summit in Brussels, Allied leaders once again reiterated this commitment: "Reaffirming NATO's defensive mandate, we are determined to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign" (NATO, 2018a).

6. This general report does not attempt to give an exhaustive account of all Allied and NATO cyber security, defence, and deterrence policies, activities, and discussions. Rather, it will provide:

- context for the cyber threat facing the Alliance;
- an overview of NATO's current cyber strategies, policies and activities; and
- policy recommendations to strengthen NATO's cyber security, defence, and deterrence.

7. This General Report was adopted by the Committee on in 2019 at the 65th NATO PA Annual Session, London (United Kingdom). Its policy recommendations also serve as a basis for NATO PA resolution *459 Strengthening NATO Cyber Security Defence and Deterrence*, also adopted by the Plenary Assembly at the NATO PA Annual Session.

II. CYBER ATTACKS IN CONTEXT

8. To provide a basis for an informed discussion of NATO cyber policies, it is essential to understand how cyber attacks fit into the current cyber threat landscape.

A. CYBER ATTACKS AND OTHER MALICIOUS CYBER OPERATIONS

9. Regrettably, the term "cyber attack" is often used very loosely in public discussions. To understand the current cyber threat landscape and devise effective cyber strategies and policies, it is essential to clearly draw distinctions between cyber attacks and other types of malicious cyber operations.

10. No universally recognised definition of a "cyber attack" exists. However, the definition put forward by the US Department of Defense (US DOD) provides a good starting point. **Cyber attacks** can be understood as "Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain" (US DOD, 2019). In contrast, the US DOD defines **cyber exploitation** (which includes cyber espionage) as actions "to gain intelligence, manoeuvre, collect information, or perform other enabling actions" in cyberspace; and **cyber-enabled information operations** as attempts "to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries" (US DOD, 2019). The category of **cyber crime** covers all criminal activities committed through the internet, computer networks, or information systems.

11. **State and state-sponsored cyber attacks** present the biggest threat to the Alliance, as they could have sufficient effects in cyber space or the physical domain to rise to the level where the Alliance would invoke Article 5. States or their proxies are not the only actors who could conduct cyber attacks. Malicious code (see Box 2) is widely available online, and bad actors can develop their own. However, planning and executing the most devastating cyber attacks requires very detailed knowledge, skills, and abilities, as well as substantial financial and organisational resources (Slayton, 2017; Davis, 2014). Currently, only states and their proxies are likely to meet this resource threshold. They are thus the central focus of this report. Of course, Allies should not be complacent about cyber attacks by terrorist groups. NATO's cyber security and defence, however, remain key to thwarting such attacks. (Deterrence of non-state actors, especially in cyber space, is very difficult.)

12. This report's focus on cyber attacks does not imply that **other malicious cyber operations** do not pose serious risks for NATO and the Allies, nor that armed forces do not play a role in countering them. Indeed, in her 2018 General Report, the General Rapporteur outlined how cyber-enabled information operations targeting election systems undermine the national security of Allies, how they constitute a part of the larger hybrid threat facing NATO, and how Allied nations could counter such threats. Allied counterintelligence officers and others are also in a constant fight against digital spies. Moreover, it may prove easier for criminals to access NATO's headquarters through cyber space than by using more traditional attack methods. In practice, the lines between different types of malicious operations are often blurry. Moreover, a growing number of Allies are recognising the long-term strategic risk presented by persistent cyber campaigns which merge a number of cyber operations – all falling below the level of armed conflict.

BOX 2: HOW CYBER OPERATIONS SUCCEED

Cyber operations employ **malicious computer code**. To succeed, an intruder must find a vulnerability, gain access, and deliver a payload (Lin, 2010).

First, an intruder needs to exploit *vulnerability* – a defect or bug – in a targeted network.
Second, intruders must gain *access* to the targeted network – either through remote access, witting or unwitting insiders, covert operations, or the supply chain.
Third, intruders need to deliver a *payload* to carry out the intended action in the penetrated networks.

Exception: **Distributed denial of service (DDoS) attacks** do not require a flaw in the targeted network. Instead, they overwhelm the network with unmanageable amounts of network traffic.

B. CYBER ATTACK RISKS DURING PEACETIME

13. Some commentators and experts have raised the fear that states or their proxies could, during peacetime, perpetrate **large-scale cyber attacks under the cover of anonymity** against military networks or civilian critical infrastructure. Certainly, such attacks can never fully be ruled out, and NATO and Allied strategies and policies must account for this threat. However, the risk of a large-scale surprise attack is smaller than headlines about a "cyber 9/11" or "cyber Pearl Harbor" imply.

14. Indeed, attackers can attempt to hide their tracks by using third-party networks and try to get away with large-scale surprise attacks. Establishing connection to a state, even when an attack is geographically traced back to a certain country, can be very challenging. An aggressor can also try to plant false flags to implicate others. At the technical level, attribution can be complicated. The defender must analyse vast reams of technical data; understand how such an attack fits with the potential attacker's goals, motivation, and capabilities; and process intelligence from a multitude of sources – all on a timeline where responses still matter (Davis et al., 2017). The **problem of attribution**, therefore, looms large in cyber policy debates.

