Policy Brief

April 2022

# NATO’s Role in Global Cyber Security

*Merle Maigre*

Malicious cyber activity has increased substantially over the past years, ranging from ransomware and espionage to politically motivated cyberattacks and sophisticated malware used in the war in Ukraine. NATO allies must remain on high alert.

The changed nature of military conflict changes the defensive mission of NATO, which faces capable opponents in cyberspace and raises the question of how to create accountability when a hostile state fails to observe globally agreed norms.

The set of action for NATO for the next five years evolves around how to impose costs and how to deny benefits against malicious actors in cyberspace.

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

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

## Introduction

What the war in Ukraine says about cyber power is yet not entirely cleared from the fog of war. Many aspects remain uncertain, but given the unpredictability of the Putin regime, the risk of an escalation in hostile cyber exchanges between Russia and NATO states remains high. What is clear is that, as of February 24, 2022, we live in a different world in which the European and global security orders have been shattered.

This brief first explores the challenge that cyber threats pose to NATO allies and how the rapidly evolving cyber-threat landscape can alter the international security environment. Secondly, it looks at developments in cyber defense policy within NATO. Finally, the brief analyzes how NATO needs to adapt to address cyber challenges, studying how allies align their sovereign interests, capabilities, and cyber doctrines with NATO operational requirements and strategic ambitions. NATO is set to issue strategic documents in 2022 that will guide the next decade of its military planning. This will certainly require more transatlantic consultation on political-military matters with an emphasis on cyber security and cyber defense.

## The Cyber Challenge to the World and NATO Allies

Malicious cyber activity has increased substantially over the past years while the world has kept turning amid the omnipresent pandemic and now war in Ukraine. States, non-state actors, and criminal groups compete and are increasingly weaponizing sensitive information and infiltrating other countries' networks to steal data, seed misinformation, or disrupt critical infrastructure.

The coronavirus pandemic further complicated the cyber-threat landscape. In March 2020, attempts to mitigate the spread of the coronavirus led to social distancing measures, travel restrictions, and remote work. In a short span of time, IT security professionals had to respond to the challenges of working from home, such as enterprise data movements when employees accessed cloud-based apps via their home internet, corporate software, videoconferencing, and file sharing.[1] Even if hardware and software solutions were in place to secure the organization's data, there were often no established policies to help employees wade through the jungle of threats and vulnerabilities they faced when moving their workplace out of the traditional office environment.[2]

According to the FireEye Mandiant Special Report: M-Trends 2021, the top five most targeted industries in 2020 were business and professional services, retail and hospitality, finance, healthcare, and high technology. The main methods used were extortion, ransom demands, payment card theft, and illicit transfers. Direct financial gain was the likely motive for 36% of intrusions, and an additional 2% of intrusions were likely perpetrated to resell access. In 2021, data theft remained an important mission objective for threat actors; in 32% of intrusions, adversaries stole data.[3]

Currently, highly organized, technically proficient criminal syndicates comprise the most significant cyber threat to allies. These groups try to steal data or extort money through ransomware. In 2021, prominent ransomware attacks struck Colonial Pipeline, the operator of the largest fuel pipeline on the East Coast of the United States; JBS, the largest meat processing company in North America; and Coop, a major supermarket chain in Sweden. Healthcare was also targeted—in May of the same year, the entire health service system of Ireland was disrupted for weeks, and over the spring and summer, dozens of hospitals in Europe and the United States were locked out of life-critical systems by ransomware attacks.[4]

Another set of threats comes in the form of belligerent state actors that seek to steal sensitive data for

Unless otherwise indicated, all links were last accessed on February 7, 2022.

[1] ENISA: European Union Agency for Cybersecurity, The Year in Review. ENISA Threat Landscape from January 2019 to April 2020, 2020.

[2] NATO Cooperative Cyber Defence Centre of Excellence, Recent Cyber Events: Considerations for Military and National Security Decision Makers, No. 10, May 2021.

