Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Digitalize the Enterprise

by Jeffrey Reynolds and Jeffrey Lightfoot

If NATO is to unlock new frontiers of innovation and harness emerging technology, digitalizing how it does business is the key.

Digitalize the Enterprise

NATO is party to the turbulent birth of a new era, one that began when the use of computer power, algorithm sophistication, and very large data sets converged to make digital technology the defining feature of the coming decade. It affects almost every aspect of human endeavor, and it underpins the future of warfare and non-military competition among state and non-state actors vying for influence, markets, and power. For NATO to carry out its enduring mission to protect the populations, territories, and forces of allied states, it must reconcile conventional diplomatic and military power with data as a strategic capability. It needs a strategy for digitalization to compete and win the conflicts of tomorrow.

NATO's Science and Technology Organization defines seven emerging disruptive technology areas with the most potential to increase the Alliance's operational and organizational effectiveness from now through 2040: artificial intelligence, autonomy, quantum technology, space technology, hypersonic technology, biotechnology and human enhancement, and novel materials and manufacturing.[1] Proficiency in *all* of them is critical for NATO's ability to conduct tomorrow's multi-domain operations, but it cannot expect to achieve strategic advantage in *any* unless it takes the intermediary step of digitalization. If the seven emerging disruptive technology areas are the locks to sustaining NATO's strategic advantage, then digitalization is the key to all of them.

Why Digitalization Matters for NATO

Digitalization can bolster NATO's ability to gather and process information, take decisions, and automate routinized processes. The scope expansion inherent to digitalization enables NATO to consolidate data inputs across a range of sectors for better situational awareness, even in areas beyond its traditional regional and functional expertise. This makes decision making the primary beneficiary of digitalization. The Alliance has clear decision making and command structures with established lines of authority and well-defined processes. Each stage of NATO's decision-making processes can be enhanced because digitalization enables the Alliance to reinforce its deterrence and defense posture *and* improve in areas of importance in the digital age: defeating both opportunistic and coordinated *disinformatziya* campaigns, predicting strategic shocks, leveraging the Internet of Things phenomenon, enhancing secure communications, and enabling sensitive information to "hide in plain sight" on the Web.

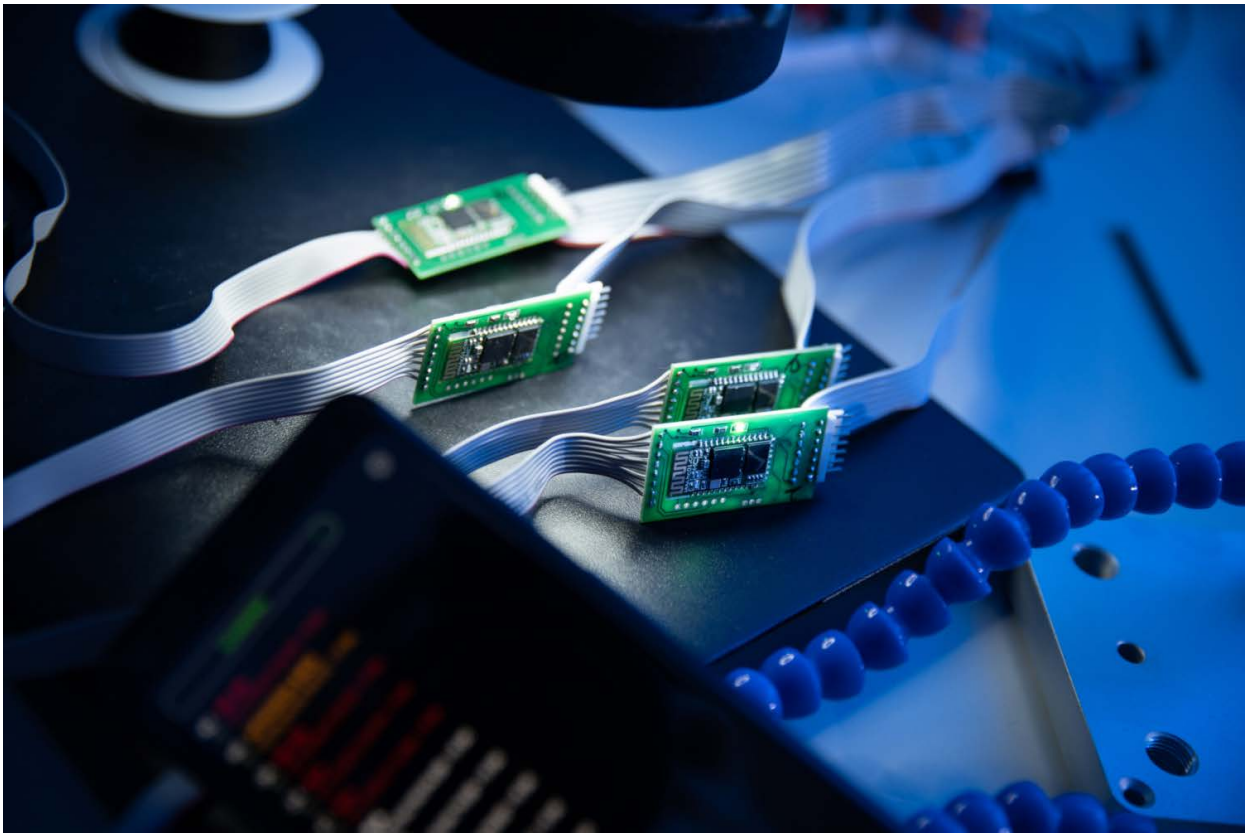
People are in the decision-making loop; they are central to every decision made by the Alliance. But automation—a core benefit of digitalization—may raise some eyebrows because it can be perceived as removing humans in decision making. This is a misconception. Digitalization does not reduce human decision-making power in NATO, it *reinforces* it. In effect, failure to digitalize *reduces* NATO's decision-making ability by having a diminished understanding of its strategic context, limited tools to respond, and antiquated processes when inevitable crises emerge.

