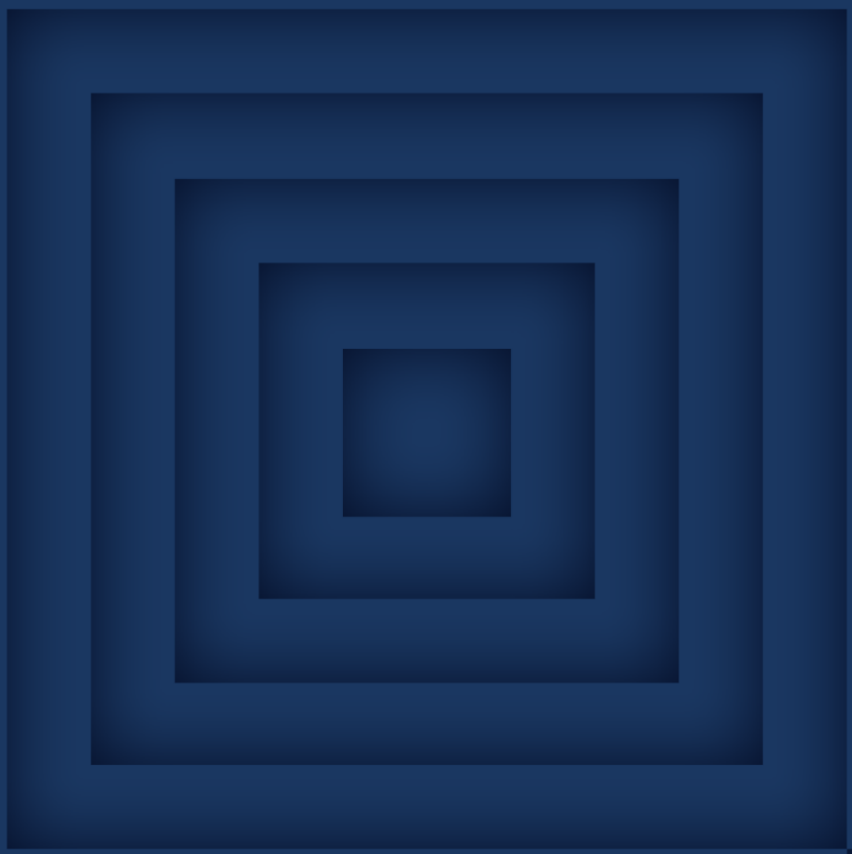
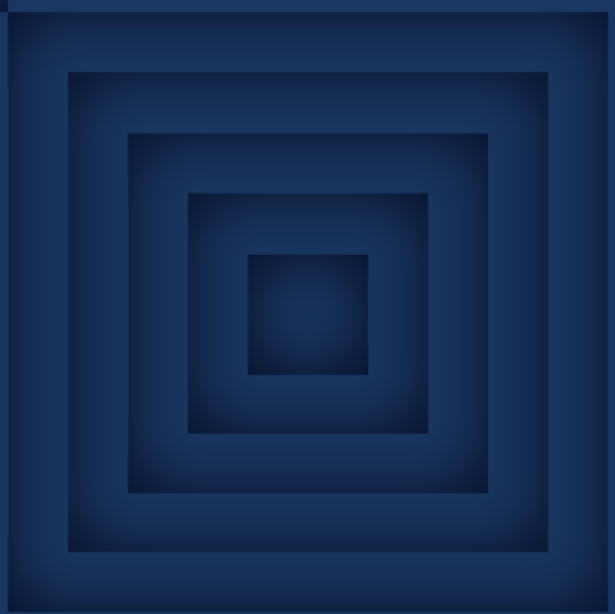
The Hague Centre
for Strategic Studies

NATO allies' offensive cyber policy: A growing divide?

Author: Dr. Max Smeets
Editors: Dr. Michiel Foulon & Dr. Jack Thompson
August 2021





HCSS Security

1. Alliances

1.3. NATO allies' offensive cyber policy: A growing divide?

Max Smeets

NATO allies have made slow but steady progress when it comes to crafting policy to deal with cyber security challenges. Yet this progress has not always been made in a collaborative fashion. Especially when it comes to the development and deployment of offensive cyber capabilities, NATO allies are increasingly *diverging* in policy. This is a worrying development and deserves more attention than it has so far received.

Steady progress

Member states agree on the critical need for a coherent cyber policy. Almost all NATO allies have developed both a cyber security strategy and a cyber defense strategy.[1] Some states have published updated versions over the years to reaffirm cyber security as an issue of national security importance, to tweak institutional responsibilities, or to articulate changes in the threat landscape. In addition, since 2018, most NATO allies have established a military cyber organization (either a command or unit) with a mandate to conduct cyber effect operations – that is, cyber operations intended to disrupt, deny, degrade or destroy.[2] There is also shared recognition that international law applies in cyberspace, although allies have yet to spell out the legal procedures for operating in this new "domain of warfare."