15. However, in recent years, governments, private companies, and research organisations have increased their **ability** to **attribute** attacks at higher levels of confidence. Forensic tools have improved, and private and state analysts have built up databases and characteristic patterns for known intruders. On a technical level, truly harmful cyber attacks are very complicated and involve many moving pieces. Thus, the more complicated the cyber attack, the more likely the attacker is to commit mistakes along the way, enabling a forensics expert to trace the origin of the attack (Lindsay, 2015). Indeed, governments within the Alliance and beyond are increasingly attributing malicious cyber incidents to states and their proxies. Such transparency on cyber incidents is increasingly collective, coordinated in policy and time, and independent of the scale, nature, or impact of the incident (Giles and Hartmann, 2019). The Rapporteur supports this emerging policy of naming and shaming perpetrators and encourages further conversations at the NATO level.

16. Even if states and their proxies could be confident they will remain anonymous, truly convincing strategic rationales for large-scale surprise attacks are lacking. Anonymous cyber attacks are **not well-suited for coercion**, for example. Coercion only works if the attacked entity knows whom to yield or make concessions to. As one analyst points out succinctly, "[p]urely anonymous coercion is almost impossible because communicating and understanding the power to hurt implies that there is someone doing the hurting and a target concerned about avoiding getting hurt" (Lindsay, 2015). As a result, if an opponent wishes to coerce through cyber attacks, he cannot hide himself. This would defeat the purpose. How can the victim give in to demands if it does not know who the attacker is? (In contrast, cyber criminals *want* to stay anonymous when, for example, they attempt to extort money from victims.)

17. Anonymity does, however, provide excellent advantages for **tactical or operational gains.** States could use cyber attacks in peacetime and crisis situations for precise, limited actions that

avoid crossing the threshold of an armed attack (Lewis, 2018). In other words, states will stay in the realm of hybrid operations in the grey zone between peace and war where norms of behaviour are lacking (Lewis, 2018). For example, they may lay the groundwork for future cyber attacks during crisis situations or armed conflicts.

18. It is very difficult to guard against episodic cyber attacks for tactical or operational gains, beyond instituting strong cyber security and defence measures. However, the bigger strategic risks for individual Allies and NATO as a whole emanate from **persistent cyber campaigns**. In such campaigns, opponents conduct numerous cyber operations in order to achieve strategic impact by corroding a state's sources of power over time (Nakasone, 2019). Allies are, therefore, refining their policies to counter such persistent campaigns. The United States, for example, has substantially changed its cyber policy as a result. The US DOD has adopted a new innovative cyber strategy of **Persistent Engagement**. In the perspective of General Paul M. Nakasone, Commander of US Cyber Command, "in cyberspace, it's the use of cyber capabilities that is strategically consequential […]. So advantage is gained by those who maintain a continual state of action" (Nakasone, 2019). Under the strategy of Persistent Engagement, the US military does not limit itself to a merely defensive posture of safeguarding its own internal networks and responding to breaches after they occur, but instead "defends forward" by seeking to "disrupt or halt malicious cyber activity at its source" (US DOD, 2018). The strategy relies on constant contact with potential adversaries globally – even in their own networks – with the intention of imposing "tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks" (US Cyber Command, 2018). The doctrine also entails a substantial focus on partnering with other actors, including both non-military government agencies and select private-sector companies (Nakasone, 2019). Persistent innovation is also key to the architects of this new strategy. As General Nakasone has argued, "superiority in cyberspace is temporary; we may achieve it for a period of time, but it's ephemeral" (Nakasone, 2019). An extensive debate about how to make Persistent Engagement fully effective is playing out in US cyber policy circles. The Rapporteur would encourage further and more intensive debate about how to tackle persistent cyber campaigns within the Alliance, recognising that important national differences between Allies exist. She thus welcomes the May 2019 meeting of Allied National Security Advisors on countering hybrid threats, where ways to improve NATO's situational awareness through better intelligence and information sharing was the main topic.

C. CYBER ATTACKS IN MILITARY OPERATIONS, CRISES, AND ARMED CONFLICT

19. Just as no modern war can be won by relying on only one set of military capabilities, cyber attacks alone cannot win a war. However, integrated with other military operations, **cyber attacks can produce significant military effects.** NATO and many other armed forces see cyber space as a distinct military domain and have begun integrating defensive and offensive cyber capabilities into their operational planning through the following measures:

- developing cyber capabilities;
- combining cyber options with other types of operations;
- reorganising their command structures;
- devising cyber doctrines and embedding them in overall doctrine; and
- examining how national and international law applies to actions in cyber space.

20. Offensive cyber capabilities can support other types of capabilities during military operations (and vice versa). Compared with traditional kinetic attacks, cyber attacks are unlikely to directly cause mass casualties or physical damage, if employed in responsible ways. Offensive cyber capabilities can, for example, help armed forces **collect intelligence** or **prepare the battlefield** by degrading, disrupting, or destroying military command and control networks or weapons and sensor systems, thus slowing down decision making or delivering tactical success (Lewis, 2016). Military networks are deliberately isolated, from both other military networks and civilian ones (Lewis, 2016). Still, as Allies think through how to integrate cyber operations into military operations, they must take great care in preventing cyber attacks from spilling over and affecting civilian networks.