[3] Fire Eye Mandiant Services, Special Report, M-Trends 2021, pp. 17-19.

[4] Ciaran Martin, "Cyber Criminals Will Cause Physical Harm," Wired, February 2, 2022.

espionage. In December 2020, Russian intelligence services infiltrated the digital systems run by US tech firm SolarWinds and inserted malware into its code. During the company's next software update, the virus was inadvertently spread to about 18,000 clients, including large corporations, the Pentagon, the State Department, Homeland Security, the Treasury, and other US government agencies. The hack went undetected for months before the victims discovered vast amounts of their data had been stolen.[5]

There are also politically motivated cyberattacks mandated by states that interfere in democratic processes and political discourse. In September 2020, the internal email system of Norway's parliament was hacked.[6] Ine Eriksen Søreide, the Minister of Foreign Affairs of Norway, underlined the significance of the attack by calling it an important cyber incident that affected the "most important democratic institution" of the country.[7] Norwegian authorities later identified Russia as the actor responsible for the attack, marking the first time that Norwegian authorities had made a political attribution to such an attack.

Since the beginning of this year, Ukraine's government has been hit by a series of cyberattacks that defaced government websites and wiped out the data on some government computers. In mid-January, hackers defaced about 70 Ukrainian websites, including the Ministries of Foreign Affairs, Defense, Energy, Education, and Science, as well as the State Emergency Service and the Ministry of Digital Transformation, whose e-governance portal gives the Ukrainian public digital access to dozens of government services. The hackers replaced the home pages of about a dozen sites with a threatening message: "be afraid and expect worse." After a couple of days, however, most of the sites were restored.[8] The international hacktivist collective Anonymous has declared "cyberwar" against Russia's government, claiming credit for several cyber incidents including distributed denial of service attacks that took down Russian government websites and Russia Today, the state-backed news service.[9]

*Around the globe, aging critical infrastructure has long been vulnerable to attack.*

The most worrying type of cyberattack is sophisticated malware designed by states or state-backed actors that act as "time bombs" in the critical cyber networks of target countries, such as the energy, telecom, and transportation sectors. Around the globe, aging critical infrastructure has long been vulnerable to attack. In 2020, the UK's National Cyber Security Centre issued a warning of Russian attacks on millions of routers, firewalls, and devices used by infrastructure operators and government agencies.[10]

On the day of the Russian invasion, ViaSat, a provider of high-speed satellite broadband services, was hacked along with one of its satellites Ka-Sat, whose users included Ukraine's armed forces, police, and intelligence service. Destructive wiper malware attacks by Russia against Ukraine included WhisperGate, discovered in January by Microsoft, in Ukraine's networks that "provide critical executive branch or emergency response functions";[11] HermeticWizard and IsaacWiper,[12] targeting multiple Ukrainian organizations just hours before the Russian invasion

[5] Jack Stubbs, Raphael Satter, and Joseph Menn, "US Homeland Security, thousands of businesses scramble after suspected Russian hack," December 14, 2020.

[6] Catalin Cimpanu, "Finland says hackers accessed MPs' email accounts," ZDNet, December 28, 2020.

[7] BBC, "Norway blames Russia for cyberattack on parliament," October 13, 2020.

[8] Kim Zetter, "What We Know and Don't Know about the Cyberattacks Against Ukraine," Substack, January 17, 2022.

[9] Monica Buchanan Pitrelli, "Global hacking group Anonymous launches 'cyber war' against Russia," CNBC, March 4, 2022.

[10] Alix Pressley, "The 'cumulative effect' of ransomware and the lessons for UK national infrastructure,“ Intelligent Cio, July 20, 2021.

[11] Microsoft Security, Destructive malware targeting Ukrainian organizations, January 15, 2022.

