G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Policy Brief

2018 | No. 039

Offense as the New Defense: New Life for NATO's Cyber Policy

By Sophie Arts

Against the backdrop of a fast-developing cyber threat landscape, NATO has struggled to enact a comprehensive strategy that sufficiently prepares allies to deter or defend themselves against cyber-attacks. While important steps have been taken, the alliance is still nowhere near ready to face cyber threats at the 'speed of relevance'. Individual members' guarantees to use their cyber capabilities on behalf of the alliance – as the United States announced this year – can help fill that gap in strategy.

Yet, without a well-defined policy agreement between the member states and a clear command structure in overseeing NATO operations, this approach risks unintended consequences – particularly as offensive cyber operations have the potential of cascading into conventional conflict. To prevent such a scenario, allies should further formalize their cyber strategy through top-down guidance and increase their cooperation with partners to broaden their spectrum of potential responses. Most importantly, NATO needs to streamline its decision-making process in the cyber domain and to define potential response scenarios – including and short of evoking the collective-defense clause under Article 5.

The cyber domain has become a critical geopolitical battleground in the current global context, with important implications for NATO. According to Secretary General Jens Stoltenberg, cyber-attacks against NATO's infrastructure increased by 60 percent between 2016 and 2017.[1] Most were state-sponsored. Meanwhile cyber interference in national networks is on the rise across member states, with the United States reporting the highest number of data breaches in 2018, followed by the United Kingdom.[2]

Against this backdrop, members have taken important steps to raise national and alliance resilience against cyber threats in the last four years. But after the July 2018 Brussels summit, NATO is not yet prepared to face the cyber threat with the necessary resolve. Estonia's cyber ambassador, Heli Tiirmaa-Klaar, stated in September that the alliance is at roughly 10 percent of readiness when it comes to understanding, responding to, and preventing cyber threats.[3] Most member-state and NATO officials agree that more needs to be done. While the alliance is moving forward with critical changes in its command structure with the aim of improving

1 Doorstep statement by NATO Secretary General Jens Stoltenberg prior to the informal meeting of EU Ministers of Defense, Tallinn, Estonia, September 7, 2017, https://www.nato.int/cps/en/natohq/opinions_146642.htm?selectedLocale=en.

2 "2018 Thales Data Threat Report", http://go.thalesesecurity.com/rs/480-LWA-970/images/2018-Data-Threat-Report-Euro-Edition-uk-es-A4.pdf.

3 Catherine Stupp, "Estonia's First Cyber Ambassador Seeks to Improve Global Cyber Defense," *The Wall Street Journal*, September 7, 2018, https://www.wsj.com/articles/estonias-first-cyber-ambassador-seeks-to-improve-global-cyber-defense-1536358734.

the efficacy of cyber operations, individual countries continue to buttress their cyber resilience at home to add to NATO's overall collective defense.

The United States, which has the most advanced cyber capabilities within NATO, has recently declared that it would contribute its national capabilities to alliance operations. At NATO's defense ministerial meeting in Brussels in October, Secretary of Defense James Mattis announced that it "will provide national cyber contributions to help NATO fight in this important domain."[4] Such efforts are in the spirit of similar guarantees already provided by the United Kingdom, Denmark, the Netherlands, and Estonia. The United States is expected to commit both defensive and offensive cyber operations to defend NATO allies.[5] For NATO, which does not have any offensive cyber capabilities of its own, this means starting to fill key gaps in defense and deterrence capabilities in a rapid and ever-expanding threat landscape. However, given the sometimes-fraught relationship between the United States and other NATO allies, which struggle to fully agree on issues from burden sharing to threat perceptions, more clear-cut agreements to streamline and regulate offensive cyber operations within the alliance may be needed.

This brief examines how the U.S. contributions in offensive cyber capabilities add to NATO's cyber resilience and assesses whether the shift from an exclusively defensive cyber posture to a more forward-leaning one bears any inherent risks. To do so, it takes stock of NATO's cyber arsenal, identifies gaps, and proposes steps that will help to ensure that the alliance is well-positioned to deter and defend against cyber-attacks in the future.

