NATO PARLIAMENTARY ASSEMBLY

SCIENCE AND TECHNOLOGY COMMITTEE (STC)

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

Draft General Report

by Susan DAVIS (United States)
General Rapporteur

087 STC 19 E | Original: English | 18 April 2019

Until this document has been adopted by the Science and Technology Committee, it only represents the views of the General Rapporteur.

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. Networks owned and operated by NATO suffer hundreds of cyber incidents every month, and intrusions into crucial networks in Allied 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 visits and biannual meetings. In recent years, the Committee has also examined specific cyber issues in depth (see Box 1).

3. This draft general report, submitted for the STC's consideration, 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 which 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 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 and took other key decisions. 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).

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, 2018).

6. This draft 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;
- Outline key elements of NATO's current cyber policies and activities; and
- Address crucial questions on how to stabilise cyber deterrence.

7. This draft report will be presented during the 2019 NATO PA Spring Session. A revised version will then be presented for adoption at the 2019 Annual Session. This version will contain concrete policy recommendations, which will provide the basis for a policy resolution to be submitted to the NATO Secretary General and Allied nations.

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*

II. CYBER ATTACKS IN STRATEGIC AND OPERATIONAL THOUGHT

8. To provide a basis for an informed discussion, it is essential to understand how cyber attacks fit into the current cyber threat landscape and emerging strategic and operational thought.

A. CYBER ATTACKS AND ATTACKERS

9. Regrettably, the term 'cyber attack' is often used very loosely in public discussions. While lines may indeed be blurry in practice, it is crucial to distinguish between proper cyber attacks and other types of cyber operations, such as cyber crimes, cyber-enabled information operations, and cyber exploitation (see Box 2). While strong cyber security and defence is the best foundation to counter all these threats, they each require very distinct policy approaches.

BOX 2: MALICIOUS CYBER OPERATIONS

Cyber crimes cover all criminal activities committed through the internet, computer networks, or information system.

Cyber exploitation (which includes cyber espionage) refers to "[a]ctions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions" (US DOD, 2019).

Cyber-enabled information operations aim to "influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries" (US DOD, 2019).

Cyber attacks can be understood as "[a]ctions 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).

10. Only a cyber attack producing sufficient military effects in cyber space or the physical domain could rise to the level where the Alliance would invoke Article 5 (see also Section IV). Of course, other cyber operations pose serious problems for NATO and the Allies. As the Rapporteur showed in her 2018 General Report, cyber-enabled information operations are part of the larger hybrid threat facing NATO. Counterintelligence officers are in a constant fight against digital spies, and it may prove easier for criminals to access NATO's headquarters through cyber space than by more traditional attack methods.

11. Cyber attacks are not only used by states or their proxies. Malicious code (see Box 3) is widely available online, and bad actors can develop their own. However, state and state-sponsored cyber attacks present the biggest threat to the Alliance. 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 can meet this resource threshold. They are thus the central focus of this draft report. Of course, Allies should not be complacent about cyber attacks by terrorist groups. However, NATO's cyber security and defence remains the key to thwarting such attacks. (Deterrence of non-state actors, especially in cyber space, is extremely difficult.)

BOX 3:
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 ATTACKS IN STRATEGIC THOUGHT

12. Pessimists paint a gloomy picture of the cyber attack threat. They fear that states or their proxies could perpetrate large-scale attacks against a) military networks in a disarming first strike or b) civilian critical infrastructure to inflict mass casualties. A state-directed cyber attack may not reach the scale of physical destruction of a “cyber 9/11”, but these threats still necessitate development of individual and cooperative cyber strategies to ensure NATO and its member states are able to counter all potential threats.

13. To develop a sophisticated cyber operation into a tailored attack option, states and other bad actors must effectively use large amounts of expertise and effort. More importantly – just like any state-directed action – cyber operations reflect national policies to advance national aims (Lewis, 2018). In this context, cyber attacks are used by states as violent or coercive actions to achieve certain political or military effects (Lewis, 2018).

14. Moreover, the strategic rationale for a nation state attacking civilian critical infrastructure is extremely weak (except perhaps in long wars as discussed below). An unprovoked attack would be illegal under international law and even a ruthless attacker should recognise that, historically, attacks on civilian critical infrastructure 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.

15. In sum, pre-emptive cyber attacks on military networks to disarm an opponent or on civilian critical infrastructure seem less plausible options for states and their proxies, although they cannot be ruled out.

C. CYBER ATTACKS IN OPERATIONAL THOUGHT

16. 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 could certainly play a critical role in compromising essential domestic and military infrastructure. Armed forces have responded to this potentiality with increased integration of defensive and offensive cyber capabilities into their operations planning (Lewis, 2018; Davis, 2014).

