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

Policy Brief

2017 | No. 23

NATO Cybersecurity: A Roadmap to Resilience

By Bruno Lété and Daiga Dege

Cybersecurity has become as crucial as conventional security, thereby shifting the realm of the security environment. Rogue actors have boosted their capabilities, and the costs of such resources owned by attackers are threatening security on both sides of the Atlantic. NATO must put forward recommendations and implement the securitization agenda in order to create an interconnected approach within different sectors.

NATO will need to continue building the force-multiplying functions of its cyber capabilities, improve effective command and decision-making structures in cyber crisis and conflicts, and enhance the interoperability between allies and partners in cyberspace. The security challenges of today require quick responses, necessitating flexible policy frameworks that allow for coercive reactions from networked actors.

Today the digitalization of crisis and conflict is a fact. Hacks, malware, and fake news are increasingly taking the place of planes, bombs, and missiles. Cyberspace empowers adversaries from across the globe to challenge our security with a mouse-click. Worldwide criminal cyber-attacks such as the WannaCry ransomware, the aggressive use of social media by Daesh to lure people into terrorism, or the alleged role of Russia to spread fake news and sew confusion in our transatlantic societies are just a taste of more to come.

For NATO, it means that the Alliance is faced with an evolving complex threat environment. State and non-state actors can use cyber-attacks in the context of military operations. In recent events, cyber-attacks, leaks, and espionage have also been part of hybrid warfare. Cybersecurity incidents can have geopolitical implications and potentially pose threats to the safety, security, and economic well-being of the Alliance as a whole. The critical question NATO is facing now is how to protect itself and its member states against hostile cyber power.

Preparing NATO for Cyber-Attacks

Cybersecurity has long been part of Alliance calculus but only recently came at earnest to the forefront of its agenda. The 2007 cyber-attacks in Estonia forced NATO to think more seriously about this type of threat, and in 2008 NATO developed its very first policy on cyber defense. The cyber-attacks fuelling the crisis in Ukraine's Crimea and Donbass regions served as a definitive wake-up call. At its 2014 Wales Summit,

NATO effectively created a mind-set of urgency, featuring cybersecurity prominently on top of the meeting's political agenda. Allies endorsed a new cyber defense policy in Wales and approved a new action plan in line with the evolving cyber threat. Thinking more creatively about the implementation of collective security in the digital context on top of the agenda for NATO.

NATO made more significant steps in cybersecurity at the 2016 Summit in Poland. In Warsaw, Allies decided to operationalize cyberspace as a domain of NATO defense policy and planning efforts, in addition to land, sea, and air. An important product of the Warsaw Summit was the so-called NATO Cyber Defense Pledge through which member states committed to prioritize the strengthening the cyber defense of national networks and infrastructures. Most member states have created national cyber defense strategies, or are reviewing their existing ones.

The concrete result of these policy shifts is a growing number of workshops, trainings, and exercises to boost the experience, resilience, and capabilities of Allies in cyberspace. A remarkable effort in this light is exercise Locked Shields, the world's largest and most advanced international technical live-fire cyber defense exercise, which is hosted annually by the NATO Cooperative Cyber Defense Center of Excellence (CCDCoE) in Tallinn, Estonia. Locked Shields challenges cybersecurity experts from NATO member states, partner countries, and industry with scenario-based, real-time cyber-attacks enabling the participants to practice defending information technology networks and systems. Cyber and hybrid warfare crisis scenarios are now also being integrated in NATO's annual Crisis Management Exercise (CMX), where Alliance civilian and military personnel test the procedures of decision-making and consultation through realistic mock Article 4 and Article 5 scenarios. These and other exercises like the annual Cyber Coalition Exercise are now an integral part of building NATO's defensive cyber capabilities.

As part of the NATO–EU Joint Declaration at the Warsaw Summit, NATO is also pressing ahead to boost its cooperation on cyber defense with the European Union as both share an interest in becoming more resilient. NATO and the EU signed a Technical Arrangement on Cyber Defense in February 2016 to strengthen cooperation, communication, and information sharing between NATO's Computer Incident Response Capability and the EU's Computer Emergency Response Team. The EU has also become a regular observer of NATO cyber defense exercises.

NATO also increasingly recognizes the importance of working with industry partners to enable the Alliance to achieve its cyber defense policy objectives. A significant effort — the NATO Industry Cyber Partnership — was launched in September 2014 as a signal that NATO and industry must work more closely together in sharing information, experience, and expertise to counter cyber threats.

