DEFEND IN THE CLOUD

Boost NATO Data Resilience

By Clara Riedenstein and William Echikson,
with Lance Landrum

ABOUT CEPA

The Center for European Policy Analysis (CEPA) is a nonprofit, nonpartisan, public policy institution headquartered in Washington, DC with hubs in London and Brussels, focused on strengthening the transatlantic alliance through cutting-edge research, analysis, and programs. CEPA provides innovative insight on trends affecting democracy, security, and defense to government officials and agencies; helps transatlantic businesses navigate changing strategic landscapes; and builds networks of future leaders versed in Atlanticism.

Cover photo: A Danish Air Force crewmember monitors the skies over Poland in their E-3A Airborne Warning and Control System (AWACS) aircraft. Credit: NATO via Flickr.

Contents

Executive Summary

Data is becoming the “currency of warfare.” Since data drives innovation in logistics and weaponry, it must be interoperable among allies, and the best way to secure and share data requires duplicating it and moving it to the cloud.

NATO is at a turning point. Rising transatlantic tensions are causing a major rethink, forcing Europe to promise to boost defense spending and consider how it could cope without the US security umbrella. Allies are prioritizing their own security and contracting national companies to build up their cloud services. Independent of the current transatlantic tensions, NATO allies and their defense ministries need to reinforce common systems for data sharing and security.

Key Recommendations

This paper details the obstacles to and provides a blueprint for reform. It builds on in-depth workshops and interviews with NATO officials, experts, and business representatives under the Chatham House rule. This paper makes two sets of recommendations. The first focuses on NATO as a digital thought leader and bridge between its 32 member states. The second explores how the alliance can lead by example, accelerating its own digital transition.

Thought Leadership

Promote Data Embassies: For data to be secure, they must be able to withstand attacks. This means securing a copy of all government data outside the country. **NATO should promote setting up “data embassies”** following Estonia’s example when backing up its critical government data in Luxembourg. The 2025 NATO Summit in The Hague is the perfect opportunity to further and strengthen a robust data security structure.

Engage the Private Sector: Tech leaders play a crucial role in supporting governments’ war-fighting efforts. **NATO should promote “secure and interoperable by design” standards as compulsory requirements for digital technologies** provided by the private sector. Companies need a seat at the table to understand government needs. This means **hosting industry forums and inviting companies to NATO military testing and experimentation**.

Reassess Procurement: NATO should **consider agile procurement models for fully digitized capabilities** (e.g., cloud, command and control systems, artificial intelligence–enabled analytics applications). **These would ideally reduce bureaucratic procedures** and ownership in a single NATO authority to reduce bottlenecks and expedite the entire process. Given the fast-evolving nature of the products in question, any contract must include robust post-sale technical support from the vendors to ensure software is constantly updated, secure, and reliable.

Action Leadership

Fix the "Say/Do" Gap: NATO does deploy dedicated teams and initiatives to achieve cloud interoperability. The Digital Policy Committee and Cyber Defense Committee oversee data standardization and cybersecurity. **The alliance's 2022 Digital Transformation Strategy announced strong initiatives**, such as a common "digital backbone," a data-sharing ecosystem, and an interoperability framework. But these initiatives need to be accelerated. **Political buy-in needs to speed up the procurement of digital services**. Acknowledging the protectionist tendencies of allies, one way to accelerate these initiatives might be through voluntary contributions. EUROPOL and INTERPOL have mechanisms that promote voluntary data sharing through a common data language.

Ensure Compliance: While allies agree on the importance of standards, they differ in implementation. If allies agree to common standards, these should be adhered to. **NATO's Strategic Commands could be empowered to test such standards in training and exercises**. NATO could also consider excluding nonconforming members from joint initiatives, and collective procurement schemes.

Introduction

A day before Russian tanks rolled into Ukraine in 2022, the Kremlin launched a major cyber offensive, deploying FoxBlade malware to target Ukraine's government data. The attack flopped. Ukraine, working with tech companies and Western intelligence, fixed most of the damage. Private sector companies moved threatened software services onto the cloud.[1] Resilient infrastructure and data backups mitigated Russian cyberattacks.

Since then, the challenges facing NATO have mounted. Russia's threat remains real and divisions within the alliance are widening. US President Donald Trump's peace overtures to Ukraine have sparked a major rethink, forcing Europe to promise to boost defense spending and consider how it could cope without the US security umbrella.

Whatever happens with transatlantic relations, NATO allies need to reinforce common systems for data sharing and security. Allied defense ministries need to communicate. Private companies entrusted with setting up ministries' sovereign cloud services must bake in this seamless communication as a product requirement.