A Complex Threat Landscape

> *"This shift from reactive to preemptive action in cyberspace marks the most significant departure from the previous U.S. cyber strategy."*

As a comparatively new and fast-developing domain, cyberspace remains much less regulated than land, air, and sea, making it a prime arena for 'gray zone' challenges. Lack of clarity even extends to the definition of cyber-attacks. According to the Tallinn Manual, a study commissioned by the NATO Cooperative Cyber Defense Center of Excellence that assesses how international law applies to cyber conflict, a cyber-attack is "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[6] This definition, like other ones, leaves significant room for interpretation.

When it comes to defining and measuring cyber-attacks, there is no clear standard that is applied across NATO countries, leading to diverging metrics. This makes it challenging to effectively compare data from different national contexts.[7] One reason why many governments and institutions have refrained from publicizing the metrics they use to measure cyber-attacks is to retain strategic ambiguity that may help to deter attacks that deliberately aim just below a defined threshold to prevent retaliation. With that in mind, NATO has steered away from a more precise definition. However, this strategy also creates gray areas that hostile actors can exploit.

4 "News Conference by Secretary Mattis at NATO Headquarters, Brussels, Belgium," October 4, 2018, https://dod.defense.gov/News/Transcripts/Transcript-View/Article/1654419/news-conference-by-secretary-mattis-at-nato-headquarters-brussels-belgium/.

5 Lolita C. Baldor, "US to offer cyberwar capabilities to NATO allies," Associated Press, https://www.apnews.com/292c4d08912c4e3f8ae29973e0ecfbbc.

6 Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York, United States of America: Cambridge University Press, 2013.

7 Stefan Soesanto, "In Cyberspace, Governments Don't Know How to Count," *Defense One*, September 27, 2018, https://www.defenseone.com/ideas/2018/09/cyberspace-governments-dont-know-how-count/151629/.

Russia, China, Iran, and North Korea are the main facilitators of global malign cyber operations,[8] with Russia leading in capabilities, closely followed by China.[9] However, their use of cyber tools varies. The U.S. National Counterintelligence and Security Center has singled out China, Russia, and Iran as being among the most capable and active actors in the field of cyber economic espionage.[10]

In line with this, the Trump administration recently voiced concerns regarding Chinese interference in U.S. domestic policy.[11] In October, the Department of Justice also indicted Chinese intelligence officers and operatives for hacking into U.S. aerospace companies to steal information. China at this point mostly seems to use cyber espionage to gain access to proprietary technology and intellectual property, seeking to further "its strategic development goals [with regard to] science and technology advancement, military modernization, and economic policy objectives".[12]

Russia is pursuing a more adversarial agenda, using cyber capabilities to gain access to information that it weaponizes in order to sow chaos and mistrust, as well as to attack critical infrastructure with the aim of eroding citizens faith in government and institutions. The very same day that Mattis made his statement in Brussels, the Dutch government announced that it had expelled four Russian military intelligence officers after blocking a Russian cyber-attack on the Organization for the Prohibition of Chemical Weapons headquarters in The Hague in April. The organization was investigating the poisoning of former Russian agent Sergei Skripal in the United Kingdom at the time.[13] Russia's rulers are also driving a state-dominated propaganda campaign to discredit the West for their domestic political ends.

NATO's Cyber Defense Today

> *"Superior cyber capabilities will not be a deterrent per se, but they can add to NATO's resilience against threats."*

With an eye on increasingly sophisticated state-driven cyber-attacks, many NATO allies are working on whole-of-government approaches to increase their readiness. Developing comprehensive cyber defense strategies is challenging, not least because this domain affects a wide variety of activities and services across the military, government, private sector, and media, with vast implications for civilian life. As such, cyber defense may require a broad set of nuanced and targeted responses as well as effective cooperation across sectors.