21. In a longer war, **civilian** critical infrastructure could become a target for an opponent. An attacker could seek to degrade the defender's war efforts, for example through attacks on defence industry facilities or power and electricity networks which military forces rely on. More doubtfully, an attacker could try to undermine public confidence. Historically, attacks on civilian critical infrastructure during armed conflicts have little military effect and normally stiffen the resistance and resilience of the population (Lewis, 2018). They do not produce the widespread political chaos or strategic effects some fear and others may hope for. However, NATO and Allied forces should not be complacent about such scenarios; they should counter them with the right mix of security, defence, and deterrence. NATO and Allied renewed focus on resilience, including the seven baseline requirements for civil preparedness adopted at the 2016 Warsaw Summit (see Box 3), is crucial in this regard.

BOX 3: NATO'S SEVEN BASELINE RESILIENCE REQUIREMENTS ON CIVIL PREPAREDNESS (NATO, 2018b)

1. continuity of government and critical government services
2. energy supplies
3. ability to deal effectively with uncontrolled movement of people
4. food and water resources
5. ability to deal with mass casualties
6. telecommunications and cyber networks
7. transportation systems

22. Policy circles within the Alliance and beyond continue to debate how cyber attacks affect **stability during crises and armed conflict**. Which types of cyber attacks would be de-escalatory, escalatory, or neutral? Would the answer differ depending on when, during a crisis or an armed conflict, they would be launched? And are there significant differences between various states on these answers? States most likely do not see a cyber attack as a viable option for a pre-emptive first strike. However, in a crisis or pre-war situation, they could perceive a significant "cost of going second" (Davis, 2014). In such situations, one side "may well be frightened of what would happen if the other side attacks *and* may be convinced that going first will be advantageous" (Davis, 2014). This could lead to high escalatory risks in a crisis. Another key problem is the difficulty of **determining the intent** of a cyber intrusion (Lindsay, 2015). When a defender detects a breach, he may not know whether the intruder wants to spy on him, conduct forward defence, gain a foothold for future defensive measures, or prepare for an imminent or future cyber attack (Slayton, 2017). It is extremely difficult to gauge intent in cyber space, and, in such cases, states tend to assume the worst (Hennessey, 2017). As a result, this can lead to misperception and an escalatory spiral (Slayton, 2017). In sum, escalation dynamics deserve considerably more attention. For now, however, the Alliance should seek to reduce escalatory risks through clear diplomatic messaging and engagement; a high level of transparency on cyber policies; examining escalation dynamics in exercises; as well as support to norm-development and confidence building measures.

III. NATO CYBER POLICY

23. At the political level, the Alliance continues to adapt its cyber security, defence, and deterrence policies through regularly updated action plans with concrete objectives and timelines. This section outlines NATO's:

- overarching strategies to counter cyber attacks;
- cyber capability development;
- the integration of cyber capabilities into NATO planning;
- concrete cooperation in NATO; and
- NATO's cyber partnerships.

A. NATO'S OVERALL CYBER STRATEGY

24. As armed forces around the world, including in potential adversary states, build up their cyber capabilities, NATO and its member states must devise strategies and policies to counter the threat of serious state-directed cyber attacks. Overall, NATO is leaning heavily on the same general

strategies it uses to counter other attacks: **dissuasion by denial** and **deterrence by punishment**. However, Allies should continue to support work on international norms and engage in serious discussions to determine if and how strategies such as persistent engagement, as outlined above, can supplement overall NATO strategy.

1. Norms in Cyber Space

25. Due to the specific characteristics of malicious cyber code, arms control, disarmament, and non-proliferation measures very likely remain beyond reach for now, most importantly because verification seems impossible. However, the further development of norms in cyber space could become an important pillar of support against such attacks. NATO continues to argue that international law applies to cyber space, including international humanitarian law and the United Nations Charter. This is also in line with the 2013 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE, 2013). The Alliance has declared its support for "work on voluntary international norms of responsible state behaviour and confidence-building measures regarding cyberspace" (NATO, 2016b). Allies have furthermore made clear that they "stand to benefit from a norms-based, predictable, and secure cyberspace" (NATO, 2018a). However, it is unrealistic to expect that NATO, as an Alliance of 29 sovereign nations, could become the primary driving force in the further development of norms. Instead, individual Allies must continue to drive this effort in the international community and encourage other member states to do the same.

2. Cyber Security and Defence

26. Strategies of dissuasion by denial aim at "dissuading an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action" (Davis, 2014). In other words, the defender must make such an attack look futile: the attacker should fail or, at the very least, not benefit from a cyber attack (Nye, 2017). Such cyber dissuasion is squarely premised on strong cyber security and defence, which is primarily a national responsibility, but NATO must and does play a role, which the next sub-sections show (see also Box 4).

BOX 4: CYBER SECURITY AND DEFENCE DEFINED

Cyber security aims "to prevent unauthorised access to, exploitation of, or damage to computers, electronic communications systems, and other information technology […] as well as the information contained therein" (US DOD, 2019).