Keeping Pace with an Evolving Threat

Today NATO faces ongoing efforts from antagonists, including non-state actors, to intimidate and destabilize member states through cyber-attacks. The notion of cyber warfare is not new, but the scale, speed, and intensity of the challenge demands a new approach toward the preparation, deterence, and defense against these threats. One important innovation that cyber activities provide an adversary is ambiguity, both of intent and attribution. The source of cyber aggression is not easy to identify and requires advanced technological capabilities that only a few member states in NATO possess. Cyber aggression is even more difficult to prove publicly because laws and regulations in cyberspace are still incomplete. For NATO, the ambiguity of cyber campaigns present challenges vis-à-vis action that needs to be collectively addressed across the political, military, civilian, and technological spectrum. The following recommendations are designed to strengthen NATO resilience in cyberspace.

More Tools to Coordinate National Efforts

The core of NATO cybersecurity efforts lie at the member-state level. NATO is responsible for protecting its own institutional information and communication systems, but it has little say in coordinating how member states develop their

national cyber defense capabilities. Despite having signed the Cyber Defense Pledge at the Warsaw NATO Summit, many member states still struggle to implement and evaluate their national cyber-security plans. As a result NATO's efforts at developing uniform, alliance-wide cybersecurity are undermined by significant inconsistencies across the national level of the member states and NATO's collective security and deterrence in cyberspace still show serious vulnerabilities against the backdrop of a growing number of attacks.

For NATO to operationalize cyberspace as a domain of NATO defense policy and planning — as was agreed at the NATO Warsaw Summit — the Alliance should have authorizations from member states to do more than just provide advice, expertise, training, or education. Similar to how NATO coordinates Allied military forces in the conventional domain, NATO could also be asked to evaluate how member states can develop, synergize, and complement their mutual national cyber defenses. At a minimum, NATO should develop standards and better indicators that allow a standardized measurement of a nation's annual progress — and should be tasked with testing and measuring members' capabilities annually. To achieve this objective, a strong cooperation with the European Union is essential. NATO and the EU could work together to design minimum cybersecurity requirements and benchmarks that would also be adopted by the European Defense Agency.

Rapid Assessment and Decision-Making Tools

The scale, speed, and intensity of today's cyber-attacks demand a new approach to respond at the political, military, and civilian level. To develop a rapid decision-making process when facing a cyber-attack NATO can take a few effective measures across its organization. First, more resources must be allocated to accurately and quickly detect and define hostile cyber actions. Further work on indications, warnings, and situational awareness is critical. In this context, NATO's various civil and military intelligence units, inter alia, could have a useful role. In addition, the Supreme Allied Commander Europe (SACEUR) could be granted more powers by the North Atlantic Council in authorizing some of the preparatory procedures. At the same time, NATO headquarters should increase the number of exercises that test rapid decisions-making procedures in complex and demanding cyber crisis-conflict scenarios.

Much can also be done at the member-state level. Allies and willing partners should continue to work on improving and updating threat assessments, and facilitating closer intelligence cooperation. In this light, Allies should identify information sharing as a clear requirement and task.

NATO could also intensify its interaction with national intelligence services and establish supply chain management partnerships with national industries. Cyber threats come in the form of networks and it takes a similarly well-organized network of international and cross-sector cooperation to defeat those threats.

Common Rules of Engagement

NATO has not commonly defined the circumstances, conditions, degree, and manner in which the use of force may apply if one of its member states suffers a cyber-attack. Triggering the authorization to use force in the context of Article 5 may be more obvious if a member state faces a large-scale, devastating cyber-attack where the source of the attack can be clearly attributed. But the need is much more urgent to define when and how NATO must respond against the day-to-day cyber intrusions that fall below the threshold of being perceived as a clear act of aggression. NATO policy still allows for too many gray zones that are being exploited by adversaries who are clever enough not to cross a line that would trigger a common response from the Alliance. Cybersecurity incidents like the alleged Russian hack of the Democratic National Committee's emails show that the United States and the NATO Allies are still unclear about the conditions and manner to respond in cyberspace. The *Tallinn Manual* published by the NATO CCDCoE offers a set of guidelines on how states can define rules of engagement, countermeasures, retaliation operations, and other forms of response within the context of the international law if they are to face an act of cyber aggression. But NATO is still far removed from having adopted a common view

and interpretation on the subject. The North Atlantic Council would still need to asses each individual cyber-attack case by case without the support of standard measurement tools and indicators that can help NATO formulate a proportionate political or military response. As more cyber policies and laws are taking shape, NATO could demonstrate political, military, and intellectual leadership by clearly defining rules of engagement in cyberspace.

