ANALYSIS

PLANNING FOR CYBER IN THE NORTH ATLANTIC TREATY ORGANIZATION

KATE MILLER
Kate Miller is a research and project assistant with the Cyber Security Project at the Harvard Kennedy School's Belfer Center for Science and International Affairs. Previously she has worked with the Center's Project on Managing the Atom and interned with the U.S. State Department, contributing to reporting on European affairs. Kate received her M.A. in International Security and her B.A. in International Relations and French, with a focus on transatlantic security.

Introduction

Over the course of the past decade the North Atlantic Treaty Organization (NATO) has worked to ensure that its mission of collective defence and cooperative security is as effective in cyberspace as it is in the domains of air, land, sea, and space. It has created several bodies and developed a collection of policies to deal with diverse aspects of cyberdefence. With the anticipated elevation of cyberspace to the fifth operational domain of warfare at the 2016 Warsaw Summit, however, the Alliance needs to consider cyber capabilities and undertake planning for operations – including offensive ones – directed beyond its networks. And it should establish a Cyber Planning Group to do it[1].

> The Alliance needs to consider cyber capabilities and undertake planning for operations - including offensive ones - directed beyond its networks.

Fortunately, while the issue of cyber operations beyond NATO's own networks is a politically difficult one given the complex mosaic of national, transnational (EU), and international law; the role of national intelligence efforts in certain types of operations; and ever-present disputes over burden-sharing, the Alliance already has invaluable experience in developing policies and procedures for contentious and sensitive tools in the form of the Nuclear Planning Group (NPG). This article will thus proceed as follows: It begins with a brief overview of actions NATO has already taken to address cyberthreats. It will then explore why these, while important, are insufficient for the present and any imaginable future geopolitical threat environment. Next, it will address the history of the NPG, highlighting some parallels with the present situation regarding cyber and drawing out the challenges faced by, and activities and mechanisms of, the NPG. Finally, it will make the case that a group modeled on the NPG can not only significantly enhance the Alliance's posture in cyberspace, but can serve as an invaluable space for fostering entente and reconciling differences on key aspects of cyber policy. It concludes that the Alliance needs to consider offensive cyber capabilities and planning, and it needs a Cyber Planning Group to do it.

Given NATO's collective defence mandate, a brief note on the use of the terms "defensive" and "offensive" operations and capabilities is appropriate and even necessary. When the term "defensive" is used here, it refers to activities within NATO's own networks, taken either to protect Alliance information systems, enhance resiliency in the event of a breach, or impede and/or remove any unauthorized presence. "Offensive" operations or capabilities cover the range of activities that may take place outside of NATO networks, including dismantling or sinkholing botnets (networks of

[1] | The views expressed are the author's own.

computers infected with malware and controlled as a group), distributed denial of service (DDoS) activities, the introduction of malicious code into adversary networks, etc.

Defensive Efforts

The Alliance, as mentioned, has created a number of bodies to address various aspects of defensive capabilities and policies in cyberspace. The NATO Communication and Information Agency (NCIA), for example, provides technical cyber security services throughout NATO, and through the NATO Computer Incident Response Capability (NCIRC) Technical Centre responds to "any cyber aggression against the Alliance[2]". Along with the NATO Military Authorities, it is responsible for identifying operational requirements, acquisition, implementation, and operating of NATO's cyberdefence capabilities. The Alliance also has a Rapid Reaction Team of six civilians, which can be deployed to NATO facilities, operational theatres, or to support an Ally enduring a significant cyberattack[3]. The NATO Consultation, Control and Command (NC3) Board provides consultation on technical and implementation aspects of cyberdefence, while the Cyber Defence Management Board (CDMB), comprised of leaders of the policy, military, and technical bodies in NATO that handle cyberdefence, coordinates cyberdefence throughout NATO civilian and military bodies[4]. At the political level, the Cyber Defence Committee is charged with political governance and cyberdefence policy in general and provides oversight and advice at the expert level. Outside of the NATO Command Structure and NATO Force Structure, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, is a research and training facility that offers crucial cyberdefence education, consultation, and research and development.