NATO's foremost priority has been to secure its own institutional infrastructure and computer networks, while supporting and encouraging allies to bolster their cyber defense capabilities through "multinational projects, education, training, and exercises and information exchange."[14] Moreover, NATO has made important adjustments to keep pace with changes in the threat landscape in the last four years. At the Warsaw summit in 2016, allies declared cyber an operational domain and adopted the Cyber Defense Pledge, which commits them to enhancing their national defenses to ensure they are capable of defending themselves "in cyberspace as in the air, on land and at sea."[15]

8 Daniel R. Coats, "Worldwide Threat Assessment of the US intelligence Community," February 13, 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

9 See comments by Dmitiri Alperovitch at Washington Post Cybersecurity Summit 2018, Global threats to U.S. national security panel, October 2, 2018, https://www.washingtonpost.com/video/postlive/cybersecurity-summit-2018-global-threats-to-us-national-security/2018/10/02/a0a82bc4-c657-11e8-9c0f-2ffaf6d422aa_video.html?utm_term=.d8c84fc881b8.

10 National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace*, 2018, https://fas.org/irp/ops/ci/feec-2018.pdf.

11 "Remarks by Vice President Pence on the Administration's Policy Toward China," October 4, 2018, https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-administrations-policy-toward-china/.

12 National Counterintelligence and Security Center, F*oreign Economic Espionage in Cyberspace*, 2018.

13 Tucker Reals, "Netherlands says Russia tried cyberattack on global chemical weapons agency," CBS News, October 4, 2018, https://www.cbsnews.com/news/russia-gru-cyberattack-operation-targeting-opcw-chemical-weapons-netherlands-2018-10-04/.

14 "NATO Cyber Defence Pledge," Press Release (2016) 124, July 8, 2016, https://www.nato.int/cps/su/natohq/official_texts_133177.htm.

15 Ibid.

Two years earlier, at the 2014 Wales summit, NATO officially expanded its Article 5, which commits members to consider an armed attack against one an armed attack against all, to include "significant" cyber-attacks.[16] The 2018 Brussels summit declaration upheld this policy and added to it by declaring that cyber effects could be integrated into the alliance's operations, arguing that "as part of NATO's defensive mandate, [allies] 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."[17] Besides this, one of the most important outcomes of the Brussels summit was the launch of a new Cyber Operations Center in Belgium that will serve to strengthen NATO's command structure and enable it to effectively integrate cyber into allied operations.[18]

Deter, then Defend?

NATO's defenses are only as strong as the sum of those of its members. Like in other domains, alliance cyber assets are not NATO-owned but provided by member states.[19] U.S. capabilities in the cyber domain are by far the most sophisticated among the allies. Besides having an edge over most competitors in the field of cyber security,[20] the United States tops rankings as a global leader in offensive cyber capabilities.[21] The recent announcement that it would contribute its capabilities to NATO operations consequently could help the alliance bolster its deterrence posture against hostile cyber-attacks.

16 Jens Stoltenberg, "Why cyber space matters as much to Nato as land, sea and air defence," *Financial Times*, July 12, 2018, https://www.ft.com/content/9c3ae876-6d90-11e8-8863-a9bb262c5f53.

17 "Brussels Summit Declaration," Press Release (2018), 074, NATO, July 11, 2018 https://www.nato.int/cps/en/natohq/official_texts_156624.htm

18 See NATO, "Cyber Defense," https://www.nato.int/cps/en/natohq/topics_78170.htm.

19 Jamie Shea, "How is NATO Meeting the Challenge of Cyberspace," PRISM, Vol. 7, No 2, December 21, 2017, http://cco.ndu.edu/PRISM-7-2/Article/1401835/how-is-nato-meeting-the-challenge-of-cyberspace/.

20 Cyber DB, "Top 10 Countries Best Prepared Against Cyber Attacks," https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/.

21 Bob Mason, "So Who Has the Most Advanced Cyber Warfare Technology?" NASDAQ, October 19, 2017, https://www.nasdaq.com/article/so-who-has-the-most-advanced-cyber-warfare-technology-cm861979.