Cyber defence covers efforts "to defeat specific threats that have breached or are threatening to breach cyberspace security measures" (US DOD, 2019).

27. In theory, **cyber security and defence** is a straightforward proposition. Defenders try to reduce vulnerabilities, block access points, and minimise the impact of payloads. Cyber security and defence include a range of preventive, passive, and active measures. Those seeking to protect their networks must strengthen their capabilities in several areas: threat identification; network protection; intrusion detection; responses against attacks; and resilience and recovery (US NIST, n.d.; see Box 5). Determined intruders are often very agile and adapt rapidly to circumvent new cyber security or defence measures. Thus Allies often turn to more active cyber defence. For example, the US DOD, under its active cyber defence concept, can synchronise defence across all government and critical infrastructure networks. In other words, they defend more than just the networks owned and operated by the DOD. A step beyond is the so-called "defend forward" concept, for example adopted by the United States in 2018. When defending forward, defenders can cross over into the attacker's networks to conduct intelligence operations; try to disrupt ongoing or even planned attacks; quickly reverse damage from attacks; and, in extreme situations, punish attackers (Hoffman and Levite, 2017; US DOD, 2018).

3. Deterrence

28. Although cyber security and defence capabilities continue to improve, most experts argue that the **offence has the advantage** in cyber space and that this is unlikely to change soon. Given sufficient time, skills, and resources, attackers can perpetrate a cyber attack, finding the targeted system's vulnerabilities, gaining access, and delivering their payload. This is a key reason why the Alliance must complement dissuasion with strategies of deterrence by punishment. In other words, they must try "to prevent an attack by threatening unacceptable damage so that *in the attacker's cost-benefit calculations* the best choice is not to attack" (Morgan, 2009). It should be noted some experts would argue that offence is not as dominant. For example, the more sophisticated cyber weapons are, the more opportunities the defender has to stop an attacker and the more errors the attacker is likely to make. Additionally, continued organisational deficiencies could be a key reason why attackers have had the advantage thus far (Slayton, 2017).

BOX 5: SOME WAYS TO ENHANCE CYBER SECURITY AND DEFENCE

- Implement basic cyber security measures
- Increase situational awareness
- Increase information sharing
- Install better detection and surveillance software
- Invest into research and development of new technologies
- Train the workforce, for example in cyber hygiene
- Incentivise workforce compliance
- Conduct cyber training and exercises
- Conduct regular cyber audits
- 'Red team' cyber security and defences
- Conclude cooperation and assistance agreements
- Deceive potential attackers (e.g. plant 'honey pots')
- Encrypt sensitive files
- Wall off sensitive parts of the network

29. NATO maintains a **cyber deterrence policy** of ambiguity. First, it does not draw a clear line for when a cyber attack is sufficiently harmful to cross the threshold to an armed attack. Second, it does not currently have an operational definition of what the collective response would be if that threshold were to be crossed. Such a cyber deterrence policy offers several advantages. If the Alliance were to set a clear threshold, the opponent would better understand how to stay below that threshold. This would strengthen deterrence of threats above the threshold but would encourage the opponent to increase attacks just below the threshold. A certain degree of ambiguity is beneficial because it could make opponents wary of going too far in their cyber attacks. The opponent always fears stepping over the invisible line, and thus prefers to tread lightly. A similar deterrence posture arguably worked well during the Cold War.

30. However, ambiguity on where the threshold lies could indeed lead an opponent who is sufficiently comfortable with taking risks to continuously exploit the "grey zones", test the defender's resolve, and conduct ever more daring cyber attacks. Arguably, the solution for such attacks cannot be found in deterrence alone, but rather in a clearly defined policy response for hybrid operations. Allied nations, individually and collectively, continue to develop such options. This is where the United States military saw a need to shift to an innovative strategy of Persistent Engagement. The Rapporteur encourages Allies to explore if and how such a strategy can be most effectively embraced together.

31. NATO's ambiguity also extends to the type of punishment it threatens were it to suffer a cyber attack. The Alliance has made clear that it neither limits punishment to similar cyber attacks nor excludes them. Instead, it keeps the option open to use the full range of Allied capabilities to deter and counter cyber attacks. Once again, this introduces useful doubt in an opponent's mind. A more technical reason for the difficulty of restricting retaliation to cyber attacks is that it is hard to credibly threaten the assets of the attacker in a similar fashion. If an attacker shuts down a power plant, would the Alliance have cyber options to attack an opponent's power plants or similar infrastructure? Would NATO even want to if it could, as it complies with the principle of proportionality and international law in all its activities? NATO's ambiguity on the type of retaliation serves a convincing purpose. It produces doubts in the would-be attacker's mind and presents more options to tailor and scale a response to re-establish deterrence.