The Alliance has also developed and endorsed a collection of policies to guide its approach to conflict in or through cyberspace. In late 2007 it adopted the NATO Policy on Cyber Defence that, as stated in the Bucharest Declaration, emphasized NATO's need to protect key information systems, share best practices, and help Allies counter cyberattacks[5]. The Strategic Concept adopted at the 2010 Lisbon Summit tasked the North Atlantic Council with developing an in-depth cyberdefence policy and action plan, mandated the integration of cyberdefence into operational planning processes, and committed to both promote the development of Allies' cyber capabilities and assist individual members on request[6]. The 2011 Cyber Defence Concept, Policy, and Action Plan updated the 2008 policy and called for the Alliance to further develop the "ability to prevent, detect, defend against, and recover from cyberattacks[7]". It also further integrated cyberdefence into existing policy processes by connecting the CDMB efforts with the Defence Policy and Planning Committee[8]. Finally, at the 2014 Wales Summit, NATO endorsed

[2] | Healey, J. and Tothova Jordan, K. NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow, 2014, [online] http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf (access: 28.05.2016), p.4.

[3] | Men in black – NATO's Cybermen, 24 April 2015, [online] http://www.nato.int/cps/en/natolive/news_118855.htm (access: 21.06.2016).

[4] | Cyber Defence, 16 February 2016, [online] http://www.nato.int/cps/en/natohq/topics_78170.htm (access: 08.06.2016).

[5] | Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic council in Bucharest on 3 April 2008, (Press Release (2008) 049) [online] http://www.nato.int/cps/en/natolive/official_texts_8443.htm (access: 30.05.2016).

[6] | Lisbon Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 20 November 2010, (Press Release (2010) 155), [online], http://www.nato.int/cps/en/natolive/official_texts_68828.htm (access: 21.06.2016); Cyber Defence, op cit.

[7] | Chicago Summit Declaration Issued by the Heads of State and Government Participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012, (Press Release (2012) 062), [online], http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en (access: 30.05.2016).

[8] | Fidler, D., Pregent, R., Vandume, A., NATO, Cyber Defense, and International Law, [in] Articles by Maurer Faculty. Paper 1672, 2013, [online] http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub (access: 08.06.2016).

an Enhanced Cyber Defence Policy, which clarified for the first time that a cyberattack on a member state could be covered by Article 5 (the collective defence clause) of the North Atlantic Treaty.

These organs and bodies all serve vital functions, but they do not go far enough. At present, the Alliance has only limited publicly articulated policy regarding the use of cyber tools to target adversaries' computers and networks in response to either cyber or kinetic/conventional attacks[9].

> “ NATO needs to address the lack of policy around how the alliance and member states may use offensive cyber capabilities in both defensive and offensive operations.

While NATO may have a classified policy or doctrine that goes beyond its statement that it “does not pre-judge any response and therefore maintains flexibility in deciding a course of action” in response to a cyber attack, this suggests a vacuum that undermines the credibility of the Alliance's collective defence and common security[10]. NATO needs to address the lack of policy around how the alliance and member states may use offensive cyber capabilities in both defensive and offensive operations. And it requires a body authorized and equipped to develop that truly comprehensive, integrated cyber policy and situate it within the Alliance's broader strategies and objectives.

The Need For Offense

The question of whether and how NATO should undertake cyber operations outside of its own networks, even in defensive, counter-attack scenarios, is not new. The Alliance has a long-standing defensive orientation and has stated on multiple occasions that its top priority is the protection of its networks and the cyberdefence requirements of the national networks upon which it relies[11]. This stance risks becoming a cyber “Maginot line” rather than an effective strategy, however, and many have argued that it must extend its focus[12]. The Atlantic Council's Franklin Kramer et. al., for example, recently called on NATO to “develop doctrine and capabilities to provide for the effective use of cyberspace in a conflict as part of NATO's warfighting capabilities[13]”. James Lewis, Senior Fellow at the Center for Strategic and International Studies (CSIS), has noted that some Alliance members already possess offensive cyber capabilities that are “essential for the kinds of combat operations that NATO forces may carry out in the future” and argues the Alliance needs to enunciate how these would be used in support of NATO activities[14]. And Jason Healey, director of the Cyber Statecraft Initiative at the Brent Scowcroft Center on International Security, has repeatedly called on the Alliance to at least consider offensive coordination if it cannot develop its own offensive capabilities[15].