17. Since cyber capabilities can produce significant military effects, NATO and many other armed forces see cyber space as a distinct military domain and have begun integrating cyber capabilities through the following measures:

- Develop cyber capabilities;
- Combining cyber options with, for example, electronic warfare, anti-satellite operations, and information operations;
- Restructuring their command structures;
- Devising cyber doctrines and embedding them in overall doctrine; and
- Examining how national and international law applies to cyber capabilities.

18. Some analysts argue that states would 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). As a counter to this, NATO member states such as the United States have developed the doctrine 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).

19. In wartime, offensive cyber capabilities are increasingly seen as supporting, to prepare the battlefield or collect intelligence. Cyber attacks are likely to only cause limited casualties or physical damage, as they mainly produce cyber or information effects, for example (Lewis, 2016):

- Degradation, disruption, or destruction of military command and control networks or weapons and sensor systems, slowing down decision making or delivering tactical success if timed right;
- Psychological effects in the defender's population or the international community, for example to undermine citizens' trust in the government's ability to win the war; and
- Producing symbolic effects for a domestic audience, for example to bolster confidence in the government's actions.

20. As the armed forces develop operational doctrines, a key concern is how to prevent cyber attacks from affecting civilian networks and perhaps causing civilian casualties. While this is indeed a crucial question, it must be noted that this risk is rather low when military networks are targeted. They are deliberately isolated from other military networks as well as civilian ones (Lewis, 2016).

21. In a longer war, critical infrastructure could become a tempting target to degrade the defender's war efforts or, more doubtfully, undermine public confidence. This includes, for example, defence industry facilities or power and electricity networks which military forces rely on. While such actions could, during wartime, be legal under international law, the attacker must weigh the benefits with the political costs.

D. STRATEGIES TO COUNTER CYBER ATTACKS

22. As armed forces around the world, including in potential adversary states, build up their cyber capabilities, NATO and its member states must devise strategies to counter the threat of serious state-directed cyber attacks.

23. 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. The Alliance has also declared its support for "work on voluntary international norms of responsible state behaviour and confidence-building measures regarding cyberspace" (NATO, 2016). Allies furthermore made clear that they "stand to benefit from a norms-based, predictable, and secure cyberspace" (NATO, 2018). However, it is unrealistic to expect that NATO, as an Alliance of 29 sovereign nations, could become the primary driving force for 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. Due to the specific characteristics of malicious cyber code, policy instruments important in other military domains – such as effective arms control, disarmament, and non-proliferation measures – very likely remain beyond reach for now, most importantly because verification seems impossible.

24. As a consequence, NATO has been utilising the same general strategies it uses to counter other armed attacks: dissuasion by denial and deterrence by punishment.

25. 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 either fail or, at the very least, not benefit from a cyber intrusion (Nye, 2017). Such cyber dissuasion is squarely premised on strong cyber security and defence (see Box 5).

BOX 4: CYBER SECURITY AND DEFENCE DEFINED

Cyber security aims "to prevent unauthorized 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).

26. Cyber security and defence include a range of preventive, passive, and active measures. They 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 4). Preventive and passive cyber security and defence measures are fundamentally reactive. However, determined intruders are often very agile and adapt rapidly to circumvent new cyber security or defence measures. Many defenders thus turn to more active cyber defence, which does not only operate on the defender's networks but can cross over into the attacker's networks to retaliate. Defenders can 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). Needless to say, the most active cyber defence measures continue to attract numerous practical, legal, and political challenges.

27. 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 could easily 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; italicised in original). It should be noted some experts would argue that the 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 the 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

III. NATO CYBER SECURITY AND DEFENCE POLICY

28. 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. The North Atlantic Council provides high-level political input and oversight; the Cyber Defence Committee manages further political governance and advances cyber policy adaptation; and the Cyber Defence Management Board coordinates policy throughout the NATO structures. Since the critical 2014 Wales Summit, NATO and the Allies have focused on:

- Developing national capabilities;
- Integrating cyber capabilities into operational planning;
- Cooperating in concrete activities; and
- Building up a strong network of partners.

A. ALLIED CYBER CAPABILITY DEVELOPMENT

29. 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).

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

- Development of the full range of capabilities to defend national cyber defences, infrastructure, and networks;
- Allocation of resources to strengthen national cyber defence capabilities;
- Deepening of interaction between national stakeholders to exchange best practices;
- Improvement of shared understanding and assessment of cyber threats;
- Enhancement of cyber skills and awareness;
- Fostering of cyber education, training, and exercises; and
- Facilitation of compliance with agreed cyber defence commitments.

B. INTEGRATING CYBER CAPABILITIES INTO NATO PLANNING

31. 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, 2016). 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, 2016). It also broadly supports NATO defence and deterrence policy.