Consider Offensive Cybersecurity

NATO now recognizes a serious cyber-attack as a potential Article 5 trigger. But the doctrine and crisis management conditions enshrined in NATO's cyber policy puts the emphasis on a defensive posture only. As such, the Alliance fails to recognize cyber as a force multiplier that could be of importance to the defense of NATO nations. Russia for instance considers offensive cyber capabilities to be an integral part of its military power and especially as a way to make up for its relative lack of conventional forces compared to NATO. The rise in connectivity, smartphone proliferation, cloud computing, growth of application development, and other technological advances open new avenues to attackers and force defenders to cover an ever-increasing number of fields. In the long run, NATO's defensive approach is not sustainable. It is time for NATO to start a debate on offensive cybersecurity and map the feasibility of coordinating counter strikes, and to establish a significant offensive cyber capability. NATO could center this debate on projecting offensive cyber warfare capabilities as a means of deterrence, similar to the perceived value of nuclear weapons to deter attacks against NATO.

Offensive security will allow the Alliance to better control the virtual battlefield. There are valuable cyber capabilities worth attaining, including the ability to conduct reconnaissance and surveillance, intercept communications, or deny resources and access. NATO may find increasing support to have a conversation on offensive cyber security with its allies. As member states are increasingly preoccupied with defense and deterrence issues in cyber-space they will show more receptivity to cooperation with NATO on developing centralized offensive cyber capabilities.

NATO and Cyber Industry Cooperation

Cybersecurity is largely market-driven. Government intelligence capabilities increasingly find it hard to keep up with the requirements for combating the surge in cyber threats. NATO should play a crucial role in facilitating contacts between those member states that seek stronger links with the private sector and encourage the role that industry can play in cyber threat deterrence and intelligence sharing. Flagship initiatives, such as the NATO Industry Cyber Partnership, are important steps in that direction but there is still a need to build more access and trust between NATO governments and industry. Educating member states and partner nations about the role of the private sector in cybersecurity is key. To make the partnership with the industry more effective NATO could play a more important role in mapping and evaluating what kind of cyber defense technologies and intelligence gathering methods the private sector offers, share lessons learned with the member states and encourage capitals to integrate the best practices into capabilities, policy, and implementation planning. NATO can also play an essential role in improving communications and information sharing between the private and the public sectors. More can be done at the NATO level to identify what kind of information between governments and companies can or cannot be shared, to develop standardized methods and formats for information sharing, and to encourage the use of automated platform capabilities to share this information quickly.

Build a Robust Public Diplomacy Campaign

The first frontier of cyber defense is the individual. Citizens who are digitally empowered, cyber aware, and cyber educated will display a more responsible behavior and automatically increase NATO's collective security in cyberspace. NATO needs a narrative on why cybersecurity matters beyond public belief that a major cyber-attack is improbable. What can NATO do in cyberspace that national security agencies cannot do? Which level of cybersecurity is needed rather than which one we can afford? NATO societies should be exposed to debate through parliaments, media, nongovernmental organizations, and academia. Externally, the Alliance must adapt to the

reality that countries hostile to NATO will continue to use their own cyber capabilities and massive state propaganda organizations to attack NATO systems and discredit everything the Alliance does. NATO has to be able to engage in and win this information war at the elite decision-maker and opinion-former levels rather than simply raise awareness of its existence and activities among a global public.

Conclusion

As NATO faces the implications of the digital age it cannot afford to be complacent and hope for the best. The Alliance will now be tested, and in this respect still finds itself in a less than optimal position to deal with the sudden shifts cyberspace has brought to the security environment. NATO must assert its credibility in cyberspace as a strong, even formidable, power in the eyes of its members and partners — and antagonists. To achieve this result, NATO will need to continue to improve the force-multiplying functions of its cyber capabilities, to improve effective command and decision-making structures in cyber crisis and conflicts, and enhance the interoperability between allies and partners in cyberspace. The security challenges of today require quick responses, necessitating flexible policy frameworks in which coercive reactions can be decided upon among networked actors. The future NATO Summits must continue to adapt the Alliance in a world that evolves toward a new digital order.

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

About the Authors

Bruno Lété is a senior fellow for security and defense policy in GMF's Brussels office. Daiga Dege is a trainee in GMF's Brussels office.

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/