Offensive cyber capabilities serve a number of purposes. They can act as an important force multiplier, especially in asymmetric conflicts. If,

[9] | For an exception, see NATO's Rules of Engagement for Computer Network Operations, contained in Series 36 of the MC-362/1 catalogue.

[10] | Defending the networks: The NATO Policy on Cyber Defence, 2011 [online] https://ccdcoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf (access: 08.06.2016).

[11] | Ibidem.

[12] | Fidler, D. et. al, op cit. p. 23.

[13] | Kramer, F., Butler, R., and Lotrionte, C., Cyber, Extended Deterrence, and NATO, [in] Atlantic Council: Brent Scowcroft Center on International Security Issue Brief, May 2016, [online] http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf (access: 03.06.2016), p. 6.

[14] | Lewis, J., The Role of Offensive Cyber Operations in NATO's Collective Defence, “The Tallinn Papers” 2015, No. 8, p. 3.

[15] | Healey, J., op cit., p. 6.

for example, conflict broke out in the Baltics, NATO or individual Allies' cyber capabilities targeting an adversary's communications, logistics, and sensors could preclude a fait accompli and buy the Alliance precious time to mobilize land, sea, or air forces[16]. This also suggests that in some ways such tools are an extension or evolution of electronic warfare (EW) capabilities, long essential to assuring information superiority and thus NATO's military effectiveness. In the 1950s, NATO promulgated an EW Policy that recognized "the establishment and maintenance of superiority in [EW] is an essential part of modern warfare" and acknowledge that "since all NATO nations and commands will be conducting [EW] operations, it is essential that the coordination and control be exercised at the highest level feasible[17]". As cyber and EW merge and cyber becomes embedded in warfighting, then, a similar policy that outlines responsibilities and national authorities pertaining to cyber operations is needed.

Offensive capabilities also create strategic flexibility, offering an option that falls between talking and bombing. This is particularly important given the hybrid warfare that has taken place in the NATO neighborhood and the low-intensity conflict work that NATO has participated in. While offensive cyber tools can have destructive and disruptive effects, they can also be temporary and/or reversible, and therefore represent an option that certain Allies may view as more palatable or acceptable. Furthermore, not only do adversaries already use offensive cyber capabilities against NATO, but if conflict breaks out they will have vulnerabilities that are best exploited using cyber means. As Matthijs Veenendaal et al. point out in a cyber policy brief for the CCDCOE, if NATO faced an air attack it would not prohibit the use of airpower – limiting itself to air defense systems – in response[18]. For member states to deny the Alliance cyber capabilities, or even the ability to plan for their use by individual Allies, fundamentally undermines NATO's deterrent posture and its credibility among both its own members and its potential adversaries. It also corrodes NATO's ability to prevail as a collective defence entity in a conflict. Finally, while there is no reason a proportional response needs to be symmetric (i.e. confined to the same domain), an enunciated offensive capability and policy on its use would also impact potential adversaries' risk calculations, forcing them to recognize that NATO can respond in kind, as well as kinetically or conventionally[19].

There are, of course, a number of challenges associated with the use of cyber capabilities, especially in a collective manner. As President Toomas Hendrik Ilves of Estonia noted at the June 2016 CyCon, when it comes to cyber, NATO members are in "intelligence agency mode" where they "share as little as possible and only when necessary[20]". This is to some extent understandable: highly targeted cyber tools often rely on intelligence that is both difficult to obtain and inherently impermanent, making national entities reluctant to share information even regarding a particular tool's anticipated effects. Unlike nuclear weapons, which have more or less the same effect no matter where deployed with the only truly important variable being scale, even partial information about the targeting or functionality of a given cyber capability may allow the target to patch a vulnerability or disconnect a particular device, rendering the tool ineffective

[16] | Kramer, F., et. al, pp. 8-9.

