Tallinn, June 2016

Cyber Policy Brief

Is NATO Ready to Cross the Rubicon on Cyber Defence?

Matthijs Veenendaal
Kadri Kaska
Pascal Brangetto

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence. It does not necessarily reflect the policy or the opinion of the Centre, NATO, any agency or any government. The authors wish to thank William Haynes III for his contribution and editorial assistance.

Allies remain reticent when it comes to discussing the options of using military (offensive) capabilities within a NATO setting.

In April 2016 Robert Work, United States Deputy Secretary of Defense, declared "[w]e are dropping cyberbombs" on ISIS.[1] Though rather rhetorically, this statement demonstrates that cyber capabilities are now seen as weapons. Although much remains unclear about the future relevance of cyberspace as a domain for military operations, it is beyond doubt that cyber capabilities can launch attacks that may cause death and destruction.

Given modern armed forces' dependency on digital technology, it is legitimate to expect that NATO would adapt to this new reality. Since 2002, NATO has invested significantly in improving the defence of its networks. However, NATO has shown little inclination to move away from its current purely defensive posture in cyber defence. At the political level, Allies remain reticent when it comes to discussing the options of using military (offensive) capabilities within a NATO setting. For most of them, cyber operations are generally still uncharted territory in which confusion abounds. Moreover, Allies that have invested heavily in cyber capabilities worry that others might benefit without making a similar investment themselves. Allies therefore remain reluctant to engage in any meaningful discussion on the position and role of cyber capabilities in military operations within the Alliance.

In order to achieve a more mature and realistic cyber defence posture, the Alliance must address two important issues. Firstly, it must clearly recognise that network defence does not equal collective defence in cyberspace. Secondly, given that NATO accepts the applicability of collective defence in cyberspace, Allies should develop the full range of military capabilities to defend the Alliance and its interests.

Adapting the Response to Cyber Attacks

NATO has declared that, if attacked through cyberspace, the North Atlantic Council will decide on the invocation of Article 5 on a case-by-case basis, essentially abstaining from pre-judging any response and therefore maintaining flexibility in deciding a course of action that may or may not be taken.[2] However, as long as NATO's cyber defence policy remains focused on and interpreted from the perspective of network defence, the envisioned flexibility will not include a course of action that involves the use of military cyber capabilities. The question then arises whether "any military force [can] credibly claim to have advanced capabilities if it does not include offensive cyber operations in its arsenal?"[3]

[1] David Sanger, 'U.S. Cyberattacks Target ISIS in a New Line of Combat', *The New York Times,* April 24 2016. http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0

[2] Steve Ranger, 'NATO updates cyber defence policy as digital attacks become a standard part of conflict'. ZDNet, June 30, 2014. http://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/. Cf. 'Defending the networks, The NATO Policy on Cyber Defence', 2011. http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

[3] James A. Lewis, 'Offensive Cyber Operations and NATO', *Tallinn Paper no. 8,* Tallinn 2015, page 2.

Apparently, the US thinks there is nothing wrong with this defensive approach. In June 2015, the US Secretary of Defense, Ashton Carter, stated that "NATO must improve its ability to defend itself against cyber attacks before it tries to build its offensive cyber warfare capabilities."[4] Carter is, of course, right that it will not be NATO that builds offensive cyber capabilities. This is no different from the other domains of warfare where Allies develop capabilities that can be deployed in a NATO setting. However, it implies that the Alliance, in its overall posture, should continue to focus on defensive measures, excluding the option for using offensive capabilities in a joint operational setting. A purely defensive posture has not been the favoured option of successful military commanders. As Clausewitz articulated it, "the defensive form in war is […] no mere shield but a shield formed of blows delivered with skill".[5]

Network Defence and Collective Defence

NATO has defined two distinct responsibilities concerning cyber defence: (a) collective defence and (b) the protection of NATO networks. In 2011, the NATO Cyber Defence Policy established that "[i]n order to perform the Alliance's core tasks of collective defence and crisis management, the integrity and continuous functioning of its information systems must be guaranteed."[6] The Wales Summit Declaration of 2014 expanded on this when the Alliance affirmed that cyber defence is part of NATO's core task of collective defence, yet the Enhanced NATO Policy on Cyber Defence of 2014 failed to delineate roles and responsibilities.[7] The task of defending the alliance against armed attacks through cyberspace with military means was thereby added on top of a policy for network defence.