Sustaining and Disruptive Digitalization in NATO

A digitalization strategy is the alignment of mundane efforts across the enterprise to electrify, automate, and move human labor beyond the critical path of routine administration in order to achieve tremendous gains in the speed, scale, and scope of operations.[2] Firms like Siemens and Airbus provide useful models of what digitalization looks like for large multinational organizations that excel in traditional industries, while seizing the opportunities that digitalization provides. As a point of departure, NATO should do what it does best and focus efforts in areas that create a "digital

1 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040: Exploring the S&T Edge*, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

2 Marco Iansiti and Karim R. Lakhani, Competing in the Age of AI: Strategy and Leadership When Algorithms and Networks Run the World (Boston: Harvard Business Review Press, 2020).



Source: adalidda.com

backbone" upon which to develop even greater capabilities: command and control (C2); intelligence, surveillance, and reconnaissance (ISR); equipment maintenance optimization and prognostic/predictive diagnostics; business process automation; and supply chain management. This is sustaining digitalization—standard fare for the Alliance because if there is a single area of undisputed dominance for NATO, it is its ability to do the "muck work" of leveraging the expertise of allies, executing programs, creating processes, and applying best practices in the development of capabilities.

Here, good work is underway. Allies are developing a common understanding of NATO's potential adversaries and the strategic context in which the Alliance must engage them. NATO Headquarters, Allied Commands Operations and Transformation, and the NATO Communications and Information Agency are developing digital capabilities, deepening relationships with innovation communities, and improving acquisition processes with an eye to the future. NATO is updating its organizational structure, aligning critical conceptual pieces, and thinking about the role of digital technology in a changing security landscape.

But beyond incremental adaptation lies the true promise of digitalization—and the peril of losing the next conflict by failing to act today. This is disruptive digitalization. For NATO to move to this more ambitious phase, a coalition of allies who are digital pioneers will need to drive this agenda forward. Disruptive digitalization assumes that NATO can increase its strategic advantage over potential adversaries by championing creative thinking and new technology over legacy capabilities and traditional ways of doing business.[3] Let's call them "game changers."[4] Here are five of them:

GAME CHANGER 1. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING (AI/ML): Of the emerging disruptive technology areas, AI deserves special mention

3 The idea of "sustaining" versus "disruptive" innovation comes from the work of Gautam Mukunda. Gautam Mukunda, "We Cannot Go On: Disruptive Innovation and the First World War Royal Navy," *Security Studies* (2010), 19 (1).

4 The authors would like to thank Richard Shultz, director of the International Security Studies Program at the Fletcher School, Tufts University, for the layout of the article. Inspired by "Showstoppers: Nine Reasons Why We Never Sent Our Special Operations Forces after al Qaeda Before 9/11," Weekly Standard, January 26, 2004.

because of its (yet unrealized) potential to expand human insight beyond natural limits. Navigating crises of the future *without* AI/ML capability is tantamount to asking diplomats and soldiers to fight battles dumb, deaf, and blind. AI/ML can help harness the data tsunami that floods current data processing capability to present an elegant and exhaustive operational picture. It can dramatically increase the realism and intensity of training programs though virtual war games and tabletop exercises so that political and military staff across the Alliance can improve decision-making and consensus-building abilities from constant practice and familiarization. Crucially, AI/ML can help NATO gain insight into the attitudes, intentions, and behaviors of potential adversaries—particularly their history, cultural practices, and psychology of their leadership—with a richness unavailable to leaders of the Alliance today.

