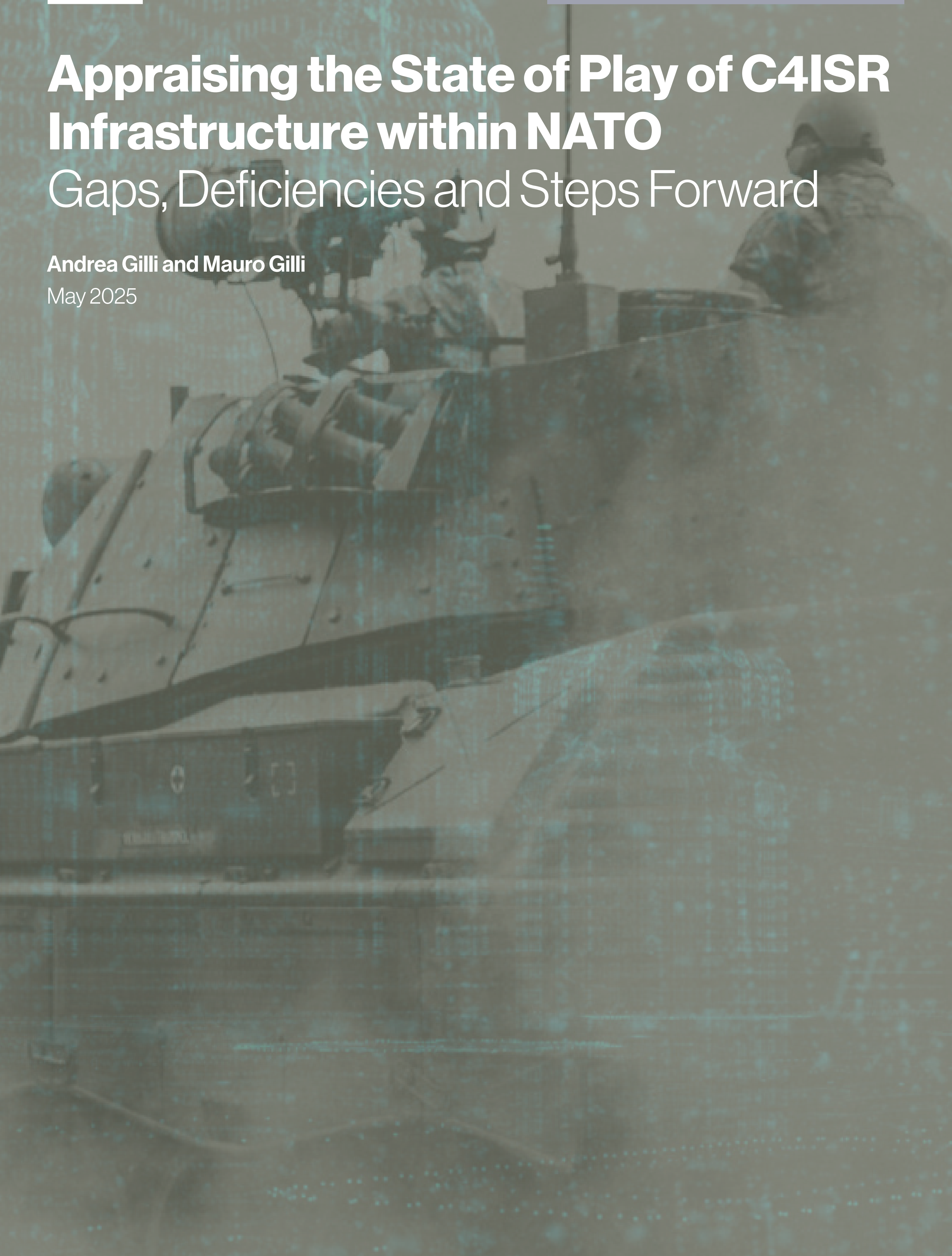
The Hague Centre
for Strategic Studies

Fit for the Future?
Towards a digitally-capable
NATO Alliance for the 21st Century



Appraising the State of Play of C4ISR Infrastructure within NATO

Gaps, Deficiencies and Steps Forward

Andrea Gilli and Mauro Gilli

May 2025

The Hague Centre
for Strategic Studies

Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward

Authors:
Andrea Gilli, Lecturer, University of St Andrews;
Mauro Gilli, Senior Researcher, ETH-Zurich.

Editor:
Tim Sweijs

May 2025

This HCSS paper is part of a series of guest contributions related to the “NATO’s digital capabilities” project, established in the run up to the 2025 NATO summit in The Hague. The research was made possible through a financial contribution from Microsoft to the Hague Centre for Strategic Studies (HCSS).

