Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Supersize Cyber

by Safa Shahwan Edwards, William Loomis, and Simon Handler

NATO should adopt a digital .2 percent policy whereby member states commit to spend .2 percent of their gross domestic product on cybersecurity and digital defense modernization.

Supersize Cyber

NATO should adopt a digital .2 percent policy, whereby member states commit to spend .2 percent of their gross domestic product (GDP) on cybersecurity and digital defense modernization, evoking the existing two percent guideline utilized by the Alliance for traditional defense expenditures. While some NATO members are awash in cybersecurity capabilities, others are not, preventing the Alliance as a whole from most effectively addressing adversaries increasingly focused on digital and information-centered threats. Cyber defense, collective response, adequate protection of current and future weapon systems, digital integration, leveling up Joint Intelligence, Surveillance, and Reconnaissance (JISR)—the debates about burden sharing are missing critical dimensions of digital transformation. NATO is grappling with how to navigate and operate in cyberspace and must follow strategy with resources.

Since its establishment, NATO's mission has been to protect its members through political and military means. How member states finance the Alliance's efforts has remained contentious, but traditionally, funding has focused on weapons and hardware. Public debates on burden sharing within NATO for too long have focused on how much member states spend on defense in isolation, without adequate prioritization of where those funds are going. Thus, the debate over the two percent guideline already threatens to pigeonhole cybersecurity, "cybered" weapons, and command and control systems under the "research and development" category, leaving them at risk of being cannibalized in favor of traditional defense acquisitions. Member states should be reimagining how to spend on defense, and where that spending is relative to emerging threats and collective security challenges. To ensure funding for cybersecurity is appropriately prioritized, NATO should adopt a .2 percent commitment to digital defense spending, building on the strong base it has developed in terms of doctrine, standards, and requirements.

A modern force, like an innovative technology company, must be able to harness, store, secure, analyze, and share vast amounts of data from anywhere on demand. Relative speed has always been a warfighting necessity, and the adaptation of commercial cloud services—the backbone of digital transformation—is critical to equipping forces with data to make quick, informed, and coordinated decisions. But digital transformation does not come cheap. For example, take the US Department of Defense's Joint Enterprise Defense Infrastructure (JEDI) project—the price tag for commercially-built cloud services is as much as $10 billion. Smaller-scale examples of critical investment in digital transformation across NATO include the British Ministry of Defence's £17.75-million contract for Microsoft's Azure private cloud services. Proportional investment is required across the Alliance to transform how forces interact amongst themselves and in turn interoperate more effectively with allies.

The proposed .2 percent target would increase by two to three times the amount most NATO member states spend on cybersecurity and offensive and defense cyber capabilities—providing the capital base for long-term investment, training, and workforce expansion to meet operational demands. This approximates to 15-20 percent of many countries' defense budgets. Considering just how frequent the use of digital networks and technology are across all aspects of the defense mission, and the need to consider the cost of IT modernization as well across the defense enterprise in each state, this .2 percent target falls right in line with an aggressive yet purposeful strategy.

As governments, militaries, and adversaries increasingly rely on cyberspace and digital tools, a reexamination of priorities and funding benchmarks is needed. The .2 percent target will enable NATO to best position itself for the digital future of conflict and warfare. Forgoing such a mandate would be a missed opportunity as member states' appreciation for cyber defense and digital capacity is increasing, and this move would complement NATO's nascent cyber doctrine and Cyber Defence Pledge. This new initiative also has the flexibility to be championed both by NATO leadership through the NATO Defence Planning Process (DPP),

An allied soldier relies on multiple sophisticated technology systems, all requiring cyber defense, during a military exercise (Source: NATO Allied Command Transformation)

which establishes spending priorities for member states, *and* outside of the Alliance structure through a public commitment by member states to invest in cyber capabilities.

Where current defense planning goals for cybersecurity and digital transformation are qualitative requirements, an aggressive quantitative target will make considerably more possible. NATO's digital transformation requirements could be broadened and enhanced to complement national efforts on cyber capabilities and know-how. For instance, NATO could be aggressive about pooling knowledge, research, intelligence, and personnel at the NATO Communications and Information Agency (NCIA), Alliance Command Transformation, and the NATO Collaboration Support Office. In doing so, NATO could serve as a force multiplier for aggressive national investments in cybersecurity and digital defense modernization.

Perhaps most importantly, this mandate is unlikely to be hijacked, spearheaded, or politicized by any one member state, like we have seen with burden sharing, but would exemplify NATO committing itself as an organization to maintaining relevance and value for years to come. Increasingly, public-facing materials from Brussels emphasize the importance of cyber defense in the face of evolving and increasingly complex cyberattacks and member states' reliance on technology. No one member state is telling NATO to do this—in fact, NATO is telling NATO to do this.

The .2 percent should be spent in three distinct areas—enabling offensive capabilities on the battlefield as "cybered" war becomes the norm, defending digital systems from laptops to combat aircraft, and transforming the information technology infrastructure of the Alliance and its members' defense organizations to meet evolving demands.