[12] ESET Research, IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine, March 1, 2022.

began; and CaddyWiper, spotted by researchers at the Slovak internet security company ESET in mid-March.[13] All of them were designed to wipe or overwrite critical files on infected systems and leave computer hard drives corrupted and unrecoverable. These incidents demonstrate that, in the words of cyber expert and Silverado Policy Accelerator think tank chairman Dmitri Alperovich, "Cyberattacks have become a theater for great-power conflict in which governments and militaries fight in the hybrid 'gray zone,' where the boundaries between peace and war are blurred."[14] The actors navigate a complex web of ambiguous and deeply interconnected challenges, where cyberattacks are not a separate front, but rather an extension of the conflict.

While they can offer some advantages in military operations, cyberattacks also have limitations in feasibility and effect. In the event of military attacks, military objectives can be supported by intelligence-gathering operations, operations aimed at disrupting the opponent's military, and psychological operations against the opponent's public.[15] Nevertheless, sophisticated cyberattacks require a lot of luck, but also skill and time—for example, the 75-minute power outage in 2016 in Kyiv took 31 months to prepare.[16]

The Russian military exercise Zapad 2021 in September included one of the largest uses of electronic warfare, which has been increasingly on display in eastern Ukraine since 2014 and in Syria since 2015. Roger McDermott, a leading analyst on Russian military developments has described that "Russia's growing technological advances in EW [electronic warfare] will allow its forces to jam, disrupt, and interfere with NATO communications, radar and other sensor systems, unmanned aerial vehicles, and other assets."[17] Russia sees EW as a seamless whole, ranging from kinetic combat operations on the battlefield to missions in cyberspace and the information domain.[18] While there were no public sources confirming any navigation or communications disruption by the Baltic-Polish defense leadership during Zapad 2021, it is nevertheless important that NATO continue to adapt to the evolving cyberthreat landscape.

## The Alliance's Achievements in Cyber So Far

Over the past fifteen years, NATO's approach to cyber issues has evolved from addressing cyber defense in primarily technical terms to viewing it as essential to the alliance's strategic context. The need to "strengthen capabilities and to defend against cyberattacks" was first acknowledged by allied leaders at their 2002 summit meetings in Prague.[19] However, after Estonia's digital infrastructure was hit by cyberattacks in 2007, NATO admitted that a confrontation between states might involve a cyber dimension, and at the Bucharest Summit in 2008 adopted its first cyber-defense policy. The 2008 conflict between Russia and Georgia demonstrated that cyberattacks have the potential to become a major component of conventional warfare.

In parallel, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was accredited as a NATO Centre of Excellence in 2008. Since then, it has grown into a strong, international knowledge hub for cyber defense, bringing together top cyber experts across fields—government, military, industry, and academia—from 29 nations for interdisciplinary research, training, and exercises in four focus areas: technology, strategy, operations, and law. The center connects a trusted community of like-minded states who wish to share information and expertise in

[13] ESET Research, CaddyWiper: New wiper malware discovered in Ukraine, March 15, 2022.

[14] Dmitri Alperovitch, "How Russia Has Turned Ukraine Into a Cyber-Battlefield," Foreign Affairs, January 28, 2022.

[15] Ibid.

[16] Ciaran Martin, "Cyber Realism in a Time of War," Lawfare, March 2, 2022.

[17] Roger McDermott, "Russia's Electronic Warfare Capabilities to 2025," ICDS, September 2017.

[18] Jonathan Marcus, "Zapad: What can we learn from Russia's latest military exercise?" BBC, September 20, 2017.

[19] NATO, Prague Summit Declaration, November 21, 2002.

cyber security. CCDCOE's best-known projects are Locked Shields, one of the world's largest and most comprehensive cyber-defense exercises; the annual cyber conference CyCon; and the Tallinn Manual, which looks at cyber operations within the context of international law. At the 2012 NATO summit in Chicago, allied leaders reaffirmed their commitment to improving the alliance's cyber defenses by bringing all of NATO's networks under centralized protection.

At the 2014 Wales summit, NATO recognized that international law applies in cyberspace and declared that, since the impact of a cyberattack could be as harmful to modern societies as a conventional attack, cyber defense is a part of NATO's collective defense mandate. Thus, NATO acknowledged that cyberspace is an operational domain for potential adversaries.