Introduction

The North Atlantic Treaty Organization (NATO) stands as the strongest military alliance in history, a product of shared principles, political cohesion, dedicated armed forces, and advanced weapon systems. Central to this superiority is NATO's Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) infrastructure, the "nervous system" that ensures unrivalled situational awareness, precision, and effectiveness.[1] By integrating data-gathering platforms, communication architectures, and data-processing capabilities, C4ISR enables NATO to anticipate and neutralize threats, achieving its core tasks of deterrence and collective defence. This infrastructure comprises both national contributions – such as tactical data links (Link 11, Link 16, and the emerging Link 22) – and NATO-owned assets, including the Airborne Early Warning and Control System (AWACS) and Allied Ground Surveillance (AGS) programs. Despite NATO's unmatched C4ISR capabilities, the Alliance faces mounting challenges in an era of renewed strategic competition. The diffusion of precision munitions, electronic warfare (EW), and cyber capabilities threatens to undermine critical C4ISR assets. For instance, Russia's advanced EW systems, demonstrated in Ukraine by jamming GPS and Link 16 signals, expose vulnerabilities in NATO's communication networks, risking operational paralysis in contested environments.[2] Concurrently, modernization efforts at the national level, if uncoordinated, risk exacerbating interoperability gaps, fragmenting the Alliance's C4ISR architecture. These challenges are compounded by over two decades of European underinvestment, which have left legacy platforms ill-equipped for multi-domain operations (MDO) and emerging threats.[3] This paper appraises the state of NATO's C4ISR infrastructure, assessing its readiness to serve as the backbone for major joint operations, identifying critical gaps and deficiencies, and proposing steps to enhance its effectiveness. Drawing on lessons from recent conflicts, such as Ukraine's integration of commercial technologies like Starlink, and NATO's own innovation efforts, the paper offers actionable recommendations for the 2025 NATO Summit.[4]

Despite NATO's unmatched C4ISR capabilities, the Alliance faces mounting challenges in an era of renewed strategic competition.

[1] Gordon B. "Skip" Davis Jr, *The future of NATO C4ISR: Assessment and recommendations after Madrid* (Washington, DC: Atlantic Council, 2023).

[2] Justin Bronk, "Airborne Electromagnetic Warfare in NATO: A Critical European Capability Gap," *Occasional Paper* (London: RUSI, 2025).

[3] Andrea Gilli, Mauro Gilli, and Niccolò Petrelli, "Rearming Europe: Challenges and Constraints," *War on the Rocks*, April 15 2025.

[4] Mila Tanghe, "What European NATO Lacks," *Insights & Analysis* (Washington, DC: CEPA, 2025).

1. NATO and C4ISR

This section examines the role of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) within NATO, detailing its components, current capabilities, and ongoing modernization efforts in the context of strategic competition. It highlights the interplay between NATO-owned and national assets, identifies key gaps, and outlines the Alliance's transition to multi-domain operations (MDO) to counter emerging threats.

C4ISR: The Nervous System of Modern Warfare. C4ISR represents the backbone of contemporary military operations, integrating sensors, communication networks, and data-processing systems to enable superior situational awareness and combat effectiveness.[5] Command and control (C2) directs forces, communications ensure secure data exchange, computers process information, and intelligence, surveillance, and reconnaissance (ISR) gather multi-domain data (e.g., ELINT, COMINT, SIGINT).[6] Evolving since the 20th century, C4ISR has become increasingly complex, driven by lethal, fast-paced warfare across land, sea, air, cyber, and space domains.[7] Early examples, such as the Battle of Britain's air defence network, laid the groundwork for modern battle networks, which now fuse data from diverse sensors, process it through advanced software, and distribute it to effectors for tactical, operational, and strategic outcomes.[8] C4ISR comprises three core elements:

- Data-Gathering Platforms: Sensors on platforms like drones, satellites, and maritime patrol aircraft collect data across domains.
- Communication Architectures: Tactical data links (TDLs) like Link 11, Link 16, and Link 22 enable secure, real-time data sharing.
- Data-Processing Systems: Command centres and AI-driven analytics fuse and analyze data for decision-making.

NATO's C4ISR infrastructure is a hybrid of national contributions and Alliance-owned assets, reflecting the collective action and coordination challenges inherent in coalition warfare.