Until recently, NATO and member states, including the United States, have relied on strictly defensive cyber tools to protect their infrastructure. However, given that this approach has done little to discourage hostile actors, the strategic value of incorporating offensive cyber operations has long been discussed. In late 2017, Stoltenberg announced that NATO would integrate cyber weapons of its members into military operations to deter and defend against threats, marking the "biggest overall policy shift in decades," according to officials.[22]

> *"Countering cyber threats with offensive operations could have a cascading effect that eventually precipitates conventional conflict."*

The U.S. decision to commit offensive and defensive capabilities to NATO follows on the heels of this move. The addition of offensive cyber tools to the defense and deterrence toolbox is not only new for NATO, it also tracks a recent shift in the U.S. posture. The White House authorized the use of offensive cyber weapons to deter foreign adversaries in September following the publication of the Department of Defense's 2018 Cyber Strategy.[23] The strategy also incorporates a new mission of "defending forward" as a means to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[24] While defending forward is, as the name suggests, defensive in nature, it entails targeting foreign cyberspace infrastructure to pre-empt incoming attacks through offensive cyber operations.

22 According to former team leader of NATO's Task Force Cyber (CISO) Col. Rizwan Ali. See Thomas E. Ricks and Rizwan Ali, "NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons," *Foreign Policy*, December 7, 2017, https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/.

23 Ellen Nakashima, "White House authorizes 'offensive cyber operations' to deter foreign adversaries," *The Washington Post*, September 20, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html?utm_term=.1f668d182794.

24 U.S. Department of Defense, "Summary: U.S. Department of Defense Cyber Strategy 2018," https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

This shift from reactive to preemptive action in cyberspace marks the most significant departure from the previous U.S. cyber strategy, published in 2015, and comes in response to persistent cyber campaigns against the United States directed by Russia and China. Taken individually, these offenses may fall short of provoking an official response, but their cumulative impact over time is a significant concern and needs to be addressed. The new forward-leaning posture of the United States seeks to address this threat preemptively without risking an escalation to conventional military uses of force.[25]

Superior cyber capabilities will not be a deterrent per se, but they can add to NATO's resilience against threats.[26] Aggressive cyber operations have already become an important element in the hybrid warfare tool kit of many adversaries. Adding offensive cyber capabilities will likely not stop this. That is why it is critical that deterrence against cyber threats not only relies on cyber operations, but also draws on the full spectrum of conventional and unconventional responses, as outlined in the 2018 Brussels summit declaration.[27]

Defensive and offensive cyber capabilities can reinforce NATO members' ability to deter and deny cyber-attacks by disincentivizing other actors from developing cyber weapons in the first place, and by convincing those with or without offensive cyber capabilities that attacks will be largely ineffective or come at an equal or greater cost to them. Proactive cyber defense also can help to anticipate and prevent an attack on computers and networks, which requires active monitoring of hostile actors. This is where offensive cyber operations provide the most strategic value. For instance, they could interfere directly with operations of adversaries by manipulating their devices and infrastructure through malware, or by shutting off power and networks from which an attack originates. They can also affect the calculations of hostile actors who may judge that the potential cost of an attack outweighs its strategic gains.

> *"Allies need to do more when it comes to finding common ground on potential policies and responses."*

On the other hand, countering cyber threats with offensive operations could have a cascading effect that eventually precipitates conventional conflict.[28] A more assertive U.S. posture on cyber could thus potentially heighten the risk of an unanticipated crisis in the cyber and conventional domains. This could have serious implications for other NATO allies that might be pulled into a conflict, especially if the lines between NATO and U.S. cyber operations are blurred, based on Mattis' recent statement.