NATO's 2016 Warsaw summit resulted in a declaration recognizing that cyberspace has evolved into a separate domain of military operations, in which the alliance "must defend itself as effectively as it does in the air, on land, and at sea." The subsequent roadmap included the drafting of a NATO cyber operations doctrine, as well as the development of military cyber capabilities. In January 2020, the Allied Joint Doctrine for Cyberspace Operations was published "to plan, execute, and assess cyberspace operations in the context of allied joint operations."[20]

At the Warsaw summit, NATO heads of state and government signed a Cyber Defence Pledge, in which they outlined how nations protect their cyber networks. NATO developed detailed questionnaires and metrics related to the pledge and uses them to regularly report on how each nation delivers on its cyber commitments.

Allies also discussed how to strengthen the cyber component of NATO's Command Structure. The Command Structure is the military backbone of the alliance; it is what makes NATO unique. NATO has continuously adapted its Command Structure over the past decades to take account of a changing security environment. In February 2018, NATO defense ministers established the Cyberspace Operations Centre (CyOC) as part of NATO's SHAPE Command Structure, with the aim of integrating the allies' cyber capabilities into NATO military-operations planning.

> ***The "eyes and ears" of the respective commanders in cyberspace, CyOC aims at enhancing situational awareness in cyberspace and helping integrate cyber into NATO's planning and operations at all levels.***

CyOC is the first cyber-dedicated entity within the Command Structure. The "eyes and ears" of the respective commanders in cyberspace, CyOC aims at enhancing situational awareness in cyberspace and helping integrate cyber into NATO's planning and operations at all levels. While CyOC operates within the existing NATO frameworks, its main aim is to equip the Supreme Allied Commander Europe with any necessary tools to operate in cyberspace.[21] As CyOC moves toward initial then final operating capacity, it will be critical that it is staffed with sufficient—and sufficiently expert—personnel.[22]

During NATO's July 2018 summit, the allies affirmed, for the first time, their determination "to employ the full range of capabilities, including cyber, to deter, defend against, and counter the full spectrum of cyber threats," shifting away from securing cyberspace with defensive measures only. The "full range" of cyber capabilities means that both defensive and offensive capabilities can be deployed by NATO, in line with its defensive mandate and in accordance with international law. As NATO will not develop or acquire any offensive capabilities, it will rely, like in other operational domains, on the voluntary contributions of allies.

[20] NATO, Allied Joint Doctrine for Cyberspace Operations, January 2020.

[21] Wiesław Goździewicz, "Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)," Cyber Defense, November 11, 2019.

[22] NATO, NATO's Role in Cyberspace, February 19, 2019.

In late 2020, a team of experts appointed by NATO Secretary General Jens Stoltenberg and chaired by Thomas de Maiziere of Germany and Wes Mitchell of the United States gave their recommendations on how NATO could enhance its political role and better coordinate military tasks and political strategies among its members. In 2021, Stoltenberg's NATO 2030 included eight of those recommendations to guide the revision of NATO's Strategic Concept.[23]

*A key feature of the new [cyber defense] policy is the prominent role of offensive cyber operations.*

At the Brussels summit in 2021, the allies endorsed a new Comprehensive Cyber Defense Policy highlighting collaboration as necessary to strong cyber defense, which recognized that "the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.[24] A key feature of the new policy is the prominent role of offensive cyber operations.[25] In Brussels, member states committed to "employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats."[26] In other words, the alliance declared it could respond to malicious cyber activities below the threshold of use of force causing significant harm with, among other things, conventional military or offensive cyberspace operations.

NATO has committed to develop its next Strategic Concept for the 2022 summit. The alliance's current Strategic Concept dates back to the Lisbon summit in 2010. It is clearly out of date, having been conceived when terrorism and energy cut-offs were the major threats and the alliance's primary mission was to cultivate partnerships with non-member states rather than to face aggressive great-power rivals.