As long as the NATO Cyber Defence Policy merely recognises that the principle of collective defence is applicable in cyberspace, while limiting possible action to the protection of networks, it will continue to cause confusion among Allies. The principle of collective defence is NATO's *raison d'être* and lies at the heart of Article 5 of the Washington Treaty. It commits the Alliance to protect and defend the Allies' territory and populations against an armed attack.[8] Consequently, the accepted core responsibility of the Alliance in cyberspace is to defend the Allies against armed attacks through cyberspace, when necessary through military means. However, the only means at its disposal is the protection of its own networks and systems. This means that while the Alliance recognises that cyberspace can be used by adversaries to launch an armed attack against it, it is impossible for the Alliance to counter such an attack in and through cyberspace. For NATO, this is rather a novel approach to its responsibilities. It would, for instance, be unimaginable that in response to an armed air attack, NATO would not allow for the use of air power, but would limit its response to the use of air defence systems.

While the Alliance recognises that cyberspace can be used by adversaries to launch an armed attack against it, it is impossible for the Alliance to counter such an attack in and through cyberspace.

While the core tasks of collective defence and the protection of own networks are clearly connected and overlapping responsibilities, they are executed under different political, legal, and organisational frameworks. The responsibility for the protection of its own networks is, in principle, the same for NATO as it is for any other large

[4] Lolita C. Baldor, 'Carter: NATO must bolster cyberdefense.' PHYS.org, June 24, 2015, http://phys.org/news/2015-06-carter-nato-bolster-cyber-defense.html#jCp.

[5] Carl Maria von Clausewitz, 'On War', translated by J. J. Graham, Hertfordshire 2013, page 411.

[6] Defending the networks, The NATO Policy on Cyber Defence, 2011. http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf

[7] NATO Wales Summit Declaration, 2014. http://www.nato.int/cps/en/natohq/official_texts_112964.htm; 'Cyber defence', NATO. 16 Feb 2016, http://www.nato.int/cps/en/natohq/topics_78170.htm.

[8] The North Atlantic Treaty, Article 5. http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

public or corporate organisation working with sensitive information. It is essential to the security and continuity of these organisations, but it is a task mostly carried out in a peacetime context and day-to-day business setting. Outside of an armed conflict, cyber attacks against NATO as an organisation will be qualified as cyber espionage, cyber crime or, in some cases, information operations; but not as armed attacks. Thus, the organisation has the obligation to protect its networks, systems and data but there is a big difference between guarding duties and combat actions. Likewise, as the Alliance will not use military means to counter these types of cyber attacks, the guiding policy should not be defined in military terminology or integrated into a larger military framework. However, that does not mean that a guiding policy for the use of cyber operations is unnecessary and it certainly does not mean that a network defence policy can substitute a cyber operations policy.

At CyCon 2016, Vice-Admiral Arnaud Coustillière, the French General Officer on Cyberdefence, explained his job to the audience as "digital combat".[9] That clearly is not and should never be the role of the NATO Communications and Information Agency (NCIA), which is the NATO body responsible for network defence. While NCIA performs an important military role in connecting the Alliance and defending its networks in an operational setting, it does not perform offensive cyber operations. Therefore, it should be clearly defined where the NCIA's role ends and where the NATO Command Structure's begins. Distinguishing network defence and information assurance from offensive military cyber operations will allow the Alliance to clarify the impact and relevance of these issues for NATO. It will allow the Alliance to develop adequate means of response for cyber threats across the spectrum, including the necessary frameworks to support these changes, and thereby improve NATO's overall military effectiveness.

NATO and Cyber Operations

Until now, the Alliance has not drawn the necessary conclusions from the recognition that "cyber attacks can threaten the prosperity, security, and stability of the Alliance".[10] The NATO Strategic Concept of 2010 commits the Alliance to "ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations".[11] Moreover, the full range of capabilities explicitly includes the "[further development of] our ability to prevent, detect, defend against and recover from cyberattacks."[12] This means that NATO must be in a position to defend the freedom and security of the Allies against threats emanating from cyberspace and be able to respond to these threats appropriately. NATO must take the responsibility to bring its cyber defence policy in line with the Strategic Concept and ensure that it has the full range of military capabilities needed to defend the Alliance and its interests in and through cyberspace.