These developments have been both reflected in, and aided by, policy progress made at the inter-governmental level. At the Prague Summit in 2002, NATO for the first time recognized that the Alliance should "Strengthen our capabilities to defend against cyber attacks."[3] In 2008, at the Bucharest Summit, there was another milestone development, when NATO adopted a "Policy on Cyber Defense," aiming to "protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack."[4] In the same year, the Cooperative Cyber Defence Centre of Excellence – a NATO accredited international research institution – was established in Tallinn, Estonia. In 2016, at the Warsaw Summit, cyberspace was officially recognized as a "domain of operations" and allies made a Cyber Defense Pledge to enhance their cyber defenses.[5] The 2018 Brussels Summit and 2020 London Summit reiterated NATO's commitment to implement the Cyber Defense Pledge and operationalize the Cyber Operations Center, responsible for situational awareness and the centralized planning of cyber operations and missions.[6] In January 2020, the Allied Joint Doctrine for Cyberspace Operations was published "to plan, execute and assess cyberspace operations (CO) in the context of allied joint operations."[7]

Steady divergence

[1] See the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), https://ccdcoe.org/library/publications/.
[2] Max Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis", Conference paper, *11th International Conference on Cyber Conflict: Silent Battle*, T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, and G. Visky (eds.) (2019), https://ccdcoe.org/ uploads/2019/06/Art_09_NATO-Members-Organizational-Path.pdf.
[3] NATO, "Prague Summit Declaration" (21 November 2002), https://www.nato.int/cps/en/natohq/official_texts_19552.htm?
[4] NATO, "Bucharest Summit Declaration" (3 April 2008), https://www.nato.int/cps/en/natolive/official_texts_8443.htm.
[5] NATO, "Warsaw Summit Communiqué" (9 July 2016), https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
[6] NATO has developed the Sovereign Cyber Effects Provided Voluntarily by Allies mechanism. This is coordinated through the CYOC. See NATO, "Brussels Summit Declaration" (11 July 2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
[7] NATO, "AJP-3.20: Allied Joint Doctrine for Cyberspace Operations" (January 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

Yet when it comes to the *direction* of allies' cyber policy, growing differences are apparent – especially in the development and deployment offensive cyber capabilities. First, even though most states now have – or are in the process of – establishing a cyber command, operational capabilities vastly differ across states. Whereas some governments are increasingly allocating significant resources to conduct cyber operations – and are now starting to benefit from these investments – the majority of allies still run their cyber commands on a budget of a few million a year – an amount that is insufficient for effective operations in the cyber domain.

Secondly, until a few years ago, NATO members' strategic visions were largely aligned. National cyber strategies shared a common threat focus on operations that could potentially cause major societal havoc, such as taking down the power grid. Allies' national strategies were also largely unified in their vision to address this threat, discussing the need for deterrence, resilience, and norms. However, this changed with the publication of the US Department of Defense's strategy on Defend Forward and US Cyber Command's vision on Persistent Engagement.[8] The United States emphasizes the need to cause friction "wherever the adversary maneuvers," operating "globally, continuously and seamlessly" (potentially) below the threshold of armed attack. "We must...maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries," in the words of NSA director and Cyber Command head Gen. Paul Nakasone.[9] Whereas deterrence is about changing your adversary's cost-benefit calculus, Persistent Engagement is about taking the opportunity away from the adversary to act.[10]

Third, NATO member positions on how international law applies – particularly the obligations of states vis-a-vis sovereignty – are now more divergent than a decade ago. Whereas countries like the Netherlands and France are located on the side of the "sovereignty as a rule" camp, the United Kingdom has taken the position that a remote cyber operation by one state into another's cyber systems or network does not violate the latter's sovereignty.

Where to go from here?

The divergence in cyber policy across NATO member states is problematic. Allies disagree on both the goals of cyber policy and the ways and means to achieve them. This can cause tension between allies, especially when it comes to the necessity and legitimacy of operating on each other's national systems and networks.

Some may argue that these differences result from differences in maturity. Some states simply have not caught up with the latest developments, goes the argument. This assumes a single path to cyber maturity or that the dynamics of cyberspace pull all states in the same direction. It suggests that – even without major policy coordination – allies' cyber policies will converge over time. But a more persuasive understanding of the current trend is that even though states can learn from each other's institutional progress, differences do not merely stem from states "lagging behind." These states are on a different policy path. This means it requires dedicated and sustained policy attention to, at a minimum, coordinating the different policies of states – and potentially bringing them closer together.

What can be done to ensure that this divergence in cyber policy does not cause further friction between allies?[11]

I have previously proposed a NATO Memorandum of Understanding (MoU) to reduce discord among the allies; the goal would be to enhance trust, transparency, and confidence between allies and to improve the effectiveness of disrupting and deterring adversaries' operations in cyberspace.[12] The main purpose of the MoU would be to reach an agreement on the equities involved in permitting signatories to conduct cyber effect

[8] U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command" (2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010; Department of Defense, "Cyber Strategy 2018: Summary" (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[9] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly*, 92:1st Quarter (2019), https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-92.aspx.

[10] That said, there is a growing awareness amongst allies that activity below the threshold can be strategically meaningful. At the Brussels Summit in 2021, allies recognized that "the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack."

[11] More on types of friction see: Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," *Lawfare*, Blog post (28 May 2019), https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

[12] Max Smeets, "U.S. cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection," *Intelligence and National Security*, 35:3 (2020).

operations in each other's networks—and the relative weight of those equities.