## Action Plan for the Next Five Years

To make NATO future-proof, it must be cyber-secure and operational. But is it doing enough to address the complex and evolving challenges of cyberspace? NATO's strategic challenge is to blend its successful conventional deterrence functions with a new strategy for cyber action. NATO's ability to send a collective message of resistance and to establish a credible threat response is its most valuable asset on the cyber-security front.

Four sets of actions for NATO are proposed. First, denying covertness by attribution: NATO should persuade opponents that they cannot be clandestine in their cyber actions. NATO and its members need to demonstrate that it is difficult or impossible to act covertly and be clear about attributing responsibility for cyberattacks.

Until recently, governments did not publicly release details on cyber incidents. But since 2018, public disclosures of cyberattacks by several Western powers indicate a new multinational policy of state transparency. The growing relevance of attribution is partially due to states becoming better at attributing cyber operations.[1] Greater public knowledge of cyberattacks heightens awareness of cyber conflicts and leads to greater public acceptance of cyber countermeasures.

Ultimately, what matters is that states engaging in unlawful actions using cyber means will face consequences. With attribution, policymakers show that they know what is happening in these networks and can investigate incidents. It also clearly spells out unacceptable behavior and can help create state practice. The best way to implement the international norms is by calling out behavior and having consequences when these norms are breached. Attribution will make clear to the malicious actor that their actions will be seen and addressed. It is the basis, under international law, for countermeasures and self-defense.

[23] Jamie Shea, "Getting NATO ready for the rest of the 21st century: Eight core ideas for 2030," Friends of Europe, April 2, 2021.

[24] NATO, Brussels Summit Communiqué, June 14, 2021.

[25] Erica D. Lonergan and Mark Montgomery, "Pressing Questions: Offensive Cyber Operations and NATO Strategy," Modern War Institute, January 25, 2022.

[26] NATO, Cyber Defence, March 23, 2022.

When should states publicly attribute cyberattacks? Effective public attribution requires a clear understanding of the attributed cyber operation and the cyber-threat actor, but also the broader geopolitical environment, allied positions and activities, and the legal context. The public attribution framework put forward by Max Smeets and Florian Egloff in March 2021[27] distinguishes four factors that act as enablers or constraints in public attribution. These factors are intelligence, incident severity, geopolitical context, and post-attribution actions. The combination of these four components enables consistent decision-making about whether to publicly disseminate information about an adversary's actions, privately tell the adversary, or restrict knowledge of the intrusion to the government and potentially other partners.

***Effective public attribution requires a clear understanding of the attributed cyber operation and the cyber-threat actor, but also the broader geopolitical environment, allied positions and activities, and the legal context.***

Collecting and processing intelligence—information about foreign countries and their agents—provides a technical basis for attribution. How could allies improve intelligence sharing to conduct more rapid attribution and enable a response to adversary cyber activity? During the Nordic-Baltic foreign ministers meeting in Tallinn in September 2020, a 90-minute tabletop exercise was organized[28] to test the ministers' ability to respond to and attribute an escalating cyberattack. They answered multiple-choice questions on communication of and possible diplomatic countermeasures to the attack. The ministers learned through first-hand experience that a timely exchange of technical intelligence can be key in attributing any cyberattack. "The shared view [of the countries involved]—especially when it comes to complicated issues—is crucial," said Urmas Reinsalu, Foreign Minister of Estonia.[29]

Attribution is only as good as the information that allies are willing to share. NATO's value can be in becoming the preferred platform for sharing cyber information. General Paul Nakasone, who heads US Cyber Command, told the House Armed Services subcommittee on intelligence that "in 35 years" he has never seen a better sharing of accurate, timely, and actionable intelligence than what has transpired with Ukraine.[30] Sharing information and intelligence with allies "builds coalitions" and can "shine a light on disinformation" campaigns, like the one Russia used to lay the groundwork for their invasion of Ukraine.