32. A key feature of a stable deterrence situation is the **ability to signal** retaliatory capabilities and resolve to enforce the deterrence threat. However, such signalling is difficult when it comes to cyber deterrence. States can hardly display malicious codes at a military parade or a defence exhibition. They must, therefore, find different ways to signal capabilities and resolve impending conflicts. For example, demonstrating capabilities in real-world situations typically makes deterrence threats more plausible (Nye, 2017). Indeed, many experts argue that recent, limited cyber attacks should, at least in part, be seen as such demonstrations (Lewis, 2018). Additionally investing in cyber capabilities in a way visible to an opponent "generally can help to signal resolve" (Lindsay, 2015). In other words, transparency on cyber security and defence measures also serves as a deterrence signal. In the limited way they can signal their cyber security and defence capabilities, NATO and individual Allies appear to be making progress. In the public realm, NATO should therefore remain as transparent as possible when it comes to its cyber capabilities. In areas where public disclosure is not an option, communicating with potential opponents through non-public channels should happen as frequently as possible.

B. ALLIED CYBER CAPABILITY DEVELOPMENT

33. In line with NATO's Article 3, each Ally has an individual responsibility to maintain and develop both individual and collective capacity to resist cyber attacks. At the NATO level, this individual responsibility is addressed through the NATO Defence Planning Process (NDPP). Under the NDPP, each Ally sets national planning targets, and the other Allies regularly examine whether the Ally has met its established goals and mandates. The first Cyber Defence Capability Targets were set in 2013. They included targets on cyber defence governance, response capabilities for NATO networks, and education and training programmes (Robinson, 2017).

34. At the 2016 Warsaw Summit, Allies agreed that enhancing the cyber defences of national networks and infrastructure had become a matter of priority. To complement the regular NDPP process, they thus committed to a Cyber Defence Pledge to strengthen capability development. Under the Pledge, member states vowed to improve their cyber resilience and response capability and conduct annual self-assessments. Allies must therefore pursue seven main objectives (NATO, 2016a):

I. "Develop the fullest range of capabilities to defend our national infrastructures and networks […];
II. Allocate adequate resources nationally to strengthen our cyber defence capabilities;
III. Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen co-operation and the exchange of best practices;
IV. Improve our understanding of cyber threats, including the sharing of information and assessments;
V. Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;
VI. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance;
VII. Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends."

C. INTEGRATING CYBER CAPABILITIES INTO NATO PLANNING

35. At the 2016 Warsaw Summit, the Alliance recognised cyber space as a domain of operations. In keeping with NATO's defensive mandate, Allies therefore recognised that NATO must defend itself in cyber space "as effectively as it does in the air, on land, and at sea" (NATO, 2016b). This recognition enables the Alliance to better "protect and conduct operations across these domains and maintain [NATO's] freedom of action and decision, in all circumstances" (NATO, 2016b). It also broadly supports NATO defence and deterrence policy.

36. The recognition of cyber space as a domain of operations portrays NATO's shift from thinking of cyber security and defence as an information assurance task to incorporating its cyber capabilities into the mission assurance task (Shea, 2017). Put differently, the Alliance is no longer solely focused on protecting NATO networks and supporting national efforts in building up cyber security and defence measures. It is increasingly focused on how to integrate cyber capabilities – including offensive cyber effects voluntarily provided by individual Allies – in NATO operations and missions. At the core of this shift is the need to encourage a coherent development of capabilities and a clear strategy for how these capabilities can be employed in an operational perspective (Robinson, 2017). Cyber capabilities have begun to add value to operations, contribute a new set of tools, and allow NATO to act at the "speed of relevance" (Robinson, 2017). As in other domains, NATO has made clear that strong political oversight and adherence to international law must be guaranteed when incorporating cyber effects.

37. Since 2016, several Allies have confirmed their willingness to contribute offensive as well as defensive cyber effects to NATO operations, namely Estonia, Denmark, Germany, Lithuania, the Netherlands, Norway, the United Kingdom, and the United States. Offensive cyber effects will not be under NATO command and control, but under the control of the contributing Ally – similar to how national special forces are employed in NATO operations. The Rapporteur encourages more Allies to follow suit to enhance NATO's overall credibility.

38. The political and legal principles guiding this integration were agreed to in November 2017. In 2018, the Alliance adopted a Vision and Strategy on Cyberspace as a Domain of Operations, with the aim of developing a proper cyber space doctrine by 2019. In practice, this will lead to closer cooperation between the Supreme Allied Commander Europe (SACEUR), Allied Command Operations (ACO), and the NATO Communications and Information Agency (NCI Agency) (Shea, 2017).

39. To effectively enable NATO's command structure to integrate cyber capabilities, Allies have additionally decided to establish a Cyberspace Operations Centre in Mons, Belgium, to be fully operational by 2023. The Centre will be responsible for providing situational awareness, coordinating cyber efforts, and centralising planning for operations and missions (Brent, 2019).

D. CONCRETE COOPERATION IN NATO

40. NATO focuses first and foremost on protecting NATO-owned and operated networks. NATO cyber cooperation also deals with enhancing cyber security and defence in Allied states through raising awareness, education, training, exercises, information sharing, and mutual assistance.