NATO's Current C4ISR Capabilities. NATO's C4ISR infrastructure is a hybrid of national contributions and Alliance-owned assets, reflecting the collective action and coordination challenges inherent in coalition warfare.

National Contributions. The majority of NATO's C4ISR capabilities are held at the national level, made available to the Alliance through contributions. These vary significantly due to differences in defence budgets, force structures, and domain specializations:

- United States: The U.S. dominates with advanced platforms in all domains, capabilities and assets. It funds and develops TDLs like Link 11 (1960s, 2.4 kbps) and Link 16 (1980s, up to 115 kbps), used by all Allies for secure data exchange.
- European Allies: Larger nations like the UK, France, and Germany and Italy possess advanced ISR but in lower numbers and reach while smaller Allies rely on tactical-level

[5] Michael A. Palmer, *Command at Sea Naval Command and Control since the Sixteenth Century* (Cambridge, MA: Harvard University Press, 2007).

[6] Norman Friedman, *Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars* (Annapolis, MD: Naval Institute Press, 2009); Barry D. Watts, *Six Decades of Guided Munitions and Battle Networks: Progress and Prospects* (Washington, DC: Center for Strategic and Budgetary Assessment, 2007).

[7] John Stillion and Bryan Clark, *What it Takes to Win: Succeeding in 21st Century Battle Network Competitions* (Washington, DC: Center for Strategic and Budgetary Assessment, 2015).

[8] Mark Denny, *Blip, Ping, and Buzz: Making Sense of Radar and Sonar* (Baltimore, MD: Johns Hopkins University Press, 2007).

systems or NATO assets.[9] European contributions are limited by two decades of underinvestment, with defence spending often below 2% of GDP.
- Domain Disparities: Air domain C4ISR (AEW aircraft) is robust, but land and sea domains lag due to lack of modernization or even phasing out of some capabilities (like anti-submarine warfare patrol aircraft). Space and cyber capabilities are concentrated among a few Allies, with only 10% of members operating ISR satellites.

National contributions include airborne early warning (AEW) aircraft, maritime patrol vessels, surveillance drones, and ground-based C2 systems, shared via Link 11 and Link 16. However, proprietary standards and uneven modernization create interoperability gaps, hindering seamless data fusion.[10]

NATO-Owned Assets. NATO owns a limited but critical set of C4ISR assets, designed to enhance collective situational awareness and interoperability:

- Airborne Early Warning and Control System (AWACS): The E-3 Sentry fleet provides real-time air surveillance and C2, monitoring NATO's eastern flank. Commissioned in the 1980s, AWACS struggles with modern EW threats due to aging technology.
- Allied Ground Surveillance (AGS): Using RQ-4D Phoenix drones, AGS delivers persistent ground ISR, supporting joint operations. Operational since 2021, it enhances NATO's ability to detect threats like missile launches.
- Link 22: Developed under the NATO Improved Link Eleven (NILE) program, Link 22 succeeds Link 11 and complements Link 16. With a 1.2 Mbps bandwidth, it supports complex data (e.g., sensor fusion, imagery) and offers enhanced security and interoperability for maritime, air, and land operations. Adopted by nations like the UK and France, Link 22 is targeted for full integration by 2030.
- Maven Smart System NATO (MSS NATO): deployed in 2025, NATO MSS enhances strategic-level C4ISR through AI-driven data fusion and analytics, processing multi-domain data to support strategic command and control (C2). Built on Palantir's Gotham platform, it integrates ISR from platforms like AWACS and AGS, reducing data overload. MSS NATO complements FMN by standardizing data across national systems, addressing interoperability delays.[11]

These assets are vital but insufficient for major joint operations, relying heavily on U.S.-provided satellite, cyber, and strategic ISR capabilities, which account for 80% of NATO's space-based C4ISR.

Gaps. NATO's C4ISR infrastructure, while unmatched globally, suffers from critical gaps stemming from a fragmented design, where NATO's C4ISR is more a sum of disparate parts than a unified architecture, exacerbated by the transatlantic capability divide. Five gaps and deficiencies deserve attention. Proprietary national systems impede data sharing, delaying joint operations – thus making Allied capabilities less interoperable. Inconsistent cyber and critical infrastructure defences, especially among smaller Allies, expose networks to attacks, as seen in the 2023 undersea cable sabotage. Limited airborne EW platforms leave NATO vulnerable to adversary jamming, such as Russia's GPS disruptions in Ukraine. Slow adoption

[9] Theo Farrell, Sten Rynning and Terry Terriff, *Transforming Military Power since the Cold War: Britain, France, and the United States, 1991–2012* (Cambridge: Cambridge University Press, 2013).