So far, NATO allies are failing to meet this goal. Few governments have moved their data onto a cloud service. Many alliance members continue to store data locally in a few vulnerable locations. NATO is just beginning its transition to a collective cloud and data-sharing ecosystem.

Most digital services that exist within the alliance are not interoperable. When they move data to the cloud, governments often opt for national companies to provide cloud services, rather than outsourcing. France has selected French company Thales as its first cloud provider, whereas Italy entrusted Italian defense company Leonardo with studying the feasibility of cloud operations for its ministry of defense.[2] Germany's public sector contracted German cloud service provider Arvato to lead operations on its first sovereign cloud.[3]

The US is just as protectionist and focused on security. Amazon, Google, Microsoft, and Oracle are designing its sovereign cloud.[4] Although it's understandable that governments seek contracts with their own national companies to support their economies, these national champions need to coordinate. Divergences in data management on a policy and technical level lead to day-to-day difficulties and hurdles in crucial intelligence sharing.

The alliance needs to digitize its operations, move them onto the cloud, and increase interoperability and data sharing. As data become the "currency of warfare" and militaries integrate artificial intelligence (AI) into many weapons systems and

Photo: British Army soldier checks computer server equipment. Credit: ipm / Alamy Stock Photo.

capabilities, it is crucial to have common infrastructure in place to process the data and share them securely.

This paper offers a blueprint for reform. NATO's 2022 Digital Transformation Strategy already contains initiatives that should be funded and implemented: a data-sharing ecosystem, an interoperability framework, and a common "digital backbone." A group of 22 NATO countries is committed to purchasing common cloud capabilities.

But these initiatives need to be set in motion. A large gap exists between what NATO says it will do, and how quickly it does it. NATO agencies lack skilled personnel. Budget procurement processes are not agile. Political initiative from the allies and cooperation with private companies is critical for the next NATO summit at The Hague; data security and interoperability must be put at the top of the agenda. Private companies that provide most governments with cloud services need to be brought into the conversation to establish "security by design" measures and improve interoperability.

Interoperability: A Military Necessity

Although war is full of human sacrifice and destruction, it is also full of logistical challenges. If allies do not have the same railway gauge, then they cannot deliver much-needed arms to the battlefield. All military alliances need to establish a level of interoperability and standardization.

Ukraine provides NATO with a case study about "military mobility," the capacity of transporting heavy military equipment quickly across the continent.[5] Red tape, legal constraints, and differing standards on bridges and roads hamper a country's military effectiveness. If a civilian bridge is too weak to hold the heavy military equipment needed during wartime, NATO's ability to defend itself is compromised.

NATO allies recognized this challenge early in the alliance's history. Without common standards for military infrastructure, the alliance would be ineffective. Set up in 1951, the Standardization Office is the oldest committee in the alliance and sets operational standards for NATO forces.[6] It manages thousands of standards set by other committees on infrastructure, armaments, aviation, communications, and logistics. Everything from firefighting equipment to airfield length is standardized, and these standards are constantly updated.[7]

NATO's military load classification for bridges, vehicles, and ferries specifies the safe amount of weight a route can withstand.[8] It dictates how the capacity is indicated (in whole numbers) and establishes standards for bridges and roads based on physical characteristics, type of traffic, and weather effects. It also classifies vehicles based on track width and length. Like a great puzzle, allied armies can transport military equipment across borders by matching the right vehicles with the right physical infrastructure.

Consider another example: fuel. It is standardized within the specified parameters. Using the wrong fuel type in a plane, called "misfueling," can cause severe engine malfunctions — loss of power or engine malfunctions. To avoid this, the Single Fuel Concept dictates that all NATO military vehicles use the same diesel, F-34.[9]

NATO also provides standards for civilian infrastructure based on the assumption that it will become dual use in a time of war. NATO's standards for airfields and runways include specifications for airfield lighting.[10]

While having these standards is prudent, their adoption and enforcement often remain ineffective. NATO lacks enforcement authority, instead relying on individual allies to comply. Former Italian Prime Minister Mario Draghi's recent report on European competitiveness revealed that NATO members provided Ukraine with 14 types of howitzers, a type of short-range cannon.[11]

Photo: As part of NATO's Unified Vision 2014 Trial, members of the Italian Air Force launch a surveillance drone (STRIX, a multi-purpose, man-portable, totally autonomous TUAS) over Oerland, Norway. Credit: NATO via Flickr.