As the second course of action, NATO should use the current crisis to accelerate the progress with setting up NATO's own cyber command and sharpen allied responses to malicious cyber actions. Overall, this would give more credibility to its cyber defense. In February 2019, allies endorsed a set of tools to respond to cumulative cyber activities, but not much has happened to take it forward. It is now time to build upon this set and develop concrete steps at the political, military, and technical levels to model alliance behavior according to the threat landscape. This means a sharper focus on future responses to high- and low-end cyberattacks along with concrete deterrence actions and tools for individual sectors and target types. Much of this is based on the high-end cyber capabilities of select individual allies called "volunteer sovereign cyber effects," where cyber-capable nations deliver voluntarily offensive cyber effects on a target designated by an operational-level

[27] Florian Egloff and Max Smeets, "Publicly attributing cyber attacks: a framework," Journal of Strategic Studies, March 10, 2021.

[28] Ministry of Foreign Affairs of Estonia, Joint Statement from Nordic-Baltic (NB8) Foreign Ministers' annual meeting, September 9, 2020.

[29] Ministry of Foreign Affairs of Estonia, Nordic and Baltic foreign ministers discuss regional and global politics in Tallinn, September 9, 2020.

[30] House Subcommittee on Intelligence and Special Operations, "Defense Intelligence Posture to Support the Warfighters and Policy Makers," March 17, 2022.

commander. The NATO Cyber Command would be responsible for matching military needs with the willingness and capabilities of the nations potentially able to deliver such effects.[31] The alliance should clarify which allies are responsible for offensive cyber operations against certain targets and the information-sharing and notification requirements.

A good plan requires practice. The scenarios of cyber responses that are under the Article 5 threshold should be regularly practiced, and the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) Locked Shields exercise is a good way to do so. Organized since 2010, it enables cyber-security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus should be on realistic scenarios simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects. Locked Shields is a unique opportunity to encourage experimentation, training, and cooperation among allies in an authentic but safe training environment.

***NATO should also make more use of its Cyber Range, a platform for NATO exercises and training in Estonia operated by the Estonian Ministry of Defense.***

NATO should also make more use of its Cyber Range, a platform for NATO exercises and training in Estonia operated by the Estonian Ministry of Defense. The Cyber Range already facilitates NATO's flagship annual cyber defense exercise Cyber Coalition, and NATO CCDCOE has based Locked Shields on Cyber Range for over a decade. The versatility and computing power of the platform allows a different, complex scenario to be simulated every year for an increasing number of participants. The technical, red-teaming exercise CrossedSwords, organized by NATO CCDCOE, tests the capabilities and skills needed when executing a full-spectrum cyber operation in real life, focusing on experimentation with integrating kinetics and offensive cyber operations in the context of a modern battlefield.

More operational- and technical-level joint activities should be practiced among allies and with like-minded partners in order to contribute to imposing costs to malicious actors in cyberspace. Given that NATO's cyber response teams are stretched thin due to protecting NATO's own networks, bi- and multilateral collaboration enables countries to share best practices and, in the event of an emergency, provide mutual rapid assistance in crisis response.

The cyber exercise Baltic Ghost originated from a series of cyber defense workshops in 2013 and should be expanded to include all NATO battlegroups in the Baltics and Poland. Currently it is facilitated by the United States European Command with the objective to develop and sustain cyber partnerships between Estonia, Latvia, Lithuania on one end, and the Maryland, Michigan, and Pennsylvania Army National Guards on the other end. Building on the success of Baltic Ghost, regular cyber exercises should take place in multinational NATO battlegroups, led by the United Kingdom, Canada, Germany, and the United States, in Estonia, Latvia, Lithuania, and Poland. Future exercises should regularly support NATO enhanced forward presence forces and train participants to respond to aggression in a contested, degraded, and denied cyberspace environment.