[10] Colin Wall and John Christianson, "Europe's Missing Piece: The Case for Air Domain Enablers," *CSIS Brief* (Washington, DC: CSIS, 2023).

[11] Sydney J. Freedberg Jr., "NATO picks Palantir's Maven AI for military planning, amid trans-Atlantic tension," *Breaking Defense*, April 14, 2025.

of artificial intelligence and machine learning (ML) limits real-time analytics for multi-domain data, projected to reach 175 zettabytes globally by 2025. Finally, aging systems like AWACS require costly upgrades to counter modern threats.

Threats. NATO's C4ISR faces three intertwined threats. First, two decades of European defence budgets below 2 percent of GDP have left legacy platforms obsolete and unable to face near-peer competitors. The diffusion of precision munitions, anti-access/area-denial (A2/AD) capabilities, drones, and advanced EW/cyber capabilities threaten C4ISR assets, potentially disrupting communications and ISR.[12] Finally, industrial-era command structures, with single points of failure, are ill-suited for distributed, digital warfare, risking operational bottlenecks.

First, two decades of European defence budgets below 2 percent of GDP have left legacy platforms obsolete and unable to face near-peer competitors.

The Future of NATO C4ISR. To address these threats, NATO is modernizing its C4ISR infrastructure, embracing Multi-Domain Operations (MDO) to integrate operations across land, sea, air, cyber, and space. MDO enables combatant commanders to fuse multi-domain data, switch between capabilities, and manage escalation, countering adversaries' advanced systems (e.g., air defences, cyber-attacks). Key modernization initiatives include:

- Joint All-Domain Command and Control (JADC2): A U.S.-led initiative, JADC2 integrates all domains via cloud-based networking, AI-driven analytics, and resilient communications (e.g., 5G, quantum-resistant encryption). NATO is aligning with JADC2 principles to replace Link 16 by the 2030s, enhancing bandwidth and interoperability.
- Federated Mission Networking (FMN): FMN standardizes mission-specific networks, enabling rapid data sharing across Allies. Operational since 2015, its 2025 spiral aims to integrate commercial 5G solutions.[13]
- Alliance Future Surveillance and Control (AFSC): Replacing AWACS, AFSC explores space-based sensors and AI analytics to ensure surveillance dominance by 2035.[14]
- Task Force X Naval Drones: Launched in 2025, this uncrewed fleet enhances maritime ISR and protects undersea infrastructure, countering hybrid threats.[15]

These initiatives leverage lessons from Ukraine, where commercial technologies like Starlink and AI-driven drone targeting have bolstered C4ISR resilience. However, modernization faces challenges, including funding disparities, bureaucratic delays, and the need for doctrinal alignment, which are explored in the next section.

[12] Oleg I. Sukharevsky (ed.), *Electromagnetic Wave Scattering by Aerial and Ground Radar Objects* (London: Routledge, 2014).

[13] Frank Gubbels, "NATO's Interoperability Challenge: is FMN on its own?," *Annual Overview 2022* (Utrecht: NATO Command and Control Centre of Excellence, 2023).

[14] Patrick Giesenfeld, "Alliance Future Surveillance and Control How: Will NATO Continue to Effectively Monitor the Skies?," *Joint Air Power Competence Centre Journal*, Vol. 37 (2024): 43-49.

[15] Elisabeth Gosselin-Malo, "NATO trials naval drones in Baltic Sea demo," *Defense News*, February 27 2025.

2. The Challenges Ahead

NATO's C4ISR infrastructure is undergoing a pivotal modernization. However, this transformation faces significant hurdles across politico-strategic, military, technological, and cultural dimensions.

Politico-Strategic Challenges. NATO's politico-military structure grapples with aligning national priorities for collective C4ISR modernization:

- Burden-Sharing Tensions: NATO Allies, reliant on U.S.-provided assets like 80% of space-based ISR, may underinvest in NATO-wide systems for a set of reasons, including budgetary pressures, other priorities or industrial considerations. However, this may create major gaps which would be hard to fill should U.S. capabilities not be available. Additionally, European defence spending seems, overall, to favour visible platforms (jets, tanks and warships) over C4ISR and, even more, digital infrastructure. As a result, initiatives like Federated Mission Networking (FMN) are delayed and, overall, the development of a sufficiently robust C4ISR architecture independent of the United States is hampered. Poland is a case in point: its massive modernization is primarily focused on traditional land capabilities, and thus only marginally it addresses the C4ISR part of the equation.[16]
- Standardization Barriers: Commercial technologies (e.g., 5G, AI) complicate doctrinal and technical alignment. Standards are not neutral and reward some principles, companies and, in turn, some countries (with export and influence) – this is why they are often resisted at the multilateral level.[17] More broadly, different approaches towards standards can hamper NATO-wide efforts: a case in point is the UK's push for proprietary satellite protocols which clashes with France's open-standard advocacy.