Unsurprisingly, this lack of standardization causes serious problems for the Ukrainians on the battlefield. The report argued that the European Union (EU) should instead create a "single authority" for defense to enforce unified common standards for weapons. NATO does not have the authority to do this, so the best its Standardization Committee can do is point to gaps in standards compliance. This weakness leads to huge divergences among members and a lack of accountability.

Data Resilience

Warfare and national security are becoming techy. AI and other emerging technologies accelerate the analytics used in tanks, air defense systems, and other military capabilities. Militaries are using and storing a huge amount of sensitive data. The data needs to be protected from both physical and cyberattacks.

As with physical infrastructure, NATO will be ineffective if it cannot share data and systems to support allies. Building secure bridges is important, but if they can't support allied trains, they are useless in wartime. The same goes for data. If they can't be securely stored and shared with allies, they will fail to assist the alliance in making much-needed rapid decisions.

Data Security

Countries are understandably tight-lipped about sensitive data. Sharing military data increases the risk of cyber espionage or interception. If one nation suffers from weak cybersecurity, sensitive data could be compromised, making it a liability for all. Data sharing and processing need to be secure, yet accessible, to authorized users.

War is unpredictable and requires the ability to take quick action. Data and information need to be accessible at a moment's notice whenever NATO is pulled into a conflict. In addition to being able to see the data unencrypted, NATO needs to ensure that the new entities, spread over the theater of operations, can connect and share data and information. The only way to achieve this goal is moving operations onto the cloud.

Most governments and ministries of defense started transferring defense operations to the cloud only in 2024. The US Department of Defense finalized contracts with private companies in 2022 to set up sovereign cloud systems.[12] It took the Italian and German departments until 2024 to sign procurement contracts for cloud services.[13] Many NATO allies do not yet have concrete plans to move operations to the cloud.

It is crucial to build trust among allies. Data security should not mean storing all of one's data within the country. If physical or digital infrastructure is destroyed, then all data vanishes. The "NotPetya" attack against Ukraine in 2017 exposed this vulnerability. Russia's military intelligence agency launched the attack through a compromised software update on Ukrainian accounting software to irreversibly destroy government data. The impact was immense, with the White House estimating damages at $10 billion.[14] This loss highlights the importance of reinforcing protections for government data.

Some countries have already taken action to mitigate the risk of data loss. In 2017, Estonia and Luxembourg signed a "Data Embassy" agreement.[15] A copy of all of Estonia's government data is stored in Luxembourg under Tier 4 security. While Estonia has its own sovereign cloud, it has understood that national security requires creating data backups.

NATO has begun moving its unclassified business activities to the cloud and will complete the operation for the Strategic Commands and most of the NATO Enterprise this year. According to some NATO sources, the movement of restricted and secret information to the cloud is also underway, but slowly.

Data Interoperability

Allies need access to each other's data on bilateral, multilateral, and alliance-wide levels. Various kinds of datasets exist for research and development, operations, communications, intelligence, and command and control. Although NATO does not need to make all data interoperable, certain datasets need to be interoperable. Without common data processing and sharing, allies cannot share time-critical intelligence or key mission information. Nor can they jointly develop, for example, AI-powered weapons. Since common standards secure physical and certain digital infrastructure, it seems logical that they would have similar standards for data processing and sharing.

This is not so. Technical and policy divergences mean allies do not have easy access to each other's data. Even the closest partners fail in basic interoperability. Take AUKUS, the trilateral partnership between Australia, the United States, and the United Kingdom (UK). The three countries are close allies, but they do not share an accreditation standard, which is an assurance that data is handled, stored, and processed safely. This means even the lowest-security-level data cannot be exchanged. The different teams cannot turn on their cameras on team meetings, nor can they work together on the same document. An effective military alliance needs to work together to be effective.

Allies have different data protection policies, which leads to difficulties. Europe's General Data Protection Regulation imposes strict limits on what information can be processed and how in the UK and EU.[16] As one interviewee told the authors of this paper, civilian data protection laws prevent tank crews from training because data collection of civilians in peacetime is prohibited.[17] The tank crews must turn off their "smart functionality" every time they encounter pedestrians. In effect, this means that militaries cannot conduct effective training with advanced equipment.

The Crossed Swords exercise, conducted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), is designed to train cyber specialists to successfully execute a full kill chain offensive cyber operations in a simulated crisis environment and also train military command elements in command and control of offensive cyberspace capabilities. Credit: NATO CCDCOE via Flickr

By contrast, the US remains more relaxed about data than its partners across the Atlantic.[18] It lacks a comprehensive data privacy law. Differences in policies complicate data sharing. If the tank in our example were a US tank, for example, it could collect civilian data, since no US law prohibits the collection. If the US wanted to share the data it collected with European allies, however, this would cause problems.