[17] | NATO Electronic Warfare Policy [in] A Report by the Standing Group to the Military Committee on NATO Electronic Warfare Policy, (MC 64), 14 September 1956, [online] http://archives.nato.int/uploads/r/null/1/0/104853/MC_0064_ENG_PDP.pdf (access: 03.06.2016), pp. 2-3.

[18] | Veenendaal, M., Kaska, K., and Brangetto, P., Is NATO Ready to Cross the Rubicon on Cyber Defence? "Cyber Policy Brief," June 2016, [online] https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf (access: 21.06.2016).

[19] | Lewis, J., op cit. p. 7.

[20] | Ilves, T., President Toomas Hendrik Ilves's opening speech at CyCon in Tallinn on June 1, 2016, [online] https://www.president.ee/en/official-duties/speeches/12281-president-toomas-hendrik-ilvess-opening-speech-at-cycon-in-tallinn-on-june-1-2016/index.html (access: 09.06.2016).

or altering its effect. Sharing such information can increase the likelihood it will be leaked and thus result in what is essentially inadvertent unilateral disarmament. Furthermore, intelligence efforts are under the control of national governments and often require enormous amounts of time and effort[21]. Although it is likely that any adversary which attacks NATO is targeted by member states' collection activities, it is an admittedly complicating factor in any Alliance effort to operate effectively outside of its own networks in cyberspace.

> “Once NATO decides it needs to address offensive capabilities, of course, a key issue will be how it develops plans and policies for their use.

An additional issue is the scale and specificity of any given cyber tool (that is, how easily it propagates and limitations on targeting) and the complicated legal environment in which NATO must operate. The Alliance has to navigate a complex web of national, EU, and international law regarding the conduct of military operations and develop policies and strategies that result from and in legal convergence. While there is evidence that software can be highly discriminate and proportionate and its spread controlled, without sufficient preparatory work its effects can be unpredictable and hard to contain. In particular, untargeted entities may be impacted (although, again, if appropriate preparatory effort is made, such entities should not experience deleterious effects even if they are infected with a piece of code or malware). This suggests additional complications for NATO, which must grapple with the risk that certain strategies will reveal or create friction or legal divergence in the Alliance[22].

The Nuclear Planning Group Model

Once NATO decides it needs to address offensive capabilities, of course, a key issue will be how it develops plans and policies for their use. This is where the experience of the NPG is illuminating, demonstrating both the limitations such a group will face as well as highlighting reasons to believe in its potential.

The Nuclear Planning Group was established in 1966 in order to address nuclear weapons in the European theater: an issue that inflamed debate from the beginning on how they might be used (and the consequences of their use) – much as offensive cyber capabilities have done[23]. The introduction of theater nuclear weapons under U.S. President Dwight D. Eisenhower's “New Look” strategy stripped non-nuclear allies of operational control of the Alliance's military posture and handed it to the Americans (and, to a lesser extent, the British), who owned the weapons and thus had significant influence over the strategies that governed them[24].

This imbalance induced dissatisfaction and stress in the Alliance that was further aggravated when new weapons were developed or major revisions in strategy (such as the Kennedy Administration's Flexible Response) were proposed. These tensions, in turn, undermined cohesion – and therefore effectiveness and credibility – within the Alliance. The NPG was thus needed not only to address actual force posture and planning issues related to command and control, but to serve the vital political purpose of preserving cohesion. In much the same way, advanced cyber warfighting capabilities are unevenly distributed among allies, and yet just as nuclear weapons were a central element in the Alliance's defensive posture, so these capabilities will be vital in any future conflict. And like theater nuclear weapons before

[21] | Lewis, J., op cit., p. 9.

[22] | Fidler, D., et. al, op cit. p. 13.

[23] | Buteux, P., The Politics of Nuclear Consultation in NATO 1965-1980, Cambridge, 1983, p. 3.

[24] | Ibidem p. 7.

the establishment of the NPG, cyber capabilities lie largely outside the Alliance's institutional framework.