Challenges Remain

While there are still many unknowns in NATO's cyber policy, the United States' announcement did clarify how its capabilities would be used in the event of a joint NATO cyber operation. As indicated by the Pentagon, the United States would maintain control over its own personnel and capabilities. This is by no means unusual and not necessarily a surprise. As in most areas, NATO does not rely on commonly owned assets for cyber defense but on national capabilities.[29] Similarly, NATO members retain command and control of cyber operations they provide. However, as the former team leader of NATO's Task Force Cyber (CISO), Col. Rizwan Ali, has pointed out, this poses a significant challenge to NATO commanders who may

25 Nina Kollars and Jacquelyn Scheider, "Defending Forward: The 2018 Cyber Strategy is Here," *War on the Rocks*, September 20, 2018, https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/.

26 Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyber War," *New York University Journal of International Law and Politics*, Vol. 47, No 2, Winter 2014, http://nyujilp.org/wp-content/uploads/2015/11/NYI203.pdf;
Robert Bebber, "There is No Such Thing as Cyber Deterrence. Please Stop," *The Cipher Brief*, April 1, 2018, https://www.thecipherbrief.com/column_article/no-thing-cyber-deterrence-please-stop

27 "Brussels Summit Declaration," Press Release (2018) 074, NATO.

28 Ibid

29 Jamie Shea, "How is NATO Meeting the Challenge of Cyberspace," *PRISM*, Vol. 7, No 2, December 21, 2017, http://cco.ndu.edu/PRISM-7-2/Article/1401835/how-is-nato-meeting-the-challenge-of-cyberspace/

not have access to many critical details implicating their decision-making process. Ultimately, Ali explained, commanders "will request an effect using cyber weaponry during an operation and one of the allies will provide that effect without any further information."[30] As a result, NATO commanders will be flying blind, lacking many important details regarding limitations of capabilities and potential conflicts with other ongoing operations.

Related to this challenge, NATO's constraints on information sharing could hurt strategic decision-making processes and cyber operations. While most experts acknowledge that intelligence capabilities within NATO are significant, these remain isolated and well-guarded by national intelligence communities.[31] More advanced information sharing, among allies and with other partners such as the EU, is critical for situational awareness and NATO's preparedness. Yet, due mostly to a lack of trust between allies, this process is far from being at an optimal level.[32]

When it comes to intelligence sharing, some allies fear that infiltration and attacks against countries with lower resilience could potentially compromise information shared by other member states. Pushback against greater transparency is especially strong on the part of the United States, which owns a large share of NATO's intelligence capabilities, making it a critical player in alliance intelligence operations from a tactical as well as strategic perspective.[33] Due to the country's outsized role in this field, NATO's intelligence adaptation is largely dependent on U.S. inclinations to share capabilities and information with other allies.[34] Although efforts to protect intelligence by minimizing sharing may be justified, elevating the role of the United States in NATO's cyber policy without increasing transparency could potentially limit tactical effectiveness.

Strategy Before Tactics

In May 2017, former Supreme Allied Commander Europe Philip Breedlove bemoaned the shortcomings of NATO's cyber policy despite "incredible cyber capability."[35] Although the alliance has begun to address the integration of cyber weapons into its arsenal via its members, which Breedlove encouraged, there still is nothing indicating that members have adopted a new comprehensive strategy for offensive cyber operations. With this in mind, Jamie Shea, the former deputy assistant secretary general for emerging security challenges at NATO, has argued that the next political guidance, which is expected in June 2019, has to be "much more expansive and detailed on operational cyber requirements and capabilities than we have seen in the past."[36] However, given that the potential timeline for conflict has been significantly shortened through technological advancements, it may be in NATO's interest to address outstanding questions sooner.

While the United States' announcement that it would contribute its capabilities could help lend credibility to NATO's cyber deterrence, further clarification is needed within NATO, particularly when it comes to its command structure in the cyber domain. Without clarity on this front, it is hard to imagine that the 29 NATO allies who have different threat perceptions, and face issues of cohesion and trust, could agree on effective response scenarios in a crisis situation. This is particularly critical, because cyber operations will be subject to political approval by the NATO allies.