41. Numerous policy, military, and technical bodies within the NATO structures play key roles in implementing NATO's cyber policies, including the Consultation, Command, and Control Board; the NATO Military Authorities; the NCI Agency; Allied Command Operations; and Allied Command Transformation. Moreover, other entities in the wider NATO family bolster Alliance cyber defence and deterrence within their respective mandates, including the NATO School in Oberammergau, the NATO Defence College in Rome, and the NATO-accredited Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn.

42. Over the years, NATO entities and the wider NATO family have initiated and implemented a multitude of cyber activities and projects. It would go beyond the scope of this report to list them all. However, notable examples include:

- The inclusion of cyber threats into the NATO Crisis Management Exercise to enhance cyber awareness across the range of officials in capitals, at NATO Headquarters, Allied Command Operations, and Allied Command Transformation;
- The establishment of a NATO Cyber Range for exercising cyber defence capabilities, provided and hosted by Estonia; and

- Several Smart Defence projects on a Malware Information Sharing Platform, Smart Defence Multinational Cyber Defence Capability Development, and Multinational Cyber Defence Education and Training.

43. The NCI Agency delivers technology and communications capabilities for NATO's requirements and provides communications and information systems. It also supports the information technology needs of NATO Headquarters, the NATO Command Structure, and NATO Agencies. The NCI Agency thus plays a key role in technology acquisition, experimentation, interoperability, systems and architecture design and engineering, and testing and technical support.

44. The NCI Agency manages the NATO Computer Incident Response Capability (NCIRC) in Mons. The NCIRC defends NATO-owned and operated networks in more than 65 locations on a continuous basis – at all levels and no matter whether networks are static, mobile, or deployed. It also provides cyber threat analysis, in addition to the work done by the Cyber Threat Assessment Cell. Another key capability of the NCIRC is its Rapid Reaction Team (RRT) capability. The RRT can be deployed to NATO sites and in operational theatres, as well as in support of an Ally upon approval by the North Atlantic Council. The RRT capability has a core of six experts and is able to respond within 24 hours of the incident.

45. The NCI Agency is currently consolidating its training facilities. By the third quarter of 2019, Portugal will host the NATO Cyber and Communication-Information Systems Academy, which will provide training to civilian and military staff on NATO's advanced IT and cyber systems. The Academy will also connect with training locations in member states, industry, and academia.

46. In February 2019, the NCI Agency also launched a new NATO Hub where Allies' cyber defenders can share best practices, exchange information, and work in an encrypted space. This is the first step towards the creation of a Cyber Security Collaboration Hub, announced in 2018.

47. The CCD COE is another important asset for Allies as a recognised source of expertise. It currently brings together 25 NATO Allies and partner countries. NATO-accredited Centres of Excellence are not part of the NATO Command Structure; they are international military organisations supporting wider Alliance needs. Key outputs include cyber research, education, training, and exercises. Perhaps the most well-known products over the years has been the Tallinn Manual on the International Law Applicable to Cyber Warfare and the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

48. Cyber exercises are an important part of increasing NATO's cyber defence. The *Cyber Coalition* exercise is run by Allied Command Transformation. It involves more than 700 participants from member nations, NATO's partners, the EU, academia, and the industry. *Cyber Coalition* aims at enhancing cooperation and coordination between Allies and testing NATO and national procedures of information sharing, situational awareness, and decision making. *Cyber Coalition 2018* specifically exercised the integration of sovereign effects provided voluntarily by Allies (Brent, 2019). The CCD COE runs two other important exercises. The exercise *Locked Shields* tests the skills of cyber experts in intensive Red Team versus Blue Team scenarios. The exercise *Crossed Swords* enables participants – experts from member states, partner countries, and industry – to defend information technology networks and systems under simulated real-time cyber attacks.

E. NATO'S CYBER PARTNERSHIPS

49. A strong network of partners is essential in an increasingly interconnected world, and this applies in particular to cyber security and defence. NATO therefore engages with a wide range of partners, including industry, academia, partner nations, and other international organisations.

50. Industry plays a central role, as an STC delegation also heard at the UK National Cyber Security Centre during a June 2019 visit. They can provide technical solutions and innovations, invest heavily in cyber security solutions, and hold granular intelligence on cyber threats. Moreover, they also own or operate a substantial share of Allied information systems. In the NATO Industry Cyber Partnership (NICP), the Alliance therefore provides a forum for NATO entities and national experts to engage with industry representatives (and academia) from member states. The NICP aims at facilitating information sharing on cyber threats and at improving the ability of Allies to detect, prevent, and respond to cyber incidents. The Partnership covers 12 priority areas, notably supply-chain management; best practices; awareness raising; education, training, and exercises; and innovation.

51. Cyber security and defence cooperation is very often a key component of NATO collaboration with partner nations. NATO has particularly deep partnerships with Georgia and Ukraine, which includes extensive cyber cooperation initiatives. Through the Substantial NATO-Georgia Package, the Alliance supports Georgia's cyber capabilities, interoperability, and cooperation with individual Allies. NATO also established a Trust Fund on Cyber Defence in conjunction with Ukraine in 2014. The Trust Fund aims at developing strictly defensive capabilities in the area of cyber security incident response, including through setting up two Incident Management Centres. Ukraine also receives NATO training in employing the Trust Fund's related technologies and equipment. Other notable recent cyber cooperation initiatives with partner nations include agreements with Finland, the Republic of Moldova, Jordan, and Iraq.