> NATO Allies, reliant on U.S.-provided assets like 80% of space-based ISR, may underinvest in NATO-wide systems for a set of reasons, including budgetary pressures, other priorities or industrial considerations.

Military Challenges. Politico-strategic challenges have direct implications on military performance. For instance, several European remotely piloted systems are incompatible with Link 16. Similarly, in NATO's 2024 Baltic Air Policing, 25% of data exchanges required manual workarounds, exposing coordination flaws or delaying operations. Along the same lines, while Ukraine could swiftly integrate Starlink-enabled ISR, NATO's siloed systems struggled to integrate cyber and air data during 2024 Steadfast Defender. At the broader military level, two distinct challenge emerge:

- C2 and expertise: Multi-domain operations require command and control arrangements capable of granting Uber-like availability of capabilities to Combatant Commanders who, in turn, must be fully aware of their performance. Otherwise, NATO cannot plan and execute its MDO operations. Devising such arrangements and nurturing a cadre of Commanders with such expertise across all the NATO enterprise and the different national echelons represents a major challenge.[18]
- Cyber and critical infrastructures vulnerabilities: Multi-Domain Operations are designed in theory, to provide a full-spectrum military superiority in all fields and domains. This logic, however, is in tension with strategic competition which aims at exploiting adversaries' vulnerabilities. As NATO and its Allies proceed towards MDO, they will inevitably invite more attacks

[16] Arthur A. Stein, "Coordination and collaboration: regimes in an anarchic world," *International Organization*, Vol. 36, No. 2 (1982): 299-324; Robert O. Keohance, *After Hegemony: Cooperation And Discord In The World Political Economy* (Princeton, NJ: Princeton University Press, 1984); Todd Sandler and Keith Hartley, *The Political Economy of NATO: Past, Present and Into the 21st Century* (Cambridge: Cambridge University Press, 1999).

[17] Phillip Taylor, "Weapons standardization in NATO: Collaborative Security or Economic Competition," *International Organization*, Vol. 36, No. 1 (1982): 95-112.

[18] Andrea Gilli, Mauro Gilli and Gorana Grgić, "NATO, multi-domain operations and the future of the Atlantic Alliance," *Comparative Strategy*, Vol. 44, No. 1 (2025): 73-91.

from adversaries against their cyber and critical infrastructures. 70% of NATO's undersea cables are exposed (as shown by the 2023 Baltic sabotage) and NATO Allies' public administrations are widely unprepared for massive cyber attacks (as highlighted by the April 28 2025 paralysis in Portugal, Spain and France). Investments in resilience not only compete with C4ISR modernization but require the development of different doctrines or corollaries.

- Operations vs preparation: Any organization faces a fundamental trade-off between current and future needs. NATO is no exception, and after three decades of low investments and dealing with asymmetric threats, reconciling this challenge may be daunting, with broader negative effects on NATO coherency among capabilities and armed forces.[19]

Technological Challenges. Technology is not neutral, and technological paths are informed by multiple factors, including culture, political institutions, bureaucratic preferences and factors' endowment (capital vs labor) at the national level. Across the Atlantic, there are significant differences in these areas and such differences are likely to inform different national technological developments which, in turn, could be difficult to integrate at the NATO level.[20]

Any technology requires human operators and as technology takes over functions, human beings grow in importance as their decisions assume greater strategic significance.