Differences in which countries trust each other are also at play. For example, the Five Eyes alliance among the US, the UK, Canada, Australia, and New Zealand has an extensive, interoperable intelligence-sharing system.[19] In contrast, other governments in the NATO alliance do not have similar arrangements and are often mistrustful of each other.

The Path Toward a Digitally Resilient Alliance

Is This NATO's Job?

Recognizing data security and interoperability as a problem is one thing. But we still must answer the question, "What should NATO do about it?" When NATO broadens its focus, uncertainties persist regarding its jurisdictional rights.

Article 3 of the North Atlantic Treaty clarifies that NATO should have a role. The article gives the alliance the right to "maintain and develop their individual and collective capacity to resist armed attack."[20] This mandate includes civilian infrastructure but could also include communications systems and data infrastructure. If these systems fail to support NATO's ability to resist armed attack, armies are left at a significant disadvantage in a digitized combat environment. If the alliance wants to employ AI and drones in the future against an armed attack, it needs digitized and interoperable defense ministries.

What role should NATO play? In some sense, the organization seems well-placed to take over such data security responsibilities. It already has a dedicated digital and technology agency, the NATO Communications and Information Agency, which manages NATO communications infrastructure and information technology.[21] That includes data storage and management. NATO's Digital Policy Committee establishes policy and standards for communications, command, and consultation; cyber defense; and data interoperability.[22]

But this is tricky. For one, establishing multinational standards takes a long time. Accounting for the pace of technological advancement, any agreed-upon standard would likely be outdated by the time it was implemented. According to one interviewee for this paper, standard setting takes around two years.[23] Since 2022, NATO has hired staff to manage material and digital standards, as well as accelerate the adoption of standards. But the work required to develop or revise standards remains daunting. As the war in Ukraine demonstrates, enforcing standards and implementing them is challenging.

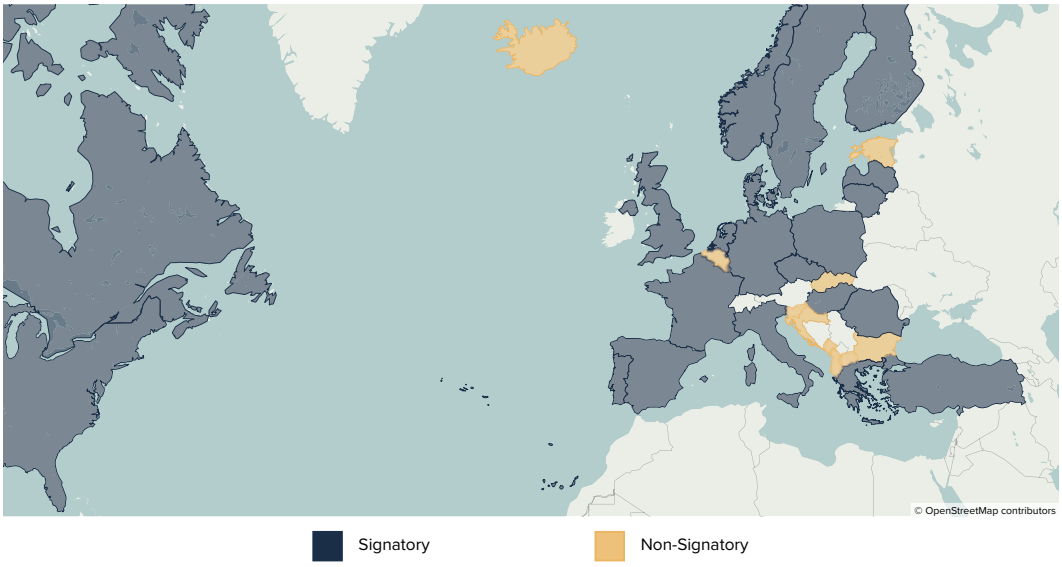
On a theoretical level, data security and interoperability fall squarely within national security. NATO has jurisdiction over collective standards related to intelligence and strategic data. But these standards can achieve their intended effect only when each ally pulls its weight, ensuring adoption and compliance.