30 Thomas E. Ricks and Rizwan Ali, "NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons."

31 For more on this issue, see Artur Gruszczak, "NATO's Intelligence Adaptation Challenge," Globsec, March 26, 2018, https://www.globsec.org/wp-content/uploads/2018/03/NATO%E2%80%99s-intelligence-adaptation-challenge.pdf.

32 Ibid.

33 Ibid.

34 Ibid.

35 Patrick Tucker, "Former NATO Commander: Alliance Needs to Take Cyber Fight to Russia's Door," *Defense One,* July 6, 2017, https://www.defenseone.com/technology/2017/07/former-nato-commander-alliance-needs-take-cyber-fight-russias-door/139242/.

36 Jamie Shea, "How is NATO Meeting the Challenge of Cyberspace."

The new Cyber Operations Center, which should be fully operational in 2023, could play an important role in that respect, but the lack of operational authority may pose a significant challenge.[37] According to NATO, the center aims to "strengthen cyber defenses and integrate cyber capabilities into NATO planning and operations."[38] But as the U.S. declaration on its potential cyber support to NATO confirms, it appears at this point that the center will serve to coordinate rather than oversee operations. This, coupled with allies' unwillingness to share intelligence that may be critical to NATO's strategic efforts, makes it difficult to envision the center as an effective tool in implementing a coherent top-down cyber strategy in the near future.

While organizational assets, like the Cyberspace Operations Center and the Cooperative Cyber Defense Center of Excellence in Estonia, are critical in bolstering NATO's cyber defense posture and awareness, allies need to do more when it comes to finding common ground on potential policies and responses ahead of actual contingencies so as to enhance their resilience and readiness to meet threats. For NATO's cyber policy, this means outlining realistic crisis scenarios and response mechanisms, while putting in place clear command and decision-making processes, thereby eliminating "gray zones" that adversaries can exploit.[39]

Next Steps

Much has been accomplished over the past few years as NATO prepares to meet and deter growing cyber threats, but its cyber policy still leaves much to the discretion of its individual members. Although in line with the essential character of NATO as an alliance rather than an institution, this approach leaves open many questions that could complicate and impede effective crisis responses. With this in mind, allies should consider the following steps to increase cyber resilience.

> "Allies must be prepared for the use of cyber warfare as part of a larger campaign."

Formalize Strategy Through Top-Down Guidance

To create greater cohesion and increase NATO's cyber resilience, allies should advance the consultation process among themselves to implement clear guidelines from the top.[40] This could be an important first step to develop political solutions at level of the North Atlantic Council that increase resilience and preparedness against cyber and other hybrid threats before implementing new cyber policies across NATO's military command structure and alliance forces. Added to that, allies should consider making member-state resilience even more of a priority by synchronizing metrics and reporting of cyber incidents as well as assets across the alliance, and by clearly defining and raising national minimum standards in capabilities.[41]

Work with Partners and Expand the Spectrum of Responses

Besides dialogue across NATO capitals, exchanges between the alliance and partners like the EU is critical. When facing cyber threats – which not only impact military infrastructure but societies as a whole – greater cooperation between NATO and the EU is key to coordinate efforts that are outside of NATO's domain. Just before the Brussels summit, Stoltenberg and European Commission President Jean-Claude Juncker signed a joint declaration

37 Robin Emmott, "NATO cyber command to be fully operational in 2023," *Reuters*, October 16, 2018, https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9.

38 "The NATO Command Structure Factsheet," NATO, February 2018, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-Factsheet-NATO-Command-Structure_en.pdf.

39 Bruno Lété and Daiga Dege, "NATO Cybersecurity: A Roadmap to Resilience," German Marshall Fund of the United States, July 3, 2017, http://www.gmfus.org/publications/nato-cybersecurity-roadmap-resilience.

40 Brittany Beaulieu and David Salvo, "NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence," German Marshall Fund of the United States, Policy Brief, 2018, http://www.gmfus.org/publications/nato-and-asymmetric-threats-blueprint-defense-and-deterrence.