NATO must be in a position to defend the freedom and security of the Allies against threats emanating from cyberspace and be able to respond to these threats appropriately.

This would also bring NATO policy in line with the strategies and policies of numerous Allies that have developed frameworks for the use of cyber capabilities in military operations. The Netherlands, for example, has declared that "[o]perational digital resources … cover defensive, offensive and intelligence-gathering elements"

[9] Public remarks made by Vice-Admiral Arnaud Coustillière at CyCon 2016, Cyber Commanders Panel on June 1, 2016. Recording forthcoming in the second half of 2016 at www.cycon.org.

[10] NATO Strategic Concept, 2010. http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf, para. 12.

[11] Ibid, para. 19.

[12] Ibid.

and defines offensive capabilities as “digital resources whose purpose is to influence or pre-empt the actions of an opponent by infiltrating computers, computer networks and weapons and sensor systems so as to influence information and systems.”[13] Similar ambitions are now being translated into specific military doctrines by many nations.

The US currently offers the most detailed and holistic overview of the role of cyber capabilities and cyber operations in military doctrine. The US has opted for an approach that views cyber capabilities as operational military capabilities to be used as part of a military operation.[14] For example, according to the National Military Strategy for Cyberspace Operations of 2006 “[the] DoD will execute the full range of military operations in and through cyberspace to defeat, dissuade, and deter threats against the US interests.”[15] In line with the overall US military doctrine, it states that “[o]ffensive capabilities in cyberspace offer the US and our adversaries an opportunity to gain and maintain the initiative. DoD cyberspace operations are strongest when offensive and defensive capabilities are mutually supporting.”[16]

If NATO is to continue to fulfil the role defined in its Strategic Concept, it will need to bridge the gap between the national cyber operations strategies of various Allies and its own policy on cyber defence. Recognising cyberspace as a domain would be an important step in the right direction for NATO. This will impel the Allies to define not only terms and definitions but also to establish common ambitions, procedures, and doctrine.

As Allies are developing operational cyber capabilities, NATO needs to start planning for their potential use in joint military operations.

The core of NATO’s activities has always been military cooperation between Allies that predominantly takes the form of joint military operations and campaigns, or collective defence of NATO territory. The NATO Defence Planning Process, designed to ensure that Allies have the necessary means and capabilities for such cooperation, enables these activities.[17] As Allies are developing operational cyber capabilities, NATO needs to start planning for their potential use in joint military operations. Regarding the possible deployment of offensive cyber capabilities, nations will wish to retain control over the use of these assets at the highest level in the foreseeable future. Cyber capabilities are still viewed by most nations as strategic assets. As these capabilities depend largely on secrecy, nations will be unwilling to delegate this to a commander in the field. For example, in the US, only the President can approve a cyber operation likely to result in “significant consequences.”[18] However, this does not mean that these capabilities are irrelevant to NATO and NATO-led operations. As these capabilities are a reality, the Alliance must plan for the contingency of nations wanting to deploy them during a NATO-led military operation.

Dealing with the need for secrecy or political sensitivity concerning specific military operations is not new for the Alliance. For example, in order to develop a full-fledged cyber doctrine, it would be useful to look at the NATO Allied Joint Doctrine for Special Operations.[19] In its introduction, it states that special operations “may be

[13] Update to the Dutch Ministry of Defence Cyber Defence Strategy. *Parliamentary document 33321, no 5.,* February 2015, page 6.

[14] In the National Military Strategy for Cyberspace Operations of 2009, the US makes the distinction between Network Defence and Cyberspace operations. United States Department of Defense, National Military Strategy for Cyberspace Operations, 2009, page 5.

[15] Ibid, page 2.

[16] Ibid, page 10.

[17] Hannes Krause, ‘NATO on its way towards a comfort zone in cyber defence’, *Tallinn paper No.3,* Tallinn 2014, page 4.

[18] Lewis, Offensive Cyber, page 8.