The third action focuses on building resilience of domestic critical infrastructures. Doors are locked to keep homes safe. Likewise, all NATO member states should address their digital insecurity by locking digital doors as individuals, companies, and countries. The strategic vulnerability to disruption and sabotage lies not so much in the military space but in the hospital booking system, logistics schedule, power grid, and thousands of other mainstream, civilian, mostly privately owned networks. Based on the 2016 Cyber Defence Pledge, in which member states committed to improving their ability to protect their cyber networks,

[31] Goździewicz, "Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)."

the alliance could formulate a NATO cyber-security baseline with concrete resilience goals to achieve or maintain the baseline. These resilience goals could then be apportioned among member states in the same way as the defense-planning capability targets.

This should come with obvious financial and investment implications. Public debates on burden sharing within NATO for too long have focused on how much member states spend on defense in isolation, without adequate prioritizing where those funds are going. Member states should be rethink defense spending relative to emerging threats and collective security challenges. To ensure funding for cyber security is appropriately prioritized, NATO should strengthen a commitment to digital defense spending, building on the strong base it has developed in terms of doctrine, standards, and requirements.

This also includes strengthening the political resilience of member states by broadening NATO consultations to include more areas of government. Regular North Atlantic Council-format meetings among member state directors of cyber authorities at the political and military levels would help build consensus on cyber policy issues.

Another course of action for NATO in cyber security is to increase its cyber capacity-building efforts for partner countries of strategic importance, reinforcing NATO's commitment to partners and projecting stability in NATO's neighborhood. This kind of cyber capacity-building could include various types of support, ranging from strategic advice and cyber institution-building in defense sectors to education and training or advice and assistance in cyber defense. The objective should to be to enable capacity-building activities for military actors, along with the provision of training, equipment, and infrastructure for security purposes. This would allow NATO to improve the capacities of partners to address crises, prevent conflicts, and cater for their own security and stability by themselves, to the benefit of their population.

As one example, NATO could fill a gap in capacity-building for partner countries by bringing together military Computer Emergency Response Teams (CERTs) to share information on incident management dynamics, a key factor in modern cyber defense. While partner countries can receive support from donors in establishing mechanisms and processes to exchange information between civilian CERTs, such cooperation and communication channels are much less developed in the military domain due in large part to the high sensitivity of the information. There is a need to extend the information-sharing practices used in civilian circles to partner countries' military CERTs. Building cyber-security capacity should focus on partners' ability to respond to and recover from cyber incidents.

> ***There is a technical aspect to hardening defenses and building redundancy in data and services, but the core of resilience lies in leadership that does not ignore the problem.***

In sum, most future conflicts will have cyber components that require a technical, political, and diplomatic response. Whether the adversary is a state's elite unit or a criminal group rendering ransomware as a service, cyber security is about risk management and solid, pragmatic defense and response measures to improve the security of the digital environment. There is a technical aspect to hardening defenses and building redundancy in data and services, but the core of resilience lies in leadership that does not ignore the problem. How our national cyber-security strategies are translated into policies and procedures needs to be understood by all stakeholders. It is now up to the alliance's member states to provide clarity and coherence to successfully draft a new Strategic Concept that includes defense and deterrence. But this is not a job for NATO alone—it requires close coordination across national governments and the private sector, and NATO and the European Union must therefore continue to work very closely on this vital issue.

April 2022

### About the Author

Merle Maigre is the senior cybersecurity expert at e-Governance Academy in Estonia. In 2017–2018, she served as director of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) in Tallinn; in 2012–2017 as the security policy adviser to Estonian Presidents Kersti Kaljulaid and Thoomas Hendrik Ilves; and in 2010–2012 in the Policy Planning Unit of the Private Office of NATO Security General Anders Fogh Rasmussen. She is a member of the Executive Board of the Cyber Peace Institute in Geneva and the International Advisory Board of NATO CCDCOE.

### Acknowledgments

This brief is part of a project at the German Marshall Fund of the United States supported by the Norwegian Ministry of Foreign Affairs.

### About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

G | M | F

Ankara • Belgrade • Berlin • Brussels • Bucharest
Paris • Warsaw • Washington, DC

www.gmfus.org