41 Ibid.

on cooperation between the two institutions and agreed to draft national plans to create "a whole-of-government approach […] to deal with challenges across the hybrid spectrum and to make societies resilient enough to be able to continue to function throughout a crisis or an armed conflict."[42] In line with this, the EU recently decided to work on a new sanctions regime that is specific to cyber-attacks, hoping to disincentivize attacks against member states. [43] With 22 member states in common, this is a prime example of how EU policies can help further NATO's security goals.

Streamline Cyber Decision-making Processes

To allow the alliance to respond swiftly in an emergency without launching lengthy debates between allies, NATO will also need to consider how cyber operations relate to its new readiness plan. In particular, allies must be prepared for the use of cyber warfare as part of a larger campaign; for instance, to prepare the ground for a kinetic attack.

The 'Four Thirties' initiative, which was launched at the Brussels summit in July, holds that by 2020, NATO members will be able to deploy 30 battalions, 30 battleships, and 30 air squadrons within 30 days, adding a significant follow-on force to NATO's Response Force and Very High Readiness Joint Task Force. Though, if successfully realized, this will be a marked improvement when it comes to mobilizing significant force numbers in a short time, this timeline does not quite prepare NATO to act at what has become known as the 'speed of relevance'.[44] Offensive cyber operations could help bridge that gap. But first the coordination of cyber efforts across NATO's command structure would have to be clarified and improved – an effort that could include expanding the emergency powers of the Supreme Allied Commander Europe.[45]

Further Define the Repertoire of Response Scenarios

Perhaps most importantly, as NATO stands ready to integrate defensive and offensive cyber operations, it should further clarify how these relate to its collective defense provision. Although NATO holds that Article 5 could be invoked following a "significant" cyber-attack against one or more of the allies,[46] officials have remained deliberately ambiguous when it comes to defining the parameters of a qualifying attack so as to discourage hostile operations that would fall just below such a specific threshold.[47] Without a clear line, allies have more room to maneuver in a cyber crisis short of invoking Article 5. However, recent experience across the alliance has yielded little proof that the strategic ambiguity in this domain is effective in preventing hostile operations.

As NATO seeks to address this challenge, it will need to assess how to develop an effective cyber policy that balances deterrence with the potential risk for escalation. With this in mind, it should establish more precise thresholds for cyber-attacks and define proportional response scenarios.[48] Without these, it will likely remain very challenging to mobilize allies to invoke Article 5 in a cyber crisis. This could be particularly difficult if a crisis were to be triggered or exacerbated by offensive cyber operations under the command of a NATO ally or if such operation on the part of NATO were used as a pretext for crisis. Considering the potential escalatory nature of a more forward-leaning posture – within NATO and driven by its largest member, the United States – these questions should be urgently addressed.

42 Timo S. Koster, "Reinforcement of NATO forces and military mobility," Netherlands Atlantic Association, https://www.atlcom.nl/upload/trans-atlantisch-nieuws/AP_4_2018_Koster.pdf.

43 "EU leaders to seek cyber sanctions, press Asia for action -draft statements," *Reuters*, October 17, 2018, http://news.trust.org/item/20181017132641-zq1cy/.

44 With new technology developing at a rapid pace, ensuring that capabilities remain abreast of innovation poses a challenge. Operating at the speed of relevance entails accelerating the pace at which weapons systems, military organizations, and operational capacities can evolve to meet future threats.

45 Robin Emmott, "NATO cyber command to be fully operational in 2023."

46 Jens Stoltenberg, "Why cyber space matters as much to Nato as land, sea and air defence."

47 Ibid

48 Bruno Lété and Daiga Dege, "NATO Cybersecurity: A Roadmap to Resilience."

The views expressed in GMF publications and commentary are the views of the author alone.

About the Author

Sophie Arts is a program coordinator supporting The German Marshall Fund of the United States' (GMF) security and defense policy work in Washington DC.

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

1744 R Street NW
Washington, DC 20009
T 1 202 683 2650 | F 1 202 265 1662 | E info@gmfus.org
http://www.gmfus.org/