[19] Allied Joint Doctrine for Special Operations (AJP-3.5), January 2009. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33694/AJP01D.pdf.

described as military activities conducted by specially designated, organized, trained, and equipped forces using operational tactics, techniques, and modes of employment not standard to conventional forces. Politico-military considerations may require low prominence, covert or discreet techniques, and the acceptance of a degree of physical and political risk not associated with conventional operations."[20] This approach may very well be comparable to an eventual one for cyber operations. At the least, it demonstrates that the Alliance is adaptable and capable of developing a working doctrine for capabilities using "specially designated forces that use techniques not standard to conventional forces" and require "covert or discreet techniques".

Conclusions & Recommendations

Much remains unclear regarding the impact, possible cascading or unforeseen effects, counter-measures by adversaries, and political consequences (escalation) of the use of offensive cyber capabilities. This uncertainty makes nations reticent to commit to specific and ambitious new policy objectives. Yet this reluctance should not forestall a comprehensive debate within NATO. Given the fact that some Allies have declared the ambition to develop offensive cyber capabilities and that these have been deployed as part of military operations, the expiration date of the current defence-limited policy appears due. In our opinion, NATO should therefore urgently:

- recognise cyberspace as a domain for military operations;
- distinguish the policy mandate applicable to network defence in peacetime from the policy mandate applicable for cyber operations in military operations and collective defence, and instigate development of a new policy that will enable the Alliance to ensure that it has the full range of capabilities necessary to deter and defend against any threat in and through cyberspace;
- develop doctrine and procedures to allow for the use of cyber capabilities as operational military capabilities.

NATO should invest in a rigorous and transparent debate on the nature and implications of operational cyber capabilities as well as in the development of policies, doctrines, procedures, and a legal framework to allow for the deployment of cyber capabilities during NATO missions.

In our opinion, regardless of NATO recognising cyberspace as a domain for military operations, the Alliance will have to cross the Rubicon on Cyber Defence and align its cyber defence policy with the overall, conventional, strategic posture as detailed in the Strategic Concept.

NATO should, therefore, invest in a rigorous and transparent debate on the nature and implications of operational cyber capabilities as well as in the development of policies, doctrines, procedures, and a legal framework to allow for the deployment of cyber capabilities during NATO missions. Even if cyberspace turns out to be a different kind of environment for military operations than the traditional domains, these discussions will help ensure that NATO maintains its relevance as a military alliance regarding cyber threats.

[20] Ibid, page 1-1.

About the Authors

MATTHIJS VEENENDAAL

Matthijs Veenendaal has been working for the Netherlands Ministry of Defence since 2006 in various policy positions. He is currently stationed as a researcher at the Strategy Branch of the NATO Cooperative Cyber Defence Centre of Excellence in Estonia. He has been closely involved in the development of cyber defence policy of the ministry of Defence and the principle author of the first Defence Strategy for operating in cyberspace (2012). He was also closely involved in the development of the two National Cyber Security Strategies of the Netherlands. Matthijs studied contemporary history at the university of Leiden and political science at the University of Texas, Austin.

KADRI KASKA

Kadri Kaska is a researcher at the NATO Cooperative Cyber Defence Centre of Excellence. As a legal and policy analyst with over 15 years of experience, her current research focus is on national cyber security strategies and organisational models, in particular cyber aspects of crisis management. She has also consulted on developing cyber security policy and strategy. Kadri holds a master's degree in Law from the University of Tartu, Estonia, and has earlier served as a legal adviser to the national Communications Regulatory Authority and the National Competition Authority, participating in the drafting of national telecommunications legislation and advising on communications resource management, standards, and competition issues.

PASCAL BRANGETTO

MAJ Pascal Brangetto is a supply officer in the French Army. He graduated from the Military Administration Academy in 2006 and served as a 1st lieutenant at the 4th French Foreign Legion Batallion as a deputy administrative and supply officer. Then he went on to serve as an administrative and supply officer at the 1st Medical Battalion in Metz and was deployed for a tour of duty in Afghanistan during the ISAF operation in 2010. Before being posted as a legal researcher at NATO CCD COE in 2013, he was a staff officer in the French Joint Supply Service Directorate in Paris. Major Brangetto is a graduate from the Institut d'Etudes Politiques in Aix-en-Provence.