32. The recognition of the 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.

33. Since 2016, several Allies have confirmed their willingness to contribute offensive as well as defensive cyber capabilities to NATO operations, namely Estonia, Denmark, the Netherlands, the United Kingdom, and the United States (Pernik, 2018). 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.

34. 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 a closer cooperation between the Supreme Allied Commander Europe (SACEUR), Allied Command Operations (ACO), and the NATO Communications and Information Agency (NCI Agency) (Shea, 2017).

35. 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).

C. CONCRETE COOPERATION IN NATO

36. Concrete cyber cooperation in NATO focuses first on protecting NATO-owned and operated networks and second on enhancing cyber security and defence in Allied states through awareness raising, education, training, exercises, information sharing, and mutual assistance.

37. Numerous policy, military, and technical bodies within the NATO structures play key roles in implementing NATO's cyber policies, including the Consultation, Control and Command 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 Cooperation Cyber Defence Centre of Excellence (CCD COE) in Tallinn.

38. 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 draft 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 Malware Information Sharing Platform, Smart Defence Multinational Cyber Defence Capability Development, and Multinational Cyber Defence Education and Training.

39. The NCI Agency and the CCD COE also bear special mentions, as they deliver very concrete results in support of the Alliance.

40. 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 principal role in technology acquisition, experimentation, interoperability, systems and architecture design and engineering, and testing and technical support.

41. 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 operational levels and no matter whether networks are static, mobile, or deployed. It also provides cyber threat analysis. Another key capability of the NCIRC is its Rapid Reaction Team (RRT) capability, which can be deployed to NATO sites, in operational theatres, or in support of an Ally upon approval by the North Atlantic Council. The RRT capability has a core of six experts, and it is able to respond within 24 hours of the incident.

42. The NCI Agency is currently consolidating its training facilities. By the third quarter of 2019, Portugal will thus 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.

43. 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.

44. The CCD COE is another important asset for Allies as a recognised source of expertise. It currently brings together 21 NATO members states 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 product 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.

45. The CCD COE also coordinates two important exercises. The flagship exercise is *Cyber Coalition*, which involves more than 700 participants from member nations, NATO's partners, the EU, the academia, and the industry. *Cyber Coalition* aims at enhancing cooperation and coordination between Allies and testing of NATO and national procedures of information sharing, situational awareness, and decision making. *Cyber Coalition* 2018 specifically exercised the integration of sovereign assets provided voluntarily by Allies (Brent, 2019). The second key exercise is *Locked Shields*, most recently conducted as *Crossed Swords* in February of 2019, which tests the skills of cyber experts in intensive Red Team versus Blue Team scenarios (Shea, 2017). *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.

D. NATO'S CYBER PARTNERSHIPS

46. 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.

47. Industry plays a central role in providing technical solutions and innovations, but 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.

48. 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.

49. 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 our coordination on cyber security and defence including in the context of our missions and operations, exercises and on education and training" (Tusk, Juncker, and Stoltenberg, 2016).

50. 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 Technical Arrangement to facilitate information sharing; and
- Strengthening cooperation on training and exercises.

51. 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.

52. In terms of exercises, the EU cyber staff participated for the first time in the 2017 *Cyber Coalition* and 2018 *Locked Shields* Exercises). 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 the *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

53. 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. NATO CYBER POLICIES AND DETERRENCE STABILITY

54. As this draft report shows, the Alliance continues to strengthen its cyber security and defence. In theory, cyber security and defence is a straightforward proposition. Defenders try to reduce vulnerabilities, block access points, and minimise the lethality of payloads. In practice, NATO has been working to consistently strengthen its collective cyber security, though much work remains to be done. Cyber deterrence is a different, and more complex, matter. Even in theory, cyber deterrence is not straightforward. Since deterrence has been a cornerstone of NATO's cyber defence strategy, this section will examine some of the key problems in cyber deterrence to lay groundwork for concrete recommendations.

A. THE PROBLEM OF ATTRIBUTION

55. The problem of attribution looms large in cyber deterrence discussions. Attackers can hide their tracks by using third-party networks. Establishing connection to a state, even when an attack is traced back to a certain country, is very difficult. An aggressor state or its proxies can also plant false flags to implicate others.

56. 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. However, at the technical level, attribution is still very difficult. 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). Critics therefore argue that cyber deterrence cannot be very stable. If the attacker can remain anonymous, how can the defender credibly threaten and warn off attackers?

57. When it comes to highly significant, state-directed cyber attacks, i.e. those NATO must care most about, this problem is unlikely to arise. Coercion – whether through cyber attacks or other means – only works if the attacked knows who to yield 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 its cyber attack capabilities, he cannot hide himself. This would defeat the purpose. How can the victim give in to demands if he does not know who the attacker is? (In contrast, cyber criminals *want* to stay anonymous when they, for example, attempt to extort money from victims.)