52. While NATO also engages with the Organization for Security and Co-operation in Europe (OSCE) and the United Nations, its deepest international partnership is with the European Union. Coordination and cooperation on cyber security and defence is a key area of the NATO-EU Strategic Partnership. This cyber partnership gained new impetus in a 2016 joint declaration between the President of the European Council, the President of the European Commission, and the NATO Secretary General, where they decided to "expand their coordination on cyber security and defence including in the context of their missions and operations, exercises and on education and training" (Tusk, Juncker, and Stoltenberg, 2016).

53. Currently, NATO and the EU are implementing 74 proposals for cooperation, and cyber security and defence are key pillars among these proposals. Concrete areas of intensifying NATO-EU cooperation include:

- integration of cyber defence in planning;
- fostering cyber research and technology innovation;
- exchanging good practices on crisis management and response at the staff level;
- analysis of threats and malware information;
- identification of potential synergies, including between the NCIRC and the Computer Emergency Response Team – EU (CERT-EU), which have already signed a Technical Arrangement to facilitate information sharing; and
- strengthening cooperation on training and exercises.

54. A 2018 report on the implementation of the various NATO-EU proposals noted the active, effective interactions and information exchanges between staff, notably on concepts and doctrines; existing training and education courses; threat indicators; threat alerts and assessments; and crisis management.

55. In terms of exercises, EU cyber staff participated in the 2017 *Cyber Coalition* and 2018 *Locked Shields* exercises for the first time. In 2017, NATO's *Crisis Management Exercise* and the EU's *Parallel and Coordinated Exercise* ran at the same time. This allowed both organisations to assess the compatibility of their crisis response systems, particularly responses to cyber and hybrid threats. Moreover, in November 2018, the EU conducted a civil-military crisis management exercise in parallel with a NATO staff command-post exercise under *Trident Juncture 18*.

BOX 6: KEY EUROPEAN ENTITIES IN CYBER SECURITY AND DEFENCE

- EU Agency for Network and Information Security
- Computer Emergency Response Team – EU
- European Cybercrime Centre
- European Defence Agency
- European Security and Defence College

56. For its part, the EU recognised cyber security as a fundamental constituent of its security as a whole and has intensified its adaptation accordingly, significantly strengthening NATO's cyber resilience. For example, the EU can now count on several key agencies to bolster its cyber security measures (see Box 6). Moreover, as a regulatory body, the EU's initiatives can substantially advance the cyber security and defence of national networks, including critical infrastructure. Other key recent policy developments include:

- the adoption of the Directive on Security of Network and Information Systems – the first set of EU-wide rules on cybersecurity – which seeks to achieve a high common level of security of network and information systems across the EU for a functional internal market;
- the development of a framework for a joint EU response to malicious cyber activities, the Cyber Diplomacy Toolbox, which offers a variety of instruments, for example the imposition of sanctions, to counter cyber threats;
- two cyber-oriented projects under the EU's new Permanent Structured Cooperation, namely on a Cyber Threats and Incident Response Information Sharing Platform and on Cyber Rapid Response Teams (CRRTs) and Mutual Assistance in Cyber Security;
- the reinforcement of the mandate of the EU Agency for Network and Information Security; and
- political progress on an EU framework for cybersecurity certification concerning online services and consumer devices.

IV. CONCLUSION

57. If they only looked at the bad cyber news flooding media outlets, policymakers could easily lose hope. However, this report's in-depth analysis of Allied and NATO cyber strategies, policies, and activities has shown that NATO is strengthening cyber security, defence, and deterrence in all dimensions. The new cyber space doctrine to be adopted by the end of 2019 will be another crucial step.

58. This progress should not lead to complacency. NATO must remain laser-focused on cyber-attacks that could threaten an Ally's territorial integrity, political independence, or national security and could, thus, lead them to invoke Article 5. The resolution 459 adopted at the 65th NATO PA Annual Session represents the Assembly's overall cyber policy recommendations. However, the Committee approved the following set of recommendations. The Rapporteur urges the Committee to closely follow progress on these recommendations through all instruments available.

Cyber Security and Defence

59. Each Ally has an individual responsibility to maintain and develop both individual and collective capacity to resist cyber attacks. Member states must therefore live up to this responsibility by fulfilling their national cyber commitments under the NATO Defence Planning Process as well as the NATO Cyber Defence Pledge. Allies and, where applicable NATO as an organisation, should redouble their efforts regarding:

- cyber capability development;
- cyber defence expenditures;
- adaption of Allied and NATO structures;
- integration of cyber effects into military operations;
- refinement of cyber strategies and policies at the national and NATO levels;
- cooperation and exchange of best practices;
- situational awareness, information sharing, and assessment;
- enhancement of skills and awareness across all national and NATO stakeholder communities;
- fostering education, training, and exercises;
- strengthening effective cyber partnerships with industry, academia, partner nations (especially NATO aspirant countries), and other international organisations, especially the EU as part of the NATO-EU Strategic Partnership;

60. Allies should also strongly consider making defensive and offensive cyber effects available for NATO operations on a voluntary basis, if they have not already committed to do so.