GAME CHANGER 2. DATA FACTORY: In light of weaponized information directed at NATO and within allies, the Alliance needs to redesign its structures to maximize the utility of data as both a source of information and a weapon. A digitalized NATO requires a data factory consisting of robust data pipelines, training data, algorithm development centers, and associated workflows and storage facilities that work together seamlessly across the Alliance. Storing, sharing, and processing huge quantities of data on the front lines in real time requires an enterprise-wide approach that connects securely to the open Internet on trusted 5G networks. A data factory becomes a strategic capability for the Alliance in part because it makes NATO an information supplier instead of a consumer for allies and partners alike, thereby reinforcing its utility as a critical hub for international security. But a data factory requires a beefed-up organizational structure to win the "battle of the narrative." This translates into the fusion of digitalized components at NATO Headquarters and throughout the NATO Command Structure under a "One NATO approach," including: information; intelligence, surveillance, and reconnaissance; corporate communications, public diplomacy, military strategic communications, and public affairs; cyber defense; operations; and related capability groups.

GAME CHANGER 3. FOOTPRINT AND REACH: The COVID-19 pandemic forced NATO to dispense with the idea that high-level meetings had to be held in person. In fact, the speed at which NATO's staff pivoted to a work-from-home posture was breathtaking in speed and success.[5] Investment in digitalization as a way to work until there is a "return to normal" is shortsighted; digitalization offers NATO two complementary advantages that provide outsized benefits when paired together. First, there's no better way to build trust than to do so face to face. A digitalized NATO could place staff members in key strategic locations to enhance understanding while remaining connected to their home headquarters. Consider the strategic benefit of a few innovation staff members embedded in Silicon Valley and Paris focusing on innovation, or political affairs officers located in Tokyo and Accra increasing geographic insight, for example. Second, digitalization can make interacting with NATO much easier for a wide range of partners. Partners wanting to develop relationships with the Alliance are often hamstrung by policy or technological limitations. But digitalization can bolster networks that allow more permissive security policy and opportunity for interaction, thereby increasing NATO's ability to connect with a broader range of partners. Put simply, digitalization enables NATO to take the critical step of matching the placement of its staff to provide the most accurate, timely, and comprehensive risk assessments of the multi-dimensional global operating domain.

GAME CHANGER 4: STAFF AND CULTURE. Dying are the days when retired soldiers and diplomats formed the bulk of NATO's staff. A digitalized NATO needs different competencies in its ranks. But NATO competes globally with the private sector for digital talent—from Allianz to a start-up in Omaha. Thus, NATO needs to reform its talent acquisition and retention policies to

5 "Success" is a subjective term here, but consider how NATO shifted in mid-March to a minimum manning posture in the commands and NATO Headquarters to keep staff and families safe. It upgraded its technical infrastructures to enable secure work from home. NATO's leadership led townhalls and webinars to keep staff apprised of developments regarding COVID-19. Work was re-prioritized to reflect the constraints that pandemic response measures placed on staff. The results are clear: NATO kept the lights on, delivered necessary work, provided much-needed medical supplies, and communicated a strong narrative of steady leadership to allied populations. Was it perfect? No, but NATO's leadership—from branch heads upward, and staff across the organization are to be commended for continuing a high degree of professional output while balancing (greatly) increased family responsibilities in demanding circumstances.

emphasize the expertise for digitalization and match expectations digital professionals are likely to have, like competitive pay and benefits, continuing education and coaching, exercises and training, flexible work arrangements, and the ability to rotate in and out of positions in other sectors to keep perishable skills current. The Alliance needs to champion the policies and cultural attributes espoused by digital professionals, like adopting agile work principles and design thinking, flatter hierarchies, experimentation, innovation, and continuous improvement.

GAME CHANGER 5: A NEW(-ISH) WAY OF WAR. Potential adversaries like Russia and China are pushing ahead with their own digitalization plans and may take a more radical approach with regard to automation of the kill chain and weaponization of information. In doing so, they are increasing risk for everyone by challenging the core assumption that warfare is a primarily human endeavor. Clausewitz still matters, but rapid development of digital-age capabilities like "killer AI" raises serious questions about the ethics and legality of digitalized warfare. Embracing digitalization enables NATO to maintain its core competencies required for collective defense, cooperative security, and crisis management while enhancing its ability to anticipate non-military threats and opportunities. Digitalization helps NATO play a major role in shaping the rules of the road for future conflict; failure to digitalize denies the Alliance opportunity to do so. Moreover, the capabilities ushered in by digitalization diversify NATO's toolset and reduce the risk of the Alliance being a powerful, but irrelevant force in an age where mastery of data is crucial to victory.

Digitalization is not a panacea, but it is the key to NATO's proficiency across all seven emerging and disruptive technology areas. A digitalized NATO carries out the same enduring mission that it has had since 1949, but the form and function of the Alliance must be different to compete and win in an increasingly complex operating environment. NATO has the tools to digitalize masterfully; its allies expect no less.

Jeffrey Reynolds is the Samuel Associates honorary fellow and contributor to the Policy Insights Forum in Ottawa, Canada. The views expressed are his/their own.

Jeffrey Lightfoot is a nonresident senior fellow at the Atlantic Council based in Washington, D.C.