What NATO Has Done

NATO has already begun work on data resilience and interoperability. The Digital Policy Committee is responsible for the technical aspects of data standardization.[24] The Cyber Defense Committee provides policy and standards for cybersecurity.[25] The alliance has published a Digital Transformation Implementation Strategy, which includes specific reference to a data-sharing ecosystem, a digital interoperability framework, and a digital backbone.[26] The alliance's Federated Mission Networking is charged with improving interoperability and collaboration in military operations. It provides a framework for information sharing across forces, and so already plays a role in ensuring that different national command and control systems can communicate effectively.

Yet data were low on the agenda at the 2024 NATO Summit in Washington. Even though "interoperability" was stated often, the Summit's official text has no mention of data resilience.[27] Other issues took priority. Even so, 22 allies signed a letter of intent to purchase the first alliance-wide cloud capability, dubbed the software for Cloud and Edge.[28] This initiative provides a multinational capability for classified networks and may eventually expand to include more or all allies. A recent NATO Cloud Conference in Brussels strengthened the political force behind the initiative.[29]

Map 1. Letter of Intent for the Allied Software for Cloud and Edge (ACE) Services



Map: Center for European Policy Analysis. Source: NATO.

Table 1. NATO Cloud Providers

Country	Cloud Providers for the Ministry of Defense	Countries of Origin for Provider
USA	Amazon Web Services, Google Support Services, Microsoft, and Oracle	USA
Turkey	HAVELSAN and MilSOFT	Turkey
France	Atos, Capgemini, and the French Alternative Energies and Atomic Energy Commission	France
UK	Amazon Web Services, Microsoft, Netcompany, and Oracle	USA, and Denmark
Germany	BWI GmbH	Germany
Poland	Microsoft Azure	USA
Italy	TIM, Leonardo, Cassa Depositi and Prestiti, and Sogei	Italy
Estonia	RIKS, Cybernetica, Dell EMC, Ericsson, OpenNode, and Telia.	Finland, USA, Sweden, Estonia
Denmark	Microsoft Azure	USA

Table: Center for European Policy Analysis.

This progress remains fragile — implementation has been lagging. Procurement remains hyper-bureaucratic and too sluggish to keep up with the pace of innovation. How exactly these services are going to be established within NATO and by whom is still unclear.

Donald Trump's return to the White House has stoked tensions and raised questions regarding US reliability in the alliance. Evolving allied dynamics and continued European security threats from Russia and its partners have forced European decision-making on necessary defense spending and evaluations of dependency on US capabilities.

These extend to digital dependency. During the past four years, France pushed the European Union to impose sovereignty requirements in its cloud certification rules. Stiff resistance from the Netherlands and the Nordics managed to remove almost all the restrictions. But today France is renewing its call — and sovereignty requirements are again under debate for cloud certification rules.

Photo: Locked Shields Partners Run 2025, organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), brought together the private sector, academia, and the defense community to test their cyber defense capabilities. Credit: NATO CCDCOE via Flickr.

US tech is squeezed. Most companies agree to provide European governments with control over the data that they store. Europeans realize that shutting themselves off from the most cutting-edge cloud services will be counterproductive. But the battle over exactly how much to depend on US tech has been reignited, and European officials gain by promoting self-sufficiency, what they call “digital sovereignty.”

Some allies now may be hesitant to hand over their sensitive data to US cloud service providers. If a US company decides to withdraw from a data resilience plan, say, then it might still own the data. In a military context, that is risky. NATO’s data-sharing ecosystem has encountered resistance. As governments become concerned with protecting their national security, they are becoming resistant to data sharing “beyond what is immediately relevant,” according to one expert.[30]

A Data Resilience Framework

NATO has a role to play in bolstering data resilience. The alliance often acts as a matchmaker for its 32 member states. While NATO as an organization cannot enforce standards itself, it can facilitate the development of shared systems.

Governments are starting to prioritize their own national security, and this certainly means securing their data. But they need to do it smarter, and that involves trusting other NATO allies. For this to happen, the alliance needs to take concrete steps. A few are outlined below.

Thought Leadership

First and foremost, NATO should facilitate its members' digital transitions, encourage security measures, and promote cooperation with the private sector.

Promote data embassies: For data to be secure, it must be able to withstand attacks. This means ensuring redundancy by saving a copy of all government data in a different physical location. In case of armed conflict, digital and physical infrastructure are at risk. The alliance should promote setting up "data embassies" across member states, following the example of Estonia and Luxembourg.

NATO should enable a framework for trusted allies to set up similar initiatives. As a forum, NATO provides a good context for these conversations. It can facilitate the sharing of lessons learned and streamline the establishment of data embassies at an alliance-wide level. The 2025 NATO Summit in The Hague is the perfect opportunity to further and strengthen a robust data security structure.

Guide the private sector: "The government's role is to be the warfighting expert and the private sector's role is to support," says one of the experts interviewed for this paper.[31] Given this clear division of labor, both parties need to be clear on their respective roles.

This means defining "secure by design" systems so allies can be confident sharing data. After a gas pipeline hack in the US in 2021, the US Cybersecurity and Infrastructure Security Agency established security principles for new technologies, which require new products to have cybersecurity measures built in.[32]

NATO should anticipate the need for such principles, laying out clear guidance for all private companies providing cloud services to allied governments. This should be done in collaboration with industry forums such as the ones NATO already hosts.[33] Private companies should be invited early and regularly to military testing and experimentation, so they understand the requirements of the systems. Equally important, NATO should include "secure and interoperable by design" as compulsory requirements for all digital technologies, systems, and services developed and provided by the private sector.

The alliance should set NATO with a clear role to provide a forum where conversations between the public sector and private companies occur on an alliance-wide level. Whichever company designs a sovereign cloud service within the alliance should be using NATO standards.

Reassess the procurement process: NATO should also consider more agile procurement models specifically tailored for fast-iterating technologies such as software-defined and fully digitized capabilities such as cloud, command and control systems (C2), and AI-enabled analytics applications. These mechanisms would ideally require fewer bureaucratic procedures and ownership of a single NATO authority/agency to reduce bottlenecks and expedite the entire process. Furthermore, given the fast-evolving nature of the products in question, any contract must include robust post-sale technical support from the vendors to ensure software is constantly updated, secure, and reliable.

Action-Guided Leadership

NATO should also lead by example. Actionable steps that accelerate NATO's digital transformation and track the progress of standards implementation will incentivize allies to take action and provide actionable steps for the digitization of all NATO members.

Fix the "say/do" gap: Many of the issues raised in this paper are not new to NATO. The alliance's Digital Transformation Strategy already announced many of the right initiatives. A common digital backbone, interoperability framework, and data-sharing ecosystem would resolve many obstacles to achieving NATO's aims for effective defense and deterrence.

But the alliance needs a sense of urgency. Political buy-in and greater flexibility are necessary to speed up the procurement of digital capabilities and jumpstart the establishment of common cloud systems. In light of increased tensions between the US and Europe, NATO remains a forum in which allies can converge. Without a common data-sharing system, NATO cannot project effective military force.

One possible solution could be voluntary contributions. An example comes from the United Nations' Centre for Humanitarian Data.[34] Through a single data language, the center facilitates data sharing among nongovernmental organizations (NGOs) and companies, which can selectively input data and choose the level of access they want. Then partners can see and use these data to develop projects and stay informed on developments across the field. EUROPOL and INTERPOL have similar data-sharing mechanisms that could serve as inspiration for the alliance.[35]

Ensure accountability and compliance: Allies agree on the importance of standards. But there are large discrepancies in implementation. If allies agree to common standards, these should be adhered to. One option for this would be closer cooperation between NATO and the EU. Unlike NATO, the EU can create enforceable material and digital standards and track their implementation.

Photo: Locked Shields 2024, the world's most advanced live-fire cyber defence exercise, concluded with an unprecedented twist. Despite the exercise's competitive nature, participating teams formed a grand coalition by sharing information. Credit: NATO CCDCOE via Flickr.

Every time a NATO standard is agreed upon, there should be clear mechanisms of verifying that it is being met by member states. NATO should explore options for testing compliance with material and digital standards as it already does with operational standards. While digital systems of participating allies are already tested for compatibility in annual readiness exercises, the Strategic Commands could be empowered to test such standards in other training and exercises. If there is a common data-sharing system or an interoperability framework, it will be valuable only insofar as NATO can rely on all allies to comply with it.

At the same time, NATO should consider specific internal mechanisms to increase the cost of noncompliance with allied standards, including the potential exclusion of nonconforming members from military exercises, joint training initiatives, and collective procurement schemes, among other options.

Conclusion

NATO has a clear mandate to secure data and enhance interoperability. The alliance cannot be effective militarily without common security standards and data sharing. As European capitals step up their defense capabilities and move toward wartime economies, NATO needs to move toward wartime digital resilience.

Although the alliance's Digital Transformation Strategy provides a good reform blueprint, NATO needs to infuse the suggested initiatives with a new sense of urgency. As war rages in Ukraine and the Russian threat mounts, the threats the alliance faces are severe, almost existential. Cracks between the US and European wings of the alliance are expanding. And yet opportunities remain. Europe is poised to boost its spending and defense self-sufficiency. NATO will remain an indispensable platform to help ensure that the money is well spent — and enables the allies to communicate and share data.

Acknowledgments

The authors are grateful to our peer reviewers who shared their thoughts and feedback on earlier versions of the report.

Special thanks to Catherine Sendak and Ronan Murphy at CEPA for their assistance throughout the research and editing process.

The authors are also grateful to the participants of our two research workshops, the interviewed experts and officials who helped shape this report, and the support of Microsoft in making this publication possible.

CEPA maintains strict intellectual independence over all publications and projects.

About the Authors

Clara Riedenstein is a Project Assistant for the Tech Policy Program at the Center for European Policy Analysis (CEPA). She received her BA from Oxford University, where she is now a graduate student in the Department of Politics and International Relations. Her academic research focuses on Internet governance, content moderation, and the moral status of AI.

William Echikson is a Non-resident Senior Fellow with the Tech Policy Program and editor of the online tech policy journal Bandwidth at the Center for European Policy Analysis (CEPA). Before joining CEPA, he worked at Google running corporate communications for Europe, the Middle East, and Africa. He began his career as a foreign correspondent in Europe for a series of US publications, including the Christian Science Monitor, the New Yorker, Wall Street Journal, Fortune, and BusinessWeek. He is the author of four books, including works on the collapse of communism in Central Europe. He also directed and wrote documentaries for BBC and PBS. Mr. Echikson graduated from Yale College with a Magna Cum Laude degree in history. He spent a year at the Harvard University Russian Research Center.

Lieutenant General Lance Landrum (Ret.) is a Non-resident Senior Fellow with the Transatlantic Defense and Security Program at the Center for European Policy Analysis (CEPA). Lance served in the US Air Force for over 31 years developing leadership experience in global operations, intelligence, surveillance, and reconnaissance, and joint requirements and capability development. Lance is the President of Team Landrum Advising and Consulting, LLC, providing strategic advice on executive-level leadership and developing enterprise strategy. Lance served as the Deputy Chair of NATO's Military Committee (2021-2023) during which he helped forge consensus by negotiating compromise among allies as the headquarters developed political-military advice for the North Atlantic Council to bolster deterrence and defense during the conflict in Ukraine. He was also the United States European Command Director of Operations, J3 and the Joint Staff J8 Deputy Director for Requirements and Capability Development. Lance has a Bachelor of Science in Engineering Mechanics, a Masters of Aeronautical Science, and a Masters in Strategic Studies.

Endnotes

1 David Ignatius, "How Russia's vaunted cyber capabilities were frustrated in Ukraine," The Washington Post, June 21, 2022, https://www.washingtonpost.com/opinions/2022/06/21/russia-ukraine-cyberwar-intelligence-agencies-tech-companies/.

2 Thales, "NATO Selects Thales To Supply its First Defence Cloud for the Armed Forces," January 25, 2021, https://www.thalesgroup.com/en/group/journalist/press-release/nato-selects-thales-supply-its-first-defence-cloud-armed-forces.; Defense Mirror.com, "Leonardo to Study Feasibility of Cloud Computing for Italian Military," February 19, 2024, https://www.defensemirror.com/news/36147/Leonardo_to_Study_Feasibility_of_Cloud_Computing_for_Italian_Military.

3 Gernot Wolf, "First Sovereign Cloud Platform for the German Administration on the Home Straight," Bertelsmann, September 24, 2024, https://www.bertelsmann.com/news-and-media/news/first-sovereign-cloud-platform-for-the-german-administration-on-the-home-straight.jsp.

4 C. Todd Lopez, "DOD Makes Headway on Cloud Computing," U.S. Department of Defense, March 29, 2023, https://www.defense.gov/News/NewsStories/Article/Article/3345260/dod-makes-headway-on-cloud-computing/.

5 Hanne Cokelaere, "Ukraine War Forces an EU Rethink of Military Mobility," Politico, November 10, 2022, https://www.politico.eu/article/ukraine-russia-war-eu-rethink-military-mobility/.

6 NATO, "NATO Standardization Office," June 9, 2017, https://www.nato.int/cps/en/natohq/topics_124879.htm.

7 NATO, "STANAG 1169 Ed: 2: 2018" March 9, 2023, https://www.intertekinform.com/en-us/standards/stanag-1169-0-. 736442_saig_nato_nato_1788811/?srsltid=AfmBOooWEldwX9KF2mPQQUXD4n4hYQhZu6u7tmYW8_oW1q2sKTZoPBdf; Supreme Headquarters Allied Powers Europe, "Criteria and Standards for Tactical Airfields," n.d., https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_archives/20121128_19530501_NU_Criteria_and_Standards_for_Tactical_Airfields.pdf.

8 NATO, "Military Load Classification of Bridges, Ferries, Rafts and Vehicles," September 14, 2017, https://edstar.eda.europa.eu/Standards/Details/cd7627b3-3384-46b0-a6cd-2cdc53645ac3.

9 NATO, "Military Fuels and the Single Fuel Concept," October 1997, https://www.nato.int/docu/logi-en/1997/lo-1511.htm.

10 Supreme Headquarters Allied Powers Europe, "Criteria and Standards for Tactical Airfields."

11 Mario Draghi, "The Future of European Competitiveness," European Commission, September 2024, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059.

12 Lopez, "DOD Makes Headway on Cloud Computing."

13 Defence Mirror.com, "Leonardo to Study Feasibility of Cloud Computing for Italian Military."; Wolf, "First Sovereign Cloud Platform for the German Administration on the Home Straight."

14 Columbia University, "NotPetya: A Columbia University Case Study" (School of International and Public Affairs Case Consortium @ Columbia, 2021), https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf.

15 "e-Governance," e-Estonia, n.d., https://e-estonia.com/solutions/e-governance/data-embassy/.

16 European Parliament, "Regulation (EU) 2016/679" (April 27, 2016), https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

17 Assessment shared by a Dutch military official in a workshop session organized by the authors via Zoom, March 2025.

18 Conor Murray, "U.S. Data Privacy Protection Laws: A Comprehensive Guide," Forbes, April 25, 2023, https://www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide/.

19 J. Vitor Tossini, "The Five Eyes – The Intelligence Alliance of the Anglosphere," UK Defence Journal, April 14, 2020, https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/.; "Five Eyes Intelligence Oversight and Review Council (FIORC)," The National Intelligence and Security Center, n.d., https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc.

20 Clara Riedenstein and Eduardo Castellet-Nogués, "The Money War with China: NATO and Economic Security," Europe's Edge, July 1, 2024.

21 "Technology and Innovation," NATO Communications and Information Agency, n.d., https://www.ncia.nato.int/about-us/technology-and-innovation.

22 "Digital Policy Committee (DPC)," NATO, last modified January 31, 2024, https://www.nato.int/cps/fr/natohq/topics_69279.htm?selectedLocale=en.

23 Assessment shared by a former US military officer and scholar in an interview with the authors via Zoom, February 2025.

24 NATO, "Digital Policy Committee."

25 "Cyber Defence," NATO, last modified July 30, 2024, https://www.nato.int/cps/en/natohq/topics_78170.htm.

26 "NATO's Digital Transformation Implementation Strategy," NATO, last modified October 17, 2024, https://www.nato.int/cps/en/natohq/official_texts_229801.htm.; NATO, NATO Digital Backbone & NATO Digital Backbone Reference Architecture (NATO, December 13, 2024), https://www.nato.int/nato_static_fl2014/assets/pdf/2024/12/pdf/241213-DBRA.pdf.

27 "Washington Summit Declaration," NATO, last modified July 10, 2024, https://www.nato.int/cps/en/natohq/official_texts_227678.htm?selectedLocale=en.

28 "Allies Launch Strategic Initiatives to Enhance Capabilities," NATO, last modified August 1, 2024, https://www.nato.int/cps/en/natohq/news_227472.htm.

29 "NATO Cloud Conference Advances Innovation and IT Security Across the Alliance," NATO, last modified January 23, 2025, https://www.nato.int/cps/en/natohq/news_232539.htm?selectedLocale=en.

30 Assessment shared by a British academic in a workshop session organized by the authors via Zoom, March 2025.

31 Assessment shared by a Dutch military official in a workshop session organized by the authors via Zoom, March 2025.

32 "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," Cybersecurity & Infrastructure Security Agency, effective May 7, 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.; "Secure by Design," Cybersecurity & Infrastructure Security Agency, n.d., https://www.cisa.gov/securebydesign.

33 "NATO-Industry Forum," NATO Allied Command Transformation, n.d., https://www.act.nato.int/activities/nato-industry-forum/.

34 "What We Do," Centre for Humdata, n.d., https://centre.humdata.org/what-we-do/.

35 "Europol Information System (EIS)," Europol, last modified December 7, 2021, https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system.; "Our 19 Databases," Interpol, n.d., https://www.interpol.int/How-we-work/Databases/Our-19-databases.

Center for European Policy Analysis HQ
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004

info@cepa.org | www.cepa.org