First, enabling offensive capabilities on the battlefield. NATO has made it clear that its cyber priorities are to "protect its own networks (including operations and missions) and enhance resilience across the Alliance." This has manifested itself mostly as enforcing best practices for basic cybersecurity, developing consensus on collective defense in cyberspace, and creating an offensive cyber framework. NATO must evolve this focus and invest in playbooks that integrate cyber with traditional capabilities, and top-level training on how to utilize them.

To achieve this, NATO must invest in "cybered" operations. "Cybered" conflict is any conflict of national

significance in which success or failure for major participants is critically dependent on digitized key activities along the path of events. One of the biggest challenges when it comes to integrating these types of capabilities is trust. When NATO agreed in 2018 to integrate allied cyber capabilities into Alliance operations, it laid a foundation for building trust and shared ties that will help alleviate this challenge. The long-term trajectory for the use of these capabilities is not for them to be shared across national armies but coordinated closely and communicated through joint exercises and regular operational collaboration.

NATO must strategically shift resources to directly address emerging threats—and that means more than traditional cybersecurity. The Alliance must work to develop doctrine, training modules, operating concepts, and technical capabilities to conduct "cybered" operations to achieve its strategic goals. With Russia continuously demonstrating its expansionist agenda, leveraging hybrid capabilities, pushing boundaries, and accusing the Alliance of aggression, NATO must be able to respond to hybrid threats with hybrid solutions. China's increasingly assertive foreign policy and long history of digital foreign adventurism pose a challenge as well.

Second, NATO must more aggressively invest in the defense of its digital systems. The Alliance is already engaged in a pitched battle across cyberspace to defend devices and networks from regular intrusion. Without adequate resourcing of the defense of these systems, no member state can have confidence in their utility in a fight. Where there is an emerging role for cyber capabilities to complement and enable traditional kinetic systems on offense, there is an overwhelming need today for defense. Resourcing this fight requires nations to commit to supporting the hiring of personnel, new technology acquisitions, and cost-intensive interoperability, including operational information sharing, joint exercises and incident response, and standardized security tools and practices.

Finally, NATO and its members must invest in digital transformation. NCIA has endorsed digital transformation—the concept of unlocking digital potential across its thirty member states—to maintain the Alliance's relevance for decades to come. However, in order for NATO to meet the challenges associated with modern adversary capabilities, member states must be not only willing to appreciate, but sufficiently fund, digital transformation.

The ability of NATO forces to best leverage data to constantly learn and improve security requires new approaches and investments in people, processes, and technologies. Preliminary investments in establishing technical teams and best practices to constantly evolve to adapt to the shifting threat landscape can contribute to long-term savings, freeing up funding for other security challenges. For example, by investing in new software development processes like DevSecOps—the practice of incorporating the development, security, and operations teams as integral components throughout the course of a continuous development cycle, rather than integrating security at the end—defense organizations can leverage data to become more efficient, secure, and responsive to operational requirements, while saving time and money in the long run.

The .2 percent commitment is a means of driving member states to help the Alliance make long-term commitments and prepare for a future cyber-enabled war and conflict by establishing a digital bedrock comprised of personnel networks and innovative capacity to maintain an upper hand in offense and defense. Programs like the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn are exemplars of the kind of investments that can yield long-term advantages if properly nurtured. Expanding the Locked Shields exercise to include real-world military units and battalion-size maneuver units will bring together technical security measures and real-world capabilities in line with the threats of contemporary battlefields.

Raising the debate over a digital .2 percent would help keep NATO valuable and relevant for the next decades of conflict. Soldiers deployed today haul cell phones and laptops, and headquarters relies on high-bandwidth connections to subordinate units, orbiting drones, and higher-echelon intelligence and command and control organizations. The modern battlefield is awash in connectivity and computing power which stitch together frontline units, support organizations, and central military administration in a single digital web. Taking advantage of these capabilities such

that they enhance NATO's lethality, maneuverability, and capacity in the decades to come requires member states to publicly commit themselves to spending targets on cybersecurity.

Mitigating emerging digital risks requires resources and long-term investment. The modern battlefield environment compresses front line and rear area; requires a combination of civilian, diplomatic, and military capabilities; and demands continued evolution of the means and modalities of collective defense. NATO can prepare itself for the conflicts of today while investing for those of tomorrow, but to do so requires public certainty of the willingness to engage in burden sharing and a collective commitment to positive evolution in the face of stagnation. The digital .2 percent commitment offers such a visible pledge and anchors states to a meaningful contribution toward continual modernization.

Safa Shahwan Edwards is the associate director in the Cyber Statecraft Initiative in the Atlantic Council's Scowcroft Center for Strategy and Security.

William Loomis is the program assistant in the Cyber Statecraft Initiative.

Simon Handler is the assistant director in the Cyber Statecraft Initiative.