At its inception, only seven states sat on the NPG at any given time: the United States, United Kingdom, Italy, and West Germany were permanently represented while the remaining seats rotated among eligible nations (i.e. those participating in the integrated military structure)[25]. (Today, all NATO members with the exception of France participate in the NPG, irrespective of their possession of nuclear weapons.) Broadly speaking, the group provided a consultative process on nuclear doctrine within NATO. In particular, it focused on three issues of nuclear planning:
(1) how and under what circumstance the Alliance may need to use nuclear weapons;
(2) the question of what objectives might be served by the use of nuclear weapons in the European theater; and
(3) what kinds of consultation should take place in circumstances where the use of nuclear weapons could be contemplated[26]. The NPG also allowed the Alliance to isolate the issues of nuclear planning and doctrine from other matters, protecting it to some extent from being impacted by disagreements over other alliance policies[27].

Significantly, the NPG largely avoided issues of ownership, physical possession, and therefore of direct control of nuclear weapons and decisions regarding their use, which resided in national governments. This was in part a response to earlier efforts to address nuclear sharing, wherein the aggregation of agreement on participation in NATO's nuclear policy and agreement on ownership, force composition, and decision-making formulae actually reinforced the intractability of the sharing issue[28]. Instead, the NPG focused on allied consultation and participation in planning, an approach that was both politically and operationally more feasible for countries controlling the weapons (primarily the United States). While avoiding joint control, this ensured non-nuclear allies could have a role in the procedures by which those possessing nuclear weapons reached decisions concerning them, offering an avenue to constrain their behavior. For the states controlling the weapons, those processes served to reinforce cohesion in the Alliance and allowed them to win support and acceptance for their nuclear policies[29].

The issue of secrecy, mandated on the part of the United States by legislation intended to restrict the spread of nuclear technology, also had a significant impact on the work of the NPG. On the one hand, this legislation, including the Atomic Energy Act, limited the amount of information on nuclear matters the U.S. government could reveal to NATO allies. In particular, the 1958 amendment to the Atomic Energy Act gave the U.S. Congress the power to veto any "atomic cooperation for military purposes with any nation or regional defence organization...[30]". On the other hand, as early as 1954, in response to the development of a Soviet nuclear capability, the United States adjusted its laws in order to supply nuclear information and materials to its NATO Allies in order to reinforce its deterrent and collective defence[31]. Furthermore, by 1961 the United States recognized that in order to get other Allies to understand and accept as doctrine its strategic innovations, it needed to relax its approach to nuclear secrecy. This led the United States to offer much more detailed information than it previously had regarding both technical characteristics of the weapons and relative force levels and strategic concepts[32].
The above considerations offer key insights into

[25] | Cyber Defence, op cit.

[26] | Buteux, P., op cit. p. 89.

[27] | Ibidem, p. 61.

[28] | Ibiden, p. 15.

[29] | Ibidem, pp. 184-186.

[30] | Nieburg, H., Nuclear Secrecy and Foreign Policy, Washington, D.C. 1964, p. 50.

[31] | Ibidem, p. 19.

[32] | Buteux op cit. p. 21-22.

how a Cyber Planning Group could function. First, issues of secrecy regarding various capabilities, while they will limit what the Group can discuss, need not prevent it from undertaking consequential work. Identifying circumstances when use might be appropriate and developing procedures for consultation regarding that use require only a general sense of their effects, allowing secrecy regarding precise operation. However, the nuclear experience also suggests that key Alliance members can overcome the habit of secrecy if there is sufficient need for information sharing to reduce friction and facilitate consensus building within NATO. Moreover, there is a sense in some segments of the United States that, as former director of the National Security Agency and Central Intelligence Agency General Michael Hayden has stated, information on U.S. cyber policies is "overprotected" and there is a need to "recalibrate what is truly secret[33]". It may be that as cyber becomes increasingly integrated into military operations, the need for cooperation will outweigh the desire for secrecy.