58. On a technical level, one should keep in mind that truly harmful cyber attacks are very complicated and involve many moving pieces. It thus becomes likely that the attacker will also commit mistakes along the way, enabling a forensics expert to trace the origin of the attack (Lindsay, 2015).

59. In sum, NATO's cyber deterrence should work in those instances where the Alliance needs it to work most: state-directed cyber attacks rising to the level of armed attacks. However, this does not solve the problem of attacks below that threshold. When an attacker does not want to coerce but merely wants to achieve tactical or operational gains, anonymity is an excellent advantage for the attacker – and one that plays out in cyber space every day.

B. AMBIGUITY ON THRESHOLDS AND PUNISHMENT

60. 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, but also poses distinct challenges.

61. 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 treading lightly. A similarly vague deterrence posture arguably worked well during the Cold War. However, ambiguity on where the threshold lies could indeed lead an opponent who is sufficiently comfortably with taking risks, to continuously exploit the 'grey zones', test the defender's resolve, and conduct ever more daring cyber attacks.

62. 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. Arguably, the solution for such attacks cannot be found in deterrence, but rather in clearly defined policy response for hybrid operations. Despite its best efforts, the Alliance continues to struggle to develop such options. Setting specific thresholds without strong options for hybrid operations would only encourage more of them. Moreover, the Allies could also find it hard to agree on and perhaps also credibly commit to a specific threshold. Thus, on balance, the policy of ambiguity on thresholds makes sense.

63. 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. While NATO would retaliate in a proportional manner, it could do so through similar cyber attacks, air strikes, or worse. 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?

64. On balance, 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. That being said, in practice, this so-called cross-domain deterrence can be complicated, problematic, and difficult to control (Nye, 2017). For example, proportional response in the mind of the defender might look escalatory to the attacker.

C. ESCALATION DYNAMICS

65. Experts still struggle to understand how cyber attacks affect stability during crises and wartime. Which types of cyber attacks would be de-escalatory, escalatory, or neutral? Would the answer differ depending on when, during a crisis or a war, they would be launched? And are there significant differences between various states on these answers?

66. As argued, states most likely do not see a cyber attack as a viable option for a pre-emptive, disarming first strike. However, in a crisis or pre-war situation, states 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.

67. In short and intense conflicts, pressures to use cyber attacks on military targets are high, as they are just another tool in the box, and the probability of attacks on critical infrastructure is still low, since they would not degrade the defender's capabilities quickly enough to make a crucial difference (Lewis, 2018). If the war is expected to last longer, the latter type of attacks could appear more tempting, however.

68. 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, pursue active defence measures, 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).

69. Escalation dynamics deserve considerably more attention by experts as well as practitioners. For now, however, several 'safe' ways exist to stabilise cyber deterrence, including clear diplomatic messaging and engagement; a high level of transparency on cyber policies; examining these dynamics in exercises; and norm-development and confidence building measures.

D. SIGNALLING CAPABILITIES AND RESOLVE

70. A key feature of a stable deterrence situation is a state's ability to signal their 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.

71. In cyber deterrence, states 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, 2015). 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 can "generally can help to signal resolve" (Lindsay, 2015). In other words, transparency on cyber security and defence measures also serves as a deterrence signal.

72. 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.

V. CONCLUDING REMARKS

73. This draft report has provided an in-depth analysis of crucial Allied and NATO cyber security, defence, and deterrence policies, activities, and discussions. It shows that cyber security, defence, and deterrence is a complex matter and many difficult questions remain.

74. In the face of the ubiquitous bad cyber news flooding media outlets, policy makers should not lose hope. Cyber security, defence, and deterrence is still an emerging topic in international security affairs. Historically, it took experts and officials in Washington and Moscow about two decades to reach basic tenets about nuclear deterrence, and understanding the military and strategic effects of air power was hardly any different.

75. The good news is that NATO is strengthening cyber security and defence along all dimensions, and deterrence remains reasonably stable when it comes to cyber attacks that could threaten an Ally's territorial integrity, political independence, or national security. However, this should not lead to complacency. The General Rapporteur will therefore continue to examine how NATO and the Allies must improve its cyber policies and activities. She will propose a strong set of recommendations at the 2019 NATO PA Annual Session, and she therefore welcomes input from Committee members during the Spring Session. Lastly, she also hopes that this draft report further informs discussions in national parliaments.

SELECT BIBLIOGRAPHY

The draft 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

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, 2018

NATO, *Wales Summit Declaration*, NATO, 2014

NATO, *Warsaw Summit Communiqué*, NATO, 2016

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

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

US DoD (Department of Defense), *DOD Dictionary of Military and Associated Terms*, DOD, 2019

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