Cyber Deterrence

61. The Alliance should continue to complement cyber security and defence measures with strategies of cyber deterrence. NATO should maintain a cyber deterrence policy of ambiguity. The Alliance should not set thresholds for when a cyber attack is sufficiently harmful to be considered an armed attack, nor for what the possible collective response would be if that threshold were crossed.

62. Allies and NATO should continue to signal their resolve and credibility to deter cyber attacks. NATO should therefore remain as transparent as possible when it comes to its cyber capabilities. In areas where public disclosure is not an option, communicating with potential opponents through non-public channels should happen as frequently as possible.

63. The Alliance should continue to seek to reduce escalatory risks through clear diplomatic messaging and engagement, a high level of transparency on cyber capabilities and policies, and support to norm-development and confidence-building measures in cyber space.

Persistent Cyber Campaigns

64. The Alliance must recognise the long-term strategic risk constituted by persistent cyber campaigns. NATO and Allies must counter such campaigns with the right mix of security, defence, and deterrence, including increased civil preparedness and resilience. A more intensive debate about such persistent cyber campaigns should take place within the Alliance. Allies must continue to refine their strategies for countering hybrid threats, including through improved situational awareness via better intelligence and information sharing and other means.

65. If feasible, Allies should also name and shame perpetrators of malicious cyber operations, in a timely manner and preferably in coordination. They should also engage in further discussions about increasing transparency at the NATO level.

SELECT BIBLIOGRAPHY

The report also draws extensively on publicly available information from NATO's and NATO entities as well as EU websites. For more information, please contact the Committee Director.

Brent, Laura, "NATO's Role in Cyberspace", *NATO Review*, 2019

Davis II, John S. et al., *Stateless Attribution: Toward International Accountability in Cyberspace*, RAND Corporation, 2017

Davis, Paul K., "Deterrence, Influence, Cyber Attack, and Cyberwar", *New York University Journal of International Law and Politics*, vol. 47, no. 2, 2014

Giles, Keir and Hartmann, Kim, *"'Silent Battle' Goes Loud: Entering a New Era of State-Avowed Cyber Conflict"*, in: Minarik, Tomas et al. (eds), 2019 11th International Conference on Cyber Conflict, Tallinn: NATO CCD COE Publications, 2019

Hennessey, Susan, "Deterring Cyberattacks: How to Reduce Vulnerability", *Foreign Affairs*, vol. 96, no. 6, 2017

Hoffman, Wyatt and Levite, Ariele E., *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?*, Carnegie Endowment for International Peace, 2017

Lewis, James A., "Cyberspace and Armed Forces: The rationale for Offensive Cyber Capabilities", *Strategic Insights*, Australian Strategic Policy Institute, 2016

Lewis, James A., "Deterrence in the Cyber Age", *Global Forecast 2015*, Center for Strategic and International Studies, 2014

Lewis, James A., *Rethinking Cybersecurity: Strategy, Mass Effect, and States*, Center for Strategic and International Studies, 2018

Lin, Herbert S, "Offensive Cyber Operations and the Use of Force", *Journal of National Security Law & Policy*, vol. 4, no. 63, 2010

Lindsay, Jon R., "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack", *Journal of Cybersecurity*, vol. 1, no. 1, 2015

Morgan, Patrick M., *Deterrence Now*, Cambridge: Cambridge University Press, 2009

Nakasone, Paul M., "An Interview with Paul M. Nakasone", *Joint Forces Quarterly*, vol. 92, no. 1, 2019

NATO, *Brussels Summit Declaration*, NATO, 2018a

NATO, *Civil Preparedness*, NATO, 2018b

NATO, *Cyber Defence Pledge*, NATO, 2016a

NATO, *Wales Summit Declaration*, NATO, 2014

NATO, *Warsaw Summit Communiqué*, NATO, 2016b

Nye, Joseph S.(Jr.), "Deterrence and Dissuasion in Cyberspace", *International Security*, vol. 41, no.3, 2017

Pernik, Piret, *Preparing for Cyber Conflict Case Studies of Cyber Command*, International Centre for Defence and Security, 2018

Robinson, Neil, "Cyber Defence at NATO: from Wales to Warsaw, and Beyond", *Turkish Policy Quarterly*, 2017

Shea, Jamie, "How is NATO Meeting the Challenge of Cyberspace?", *Prism,* vol. 7, no.2, 2017

Slayton, Rebecca, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment", *International Security*, vol. 41, no. 3, 2017

Stoltenberg, Jens, *Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London*, NATO, 23 May 2019

Tusk, Donald, Juncker, Jean-Claude, and Stoltenberg, Jens, *EU-NATO Joint Declaration*, 2016

UN GGE, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2013

US Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, 2018

US DOD, *DOD Dictionary of Military and Associated Terms*, DOD, 2019

US DOD, *Summary: Department of Defense Cyber Strategy*, US DOD, 2018

US NIST, (National Institute of Standards and Technology), *Cybersecurity Framework*, n.d.