Another useful lesson that may serve to reduce friction at the outset is that Allied or joint control of offensive capabilities – especially those that rely on extensive intelligence efforts – is likely politically impossible and operationally undesirable. That does not negate the value of consultation and an allied approach to planning for their use, however. Developing a collective understanding of how and under what circumstances these capabilities may be deployed by members on behalf of the Alliance, and the possible consequences of that deployment, can enhance its defensive and deterrent posture by expanding its arsenal and lending credibility to threats to utilize it. It is also vital that interested parties understand what tools and resources are and are not available for their defence in order to assure effective planning.

Furthermore, while Allied use of cyber capabilities that can result in significantly destructive outcomes will likely be highly constrained for the foreseeable future, there is no reason the Alliance should not develop doctrine and/or policies regarding the use of activities such as distributed denial of service attacks or dismantling botnets[34]. These are activities regularly deployed against the Alliance and its member states that, in a time of conflict, may be useful to NATO. Just as the NPG discussed the possibility of using theater weapons to slow a conventional invasion, for example, a Cyber Planning Group should examine how limited offensive tools such as denial of service activities or actively hunting and dismantling a botnet can offer a stopgap measure to disrupt an adversary's malicious activity, even if said adversary is not attacking by cyber means. During the 2008 war between Georgia and the Russian Federation, for example, Georgia's efforts to respond to Russian military maneuvers were impeded by widespread denial of service attacks, website defacements, and related activities that impacted the government's ability to communicate with its populace as well as the outside world[35]. Such capabilities would be useful for NATO and/or its member nations in the event of a conflict.

Finally, it is important to appreciate that the establishment of a Cyber Planning Group would constitute a statement of policy in and of itself, regardless of what it may accomplish. Just as creating the NPG signaled to both the Soviet Union and to NATO members that the issue of theater nuclear weapons was a vital one demanding

[33] | Hayden, M., Statement of The Honorable Michael V. Hayden, (Testimony), Cyber Threats and National Security, House Select Intelligence Committee, (4 October 2011), [online], http://congressional.proquest.com.ezp-prod1.hul.harvard.edu/congressional/result/congressional/pqpdocumentview?accountid=11311&groupid=103838&pgId=43b-c3ae6-fbd2-47a7-b887-914ecc3d3224 (access: 21.06.2016).

[34] | This principle has been acknowledge, allowing work to begin on Allied Joint Doctrine for Cyberspace Operations. It is unclear to the author to what extent this doctrine may address activities outside NATO networks, however.

[35] | Bumgarner, J., and Borg, S., Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008, 2009 [online] http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf (access: 30.05.2016).

dedicated study by the Alliance, so a Cyber Planning Group could emphasize for Allies and adversaries alike the seriousness with which NATO addresses the issue of comprehensive, integrated cyber operations.

Conclusion

NATO's member states have proven sensitive to discussing cyber capabilities directed beyond its own networks, let alone the question of whether and how the Alliance may use them[36]. Rather than indicating that NATO should let the issue lie, however, the contentious nature of the issue and absence of discussion suggest that consultation and efforts to build consensus are important for alliance cohesion in a volatile and divisive international environment. The fact of the matter is that these capabilities are likely to be crucial in any future conflict. Consultative procedures may serve to reveal and then reduce fractures in the Alliance before those conflicts break out.

The Alliance's central mission of collective defence, including in cyberspace, will soon require a comprehensive cyber operations policy in order to maintain the credibility of both its deterrent and defensive posture. It is an admittedly challenging issue, with many conflicting aspects, but to continue to ignore it will limit NATO's ability to serve as a useful mechanism for handling collective defence, common security, and crisis management. Therefore, NATO should take up the invaluable lessons offered by the experience of the Nuclear Planning Group and either expand the portfolio of the current Cyber Defence Committee (and perhaps the CDMB) to include offensive cyber tools and operations or establish a new body modeled on the NPG.

One of the most remarkable features of the Alliance has been its ability to remain relevant by evolving to address changing threats, ranging from Soviet military power in Europe to international terrorism. By engaging in consultations focused on understanding when offensive cyber capabilities will be most useful and appropriate and what objectives they can help achieve, and developing a coherent yet flexible doctrine, a Cyber Planning Group will assure NATO's continued relevance – and thus its future. ■

[36] Fidler, D., et. al, op cit. p. 24.