- Data: In order to work, C4ISR architectures cannot just be present, they require large libraries of data gathering in different tactical, operational, environmental and adversarial environments. Lacking a comprehensive C4ISR architecture, European countries also lack this type of data and will require extensive time, experimentation and operations to gather.[21]
- Diverging Approaches: Between the Atlantic and even within Europe there are different approaches to digital technologies, spanning from data governance to the very technological underpinnings. Currently, these differences slow down adoption of digital technologies. In the future, should European countries devise different paradigms around for artificial intelligence, such divergence could further complicate integration.[22]
- Culture. Digital transformation disrupts hierarchical culture traditionally characterizing military organizations. In a data-rich world, probabilistic reasoning replaces deterministic decision-making, and data fluency trumps experience.[23]
- Institutions: All NATO and Allies' defence institutions have emerged or been organized in the industrial era. They are thus designed around rigid, vertical and centralized, years-long planning and procedures. This design is, however, increasingly unfit for our digital era, where more flexible, horizontal, decentralized and short-span planning and procedures yield more benefits. Reforming these big bureaucracies require political capital, bureaucratic ingenuity and talented individuals – all factors which may not be easy to access.[24]
- Human capital: Any technology requires human operators and as technology takes over functions, human beings grow in importance as their decisions assume greater strategic significance. At the higher-end level, NATO and its Allies will thus increasingly need a cadre of officers fluent in digital technologies. At the lower end, among others, such officers will need to handle the traditional challenges new technologies generate, including biases about excessive trust and opposition, data overload and unsustainable tempo. [25]

[19] Andrea Gilli, Mauro Gilli and Nicolò Petrelli, "Before Vegetius: Critical Questions for European Defense," *Policy Brief* (Milan: Institute for European Policy Making, 2024).

[20] Donald MacKenzie, *A Historical Sociology of Nuclear Missile Guidance* (Cambridge, MA: The MIT Press, 1990).

[21] Gilli, Gilli and Petrelli, "Rearming Europe."

[22] Giorgio Presidente, "The Technological Paradigm, Stupid," *Policy Brief*, No. 33 (Milan: Institute for European Policy-Making, 2025).

[23] Ethan Mollick, *Co-Intelligence: Living and Working with AI* (London: W. H. Allen, 2024); Edward N. Luttwak and Eitan Shamir, *The Art of Military Innovation: Lessons from the Israel Defense Forces* (Cambridge, MA: Harvard University Press, 2023).

[24] Andrew McAfee, *The Geek Way: The Radical Mindset that Drives Extraordinary Results* (New York, NY: Little, Brown & Company, 2023).

[25] Ajay Agrawal, Joshua Gans and Avi Goldfarb, *Prediction Machines: The Simple Economics of Artificial Intelligence* (Boston, MA: Harvard Business Review Press, 2018); 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).

3. Conclusions

NATO's Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) infrastructure, the linchpin of its military dominance, is at risk of obsolescence without urgent, coordinated action. This paper has assessed NATO's capabilities – national assets like Link 16 and NATO-owned systems like AWACS – revealing critical deficiencies in interoperability, electronic warfare (EW), cyber resilience, and multi-domain operations (MDO) adoption. Interoperability gaps delay 25% of data exchanges, as seen in 2024 Baltic Air Policing. Cyber vulnerabilities expose 70% of undersea cables, and only 40% of NATO forces are MDO-certified, while Ukraine's agile Starlink-enabled ISR is largely unfeasible within NATO, at this stage. European underinvestment and cultural resistance to AI-driven command and control (C2) exacerbate these challenges.

Yet, NATO's modernization initiatives – Joint All-Domain Command and Control (JADC2), Federated Mission Networking (FMN), Alliance Future Surveillance and Control (AFSC), Task Force X Naval Drones, DIANA, and the European Defence Fund (EDF) – offer major-to-transformative potential. Ukraine's integration of commercial technologies and DIANA's 70-company 2025 accelerators demonstrate the power of innovation. To secure its C4ISR edge, NATO must act decisively at the 2025 Summit with three high-impact recommendations:

NATO's C4ISR infrastructure, the linchpin of its military dominance, is at risk of obsolescence without urgent, coordinated action.

- Synergize National and Alliance Investments: Allies must align national C4ISR budgets with NATO's DIANA, EDF, and EU's PESCO initiatives and programs, targeting a 50% European space ISR and EW contribution by 2030. France's CSO satellites and the UK's Skynet show the way, but funding gaps and competing priorities require a NATO-led investment framework to prioritize digital infrastructure over platforms.
- Accelerate AI-Driven C2 Transformation: NATO must achieve 50% AI-integrated C2 by 2030 through MSS NATO and DIANA, scaling Ukraine's AI-driven drone targeting model. This requires overcoming EU GDPR barriers, projected to delay 30% of AI projects, by establishing a NATO-wide data-sharing protocol by 2027 (eventually supported by EDF funding).
- Reform Culture and Procurement: NATO Allies should first agree to reach specific targets in terms of data fluency for their officers by 2027. Second, a concerted effort for decentralizing C2, to mirror Ukraine's junior officer empowerment, should be launched. Finally, NATO should launch an Alliance-wide initiative to reform national procurement for software acquisition.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl