The Hague Centre
for Strategic Studies

Securing the Digital Backbone

NATO's Quest for Interoperability in the Age of Emerging Disruptive Technologies

Hans Horan, Sofia Romansky and Davis Ellison

June 2025

The Hague Centre
for Strategic Studies

Securing the Digital Backbone

NATO's Quest for Interoperability in the Age of Emerging Disruptive Technologies

Authors:
Hans Horan, Sofia Romansky and Davis Ellison

Contributions by:
Emma Genovesi

Series Editor:
Tim Sweijs

June 2025

This HCSS paper is part of a series 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).

The research was made possible through a financial contribution from Microsoft to The Hague Centre for Strategic Studies (HCSS). Responsibility for the contents and for the opinions expressed, rests solely with the authors.

Introduction

In an era marked by mounting geopolitical tensions, NATO's ability to maintain and enhance interoperability among its allies has never been more critical. Central to this effort is the development and refinement of C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) systems, which form the digital nervous system of the Alliance.

Historically, NATO's C4ISR capabilities have enabled it to respond to emerging threats in a timely and unified manner. For example, the Alliance's members' ability to gather and disseminate intelligence ahead of Russia's 2022 invasion of Ukraine demonstrated the importance of robust command and communication structures in preserving deterrence for the alliance members.[1] However, the character of war is now fundamentally reshaped by emerged or emerging disruptive technologies (EDTs) such as artificial intelligence (AI), cyber capabilities, and, in the longer term, quantum computing.[2] To maintain an agile decision-making process, NATO must keep pace with the digital demands of 21st-century warfare, which involves the ability to manage vast and diverse data streams while deploying systems capable of real-time analysis, and dissemination across domains.[3]

Interoperability is frequently neglected in favour of national preferences, resulting in fragmented investments, siloed systems, and underdeveloped digital frameworks.

As such, the imperative to modernise and integrate C4ISR capabilities has become urgent. Contemporary conflicts increasingly demand faster, more agile, and fully integrated network operations across land, air, sea, cyber, and space. Ukraine's effective use of digital-enabled C4ISR systems against a materially superior adversary illustrates that the ability to operationalise information and technology is now as decisive as a force's physical structure or equipment.

Yet, the political, institutional[4], and technological barriers of alliance management often obscure or hinder the integration of these C4ISR capabilities. Interoperability is frequently neglected in favour of national preferences, resulting in fragmented investments, siloed systems, and underdeveloped digital frameworks. These interoperability deficiencies are particularly acute for NATO's European members (hereafter referred to as NATO Europe), many of whom lack secure cloud infrastructure, scalable AI-processing capabilities, and standardised digital architectures. C4ISR systems constitute the foundation upon which credible deterrence and effective military action are built.

1 Kristian Gustafson et al., 'Intelligence Warning in the Ukraine War, Autumn 2021 – Summer 2022', *Intelligence and National Security* 39, no. 3 (15 April 2024): 400–419, https://doi.org/10.1080/02684527.2024.2322214; 'NATO Review - Intelligence Disclosure as a Strategic Messaging Tool', NATO Review, 16 December 2024, https://www.nato.int/docu/review/articles/2024/12/16/intelligence-disclosure-as-a-strategic-messaging-tool/index.html.

2 Rachel Kufakunesu, Herman Myburgh, and Allan De Freitas, 'The Internet of Battle Things: A Survey on Communication Challenges and Recent Solutions', *Discover Internet of Things* 5, no. 1 (10 January 2025): 4, https://doi.org/10.1007/s43926-025-00093-w.

3 Damjan Štrucl, 'Comparative Study on the Cyber Defence of NATO Member States', *NATO CCDCOE*, 2021, 5, https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf; Kavita Sahu et al., 'Military Computing Security: Insights and Implications', *Journal of The Institution of Engineers (India): Series B*, 21 August 2024, 1, https://doi.org/10.1007/s40031-024-01136-6; Imre Porkoláb, 'An AI Enabled NATO Strategic Vision for Twenty-First-Century Complex Challenges', in *Artificial Intelligence and Global Security*, ed. Yvonne R. Masakowski (Emerald Publishing Limited, 2020), 153–65, https://doi.org/10.1108/978-1-78973-811-720201009; Олександр Передрій et al., 'A Conceptual Approach to Improving the Information Support of the Prospective Armed Forces of Ukraine', Міжнародний Науковий Журнал *«Military Science»* 2, no. 1 (3 April 2024): 72, https://doi.org/10.62524/msj.2024.2.1.06.

4 Political barriers stem from conflicting interests and power dynamics among actors, while institutional barriers arise from rigid structures, rules, or processes within organisations or systems.

Within NATO, the effort to achieve actionable interoperability is distributed across several key structures, including the NATO Digital Staff in Brussels,[5] the NATO Communications and Information Agency (NCIA) in Brussels,[6] and the NATO Standardisation Office (NSO).[7] These structures are supported by broader multinational initiatives such as the EU's Robust Communication Infrastructure and Networks project.[8] However, persistent gaps in capabilities and coordination remain regarding technological & capability shortfalls, institutional barriers to transformation, organisational hurdles, and cultural resistance between NATO member states.

To examine these technological, institutional, and organisational barriers, The Hague Centre for Strategic Studies (HCSS) has commissioned a paper series to examine how these barriers have prevented NATO, and particularly its European members, from developing integrated, resilient, and interoperational C4ISR systems, and what solutions can be devised to overcome these them. The series includes *Antonio Calcara's "NATO's Digital Modernisation: The Case of Cloud Computing"*, *Kateryna Bondar's "How Ukraine's War is Reshaping C4ISR for the Modern Battlefield"*, *Andrea and Mauro Gilli's "Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward"*, and *Elsa Kania's* paper *"Command Confrontation: Considering China's Evolving Command Capabilities and Implications for NATO"*.

While NATO has recognised the strategic importance of C4ISR modernisation, the gap between ambition and capability remains wide.

Together, these papers offer a multifaceted perspective on the challenges NATO faces in adapting to a digital battlespace that is increasingly defined by speed, complexity, and technological innovation. This Capstone document synthesises some of the key insights offered in these standalone papers. It assesses NATO's structural C4ISR deficiencies and outlines measures to promote interoperability going forward, providing a comprehensive framing of the problem and a clear agenda for reform.

While NATO has recognised the strategic importance of C4ISR modernisation, the gap between ambition and capability remains wide. NATO's current digital interoperability challenge is further exacerbated by the impact of EDTs on the conduct of contemporary and future war. This paper identifies internal shortcomings, stemming from outdated systems, institutional fragmentation, and cultural resistance, as key factors undermining the Alliance's ability to meet the demands of 21st-century warfare. As such, the following sections proceed by exploring the challenges of EDTs and how they are changing the character of war, NATO's struggles to achieve digital interoperability, and solutions on how NATO can achieve interoperability.

5 'NATO Digital Staff', n.d., https://diweb.hq.nato.int/Pages/NDS.aspx.

6 NATO, 'NATO Communications and Information Agency (NCI Agency)', NATO, accessed 12 May 2025, https://www.nato.int/cps/en/natohq/topics_69332.htm.

7 NATO, 'NATO Standardization Office (NSO)', NATO, accessed 12 May 2025, https://www.nato.int/cps/en/natohq/topics_124879.htm.

8 'Robust Communication Infrastructure and Networks (ROCOMIN) | PESCO', Permanent Structured Cooperation (PESCO), n.d., https://www.pesco.europa.eu/project/robust-communication-infrastructure-and-networks-rocomin/.

The Challenges: Emerging Disruptive Technologies and The Changing Character of War

The accelerating impact of emerging disruptive technologies (EDTs) is reshaping the contemporary battlefield, fundamentally altering the character of conflict.[9] Advances in AI, cyber capabilities, and cloud computing, amongst others, are redefining the speed, complexity, and integration of military operations.[10] In the near future, quantum computing will impact security as well as communication. Central to exploiting these technologies is the development of resilient, digitalised C4ISR networks.[11] Without a resilient digitalised C4ISR, modern multi-domain operations (MDO) - the ability to fight seamlessly across land, sea, air, space, and cyber domains – are highly difficult.[12]

The accelerating impact of emerging disruptive technologies (EDTs) is reshaping the contemporary battlefield, fundamentally altering the character of conflict.

The ongoing war in Ukraine has notably demonstrated the criticality of C4ISR to operational success.[13] As Kateryna Bondar's "How Ukraine's War is Reshaping C4ISR for the Modern Battlefield" paper illustrates, Ukraine's armed forces, despite constrained resources, rapidly adapted their C4ISR capabilities through innovation, decentralisation, and the integration of commercial technologies.[14] Ukrainian forces operationalised cloud-based battlefield management systems to gain strategic advantages on the battlefield.[15] Systems such as Delta enabled decentralised command structures, leveraged AI-driven ISR for real-time intelligence, and enforced strict communications discipline to protect vulnerable command nodes.[16]

These adaptations enabled Ukraine to counter a materially superior Russian adversary and maintain operational cohesion across a vast, dynamic front. The Ukrainian experience provides a salient lesson: technological sophistication alone is insufficient without agile,

9 Porkoláb, 'An AI Enabled NATO Strategic Vision for Twenty-First-Century Complex Challenges'.

10 Department of Defense USA, 'DoD Critical Technology Area Transitions: FY2021 – 2024', 2021, https://dod-cta.s3.us-west-2.amazonaws.com/DoD%20CTA%20Transitions_FY2021-2024_Approved%20for%20Public%20Release_2.pdf; Ministry of Defence UK, 'Defence Technology Framework' (Ministry of Defence UK, September 2019), https://assets.publishing.service.gov.uk/media/5d763a3ce5274a27d0fd-d8cf/20190829-DTF_FINAL.pdf; President of the Russian Federation, 'Executive Order on the Scientific and Technological Development Strategy of the Russian Federation', Pub. L. No. 145 (2024), https://gsom.spbu.ru/images/cms/data/29_06_2012_international_week_for_participants_of_chinese_university_of_hong_kong_mba_programs/sd/en_ukaz_o_strategii_nauchn-tehn_razvitiya_rf.pdf.

11 Puneet Bhalla, 'Synergy Journal of the Centre for Joint Warfare Studies', Joint Multi-Domain C4ISR for the Indian Armed Forces, 1, no. 1 (October 2022): 79, https://cenjows.in/wp-content/uploads/2022/11/Synergy-_October_2022_-Online.pdf#page=89.

12 Ludovico Caprio et al., 'NATO MultiDomain Operations: Challenges for the European Land Forces' (The European Land Force Commanders Organisation), 28, accessed 12 May 2025, https://finabel.org/wp-content/uploads/2024/10/FFTPersonal-Paper-Format-copia-1.pdf.

13 Andrea Gilli and Mauro Gilli, 'Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward' (The Hague Centre for Strategic Studies, n.d.), 5; Karishma Asthana, 'Top 8 Cloud Vulnerabilities | CrowdStrike', CrowdStrike.com, 26 November 2024, https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-vulnerabilities/.

14 Elsa B. Kania, "Command Confrontation: Considering China's Evolving Command Capabilities and Implications for NATO" (The Hague Centre for Strategic Studies, June 2025).

15 Kateryna Bondar, 'How Ukraine's War Is Reshaping C4ISR for the Modern Battlefield' (The Hague Centre for Strategic Studies, May 2025), 3,7.

16 Bondar, 'How Ukraine's War Is Reshaping C4ISR for the Modern Battlefield'; Paolo Giordano, 'Battlefield Innovation: Ukraine's DELTA System Paves the Way for Allied Interoperability at CWIX24', NATO's ACT, 12 July 2024, https://www.act.nato.int/article/delta-system-cwix/.

human-centric command frameworks and a feedback-driven operational culture.[17] Without resilient, digitally enabled C4ISR systems, even technologically advanced forces are vulnerable to strategic setbacks.

Looking beyond Ukraine, the future trajectory of warfare points to even greater challenges. As Elsa Kania's paper "Command Confrontation: Considering China's Evolving Command Capabilities and Implications for NATO" shows, China's People's Liberation Army (PLA) is pursuing an ambitious agenda of "intelligentised" warfare, integrating AI deeply into command structures to accelerate decision-making and compress the traditional OODA (observe–orient–decide–act) loop.[18]

China's investment in quantum communications and computing suggests an intention to further disrupt traditional military hierarchies of advantage in the coming decades.

The PLA envisions AI-driven command systems that autonomously process intelligence, surveillance, and reconnaissance (ISR) data[19]. Such ISR systems would support operational planning and optimise force coordination, seeking to achieve decision-making superiority over solely human-led systems. Furthermore, China's investment in quantum communications and computing suggests an intention to further disrupt traditional military hierarchies of advantage in the coming decades.[20] These developments underscore the need for NATO members to further enhance their C4ISR frameworks. In addition, it will make sure the Alliance does not fall behind its adversaries' technological advances and remains resilient to the increasing utilisation of AI to outpace human decision-making.[21]

The challenge outlined in the previous sections is magnified for multinational alliances such as NATO, and especially for its European members. Unlike national militaries, alliances must standardise C4ISR capabilities across diverse sovereign actors, disparate industrial bases, and varied strategic cultures.[22] Political sensitivities surrounding data sovereignty, classification levels, and procurement autonomy often hinder technological standardisation.[23] Without a common digital backbone and interoperable C4ISR frameworks, the ability to conduct MDO at alliance scale under the pressures of high-intensity conflict will be critically undermined.[24]

17 Bondar, 'How Ukraine's War Is Reshaping C4ISR for the Modern Battlefield', 1,3,6,9; Kateryna Bondar, 'Closing the Loop: Enhancing U.S. Drone Capabilities Through Real-World Testing', 21 January 2025, https://www.csis.org/analysis/closing-loop-enhancing-us-drone-capabilities-through-real-world-testing.

18 Kania, "Command Confrontation: Considering China's Evolving Command Capabilities and Implications for NATO", 1–11.

19 Tye Graham and Peter W. Singer, 'New Products Show China's Quest to Automate Battle', Defense One, 2 March 2025, https://www.defenseone.com/threats/2025/03/new-products-show-chinas-quest-automate-battle/403387/.

20 'China's Long View on Quantum Tech Has the US and EU Playing Catch-up | Merics', 14 December 2024, https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch.

21 Kania, "Command Confrontation: Considering China's Evolving Command Capabilities and Implications for NATO", 1,7,8,11.

22 Aagachi, 'In Brief: C4ISR - A Five-Step Guide to Maintaining NATO's Comparative Military Edge over the Coming Decade', *Atlantic Council* (blog), 16 March 2023, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/in-brief-c4isr-a-five-step-guide-to-maintaining-natos-comparative-military-edge-over-the-coming-decade/; Andrea Locatelli, 'The Technology Gap in Transatlantic Relations: A Cause of Tension or a Tool of Cooperation?', *Journal of Transatlantic Studies* 5, no. 2 (1 September 2007): 133–54, https://doi.org/10.1080/14794019908656860; Tim Sweijs, 'Maintaining NATO's Technological Edge' (The Hague Centre for Strategic Studies, 2019), https://hcss.nl/report/maintaining-natos-technological-edge/; Tim Sweijs, 'Reinvigorating NATO's Edge: Military Innovation and the Strategic Concept', GLOBSEC - A Global Think Tank: Ideas Shaping the World, 19 May 2022, https://www.globsec.org/what-we-do/publications/reinvigorating-natos-edge-military-innovation-and-strategic-concept.

23 Dennis Broeders, Fabio Cristiano, and Monica Kaminska, 'In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions', *JCMS: Journal of Common Market Studies* 61, no. 5 (2023): 1261–80, https://doi.org/10.1111/jcms.13462.

24 NATO, 'Countering Hybrid Threats', NATOa, 5 July 2024, https://www.nato.int/cps/en/natohq/topics_156338.htm; NATO, 'NATO DIGITAL BACKBONE & NATO DIGITAL BACKBONE REFERENCE ARCHITECTURE' (NATOb, 2024), https://www.nato.int/nato_static_fl2014/assets/pdf/2024/12/pdf/241213-DBRA.pdf.

Considering the aforementioned interoperability challenges, the criteria for success on the modern battlefield is increasingly changing. Indeed, technological investment, rapid adaptation, decentralisation, human-machine integration, and robust command resilience have become the prerequisites for success. Future adversaries are highly likely to increasingly leverage AI and other EDTs to exploit any NATO vulnerabilities in C4ISR speed, integration, and decision-making if they fall behind.[25] As such, to maintain strategic coherence and operational effectiveness, NATO as an alliance must urgently modernise its digital command architecture, institutionalise continuous learning, and build the technical and organisational foundations necessary for alliance-wide interoperability in a transformed conflict environment.[26]

With this framework in mind, any effort to enhance NATO's C4ISR capabilities must begin by confronting the internal challenges that obstruct progress. The next section will focus on these foundational shortcomings, namely technological, institutional, and cultural.

Uneven modernisation efforts and the persistence of legacy platforms have compounded two decades of underinvestment in C4ISR technology in NATO Europe.

The Problem: NATO's Struggle for Digital Interoperability

NATO recognises the urgent need to modernise its C4ISR infrastructure in response to the demands of MDO and emerging disruptive technologies.[27] Despite this recognition, significant deficiencies persist, particularly among its European member states. These challenges span several dimensions: technological and capability deficits related to outdated systems and underinvestment; institutional barriers that stem from divergent national priorities and procurement practices; organisational and cultural resistance within military structures that inhibit agile adaptation; and broader fragmentation across national and industrial boundaries. These aforementioned factors obstruct interoperability and the development of a unified digital backbone.[28]

3.1 **Technological & Capability Shortfalls**

NATO Europe remains critically under-equipped vis-à-vis the essential digital enablers of modern C4ISR. As Andrea and Mauro Gilli's "*Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward"* observed, uneven modernisation efforts and the persistence of legacy platforms have compounded two decades of underinvestment in C4ISR technology in NATO Europe. This has left many European militaries reliant on outdated, nationally fragmented systems that lack the resilience and

25 'China's Long View on Quantum Tech Has the US and EU Playing Catch-up | Merics'; Kania, "Command Confrontation: Considering China's Evolving Command Capabilities and Implications for NATO", 1; Gordon, 'The Future of NATO C4ISR', 4.

26 Paolo Giordano, 'Allied Command Transformation and Innovation: Advancing NATO's Strategic Edge', *NATO's ACT* (blog), 4 April 2025, https://www.act.nato.int/article/act-innovation-advancing-strategic-edge/; Paolo Giordano, 'NATO Centres of Excellence: Powering the Alliance's Digital Transformation', *NATO's ACT* (blog), 2 April 2024, https://www.act.nato.int/article/coes-powering-alliance-digital-transformation/.

27 Gordon Adams et al., *Bridging the Gap: European C4ISR Capabilities and Transatlantic Interoperability*, Defense & Technology Papers (Washington, DC: Center for Technology and National Security Policy, National Defense University, 2004), https://purl.fdlp.gov/GPO/gpo131683.

28 'The Future of EU Cohesion: Scenarios and Their Impacts on Regional Inequalities | Think Tank | European Parliament', 17 December 2024, https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2024)762854.

interoperability demanded by contemporary conflict.[29] NATO Europe has initiated efforts such as the Federated Mission Networking and Alliance Future Surveillance and Control to modernise and connect forces.[30] Nevertheless, these initiatives remain in their early stages and are insufficient to keep pace with the accelerating rate of technological diffusion and adversarial innovation. This insufficiency largely stems from the fact that they often run in standardisation, testing, and validation cycles of 6 months to 1 year, with this cycle excluding the actual implementation phase. As such, such a long cycle is unable to keep pace with the rapid progression of technological transformations, which in cases like AI take every 6 months.[31]

While the US does suffer from significant delays and inefficiencies due to bureaucracy within the Department of Defence (DoD), many European nations still lack secure, scalable cloud architectures, high-performance AI processing capabilities, and standardised digital frameworks.

The capability gap between European allies and the United States is notable. The US possesses more robust C4ISR assets, including integrated airborne surveillance systems, global communications architectures, and AI-enabled decision-support capabilities.[32] While the US does suffer from significant delays and inefficiencies due to bureaucracy within the Department of Defence (DoD), many European nations still lack secure, scalable cloud architectures, high-performance AI processing capabilities, and standardised digital frameworks.[33]

Indeed, Calcara's *NATO's Digital Modernisation: The Case of Cloud Computing* highlights that cloud computing is a critical enabler for storing, processing, and distributing vast data flows necessary for real-time C2. However, it is still unevenly adopted across Europe. Indeed, Europe's diverging national strategies, regulatory inconsistencies, and limited industrial integration hamper progress regarding cloud computing.

Efforts to develop new combat cloud infrastructures, such as Europe's Future Combat Air System (FCAS) and the Global Combat Air Programme (GCAP), risk creating stovepiped solutions that are not interoperable across NATO. This is especially true unless stringent, early coordination mechanisms are put in place.[34] Without a coherent digital backbone enabling seamless information sharing, situational awareness, and distributed decision-making, NATO Europe will struggle to operate effectively in a future battlefield shaped by speed, decentralisation, and complexity.

While this section has predominantly focused on developments in C4ISR and cloud capabilities for the Alliance, there are other deficiencies related to this that merit equal attention. In particular, improving sovereign European-owned space assets is a necessity to improve C4ISR, due in no small part to the animosity and conflicting interests of the US as of writing, given its primary provider role in European space intelligence. Improved cloud assets can only go so far as the assets they support, and space-based platforms are an area of particular European deficiency and interest.

---

29 Gilli and Gilli, 'Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward', 5–6; M.M. McGreer and K.Y. Jo, 'Global Command and Control System (GCCS) Technical Architecture', in *Proceedings of MILCOM '94*, 1994, 859–63 vol.3, https://doi.org/10.1109/MILCOM.1994.473850; NATO, 'Science & Technology Trends 2023-2043 Across the Physical, Biological, and Information Domains', *NATO Science & Technology Organization* 1 Overview (03/23): 18, 46, 100, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf.

30 Gilli and Gilli, 'Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward', 4.

31 Cliff Saran, 'Microsoft Ignite: AI Capabilities Double Every Six Months | Computer Weekly', ComputerWeekly.com, 20 November 2024, https://www.computerweekly.com/news/366615931/Microsoft-Ignite-AI-capabilities-double-every-six-months.

32 Gordon, 'The Future of NATO C4ISR'; 'House of Lords - European Defence Capabilities: Lessons from the Past, Signposts for the Future - European Union Committee' (UK Parliament, 2012), https://publications.parliament.uk/pa/ld201012/ldselect/ldeucom/292/29203.htm.

33 Andrea Gilli and Mauro Gilli, "Appraising the State of Play of C4ISR Infrastructure within NATO Gaps, Deficiencies and Steps Forward", March 10, 2025, pp.2-4.

34 Antonio Calcara, 'NATO's Digital Modernisation The Case of Cloud Computing' (The Hague Centre for Strategic Studies, May 2025), 4–5.

3.2 **Institutional Barriers to Transformation**

Beyond technological shortfalls, NATO Europe faces deep-seated institutional barriers that inhibit rapid digital transformation. The Alliance's multinational character, while a strategic strength, creates profound complications for C4ISR modernisation.[35] Differences in threat perceptions, national sovereignty concerns, and varying levels of digital maturity among allies hinder the development of standardised frameworks and common procurement strategies. These discrepancies stem from various structural and strategic factors, such as differing national defence budgets, procurement cycles, and levels of political prioritisation for military modernisation. [36]

The Alliance's multinational character, while a strategic strength, creates profound complications for C4ISR modernisation. Differences in threat perceptions, national sovereignty concerns, and varying levels of digital maturity among allies hinder the development of standardised frameworks and common procurement strategies.

However, the aforementioned institutional constraints are not limited to just government decision-making; they also extend to the Alliance's relationship with industry. Such issues lead to uneven adoption of advanced technologies across the Alliance, resulting in capabilities gaps between allies.

3.3 **Cultural Resistance**

The aforementioned technological disparity, rooted in both historical defence investment patterns and divergent national priorities for EDT development, creates operational friction within NATO.[37] The ideal state of C4ISR for NATO member states would be a seamlessly integrated network where all allies can access and contribute to a shared, secure, and real-time information environment. This would mean a system in which intelligence from various sources - satellites, unmanned systems, cyber domains, and open-source intelligence - is instantly processed and analysed using AI-driven tools and disseminated across all command levels of all member states.[38]

Such a system would ensure that decision-makers receive accurate, up-to-date intelligence regardless of their individual defence budgets or technological baselines. Moreover, it would allow allies to communicate with each other on a common basis.[39] This would decrease response times across member states and in MDO, enabling NATO to be proactive instead of reactive to emerging threats.[40] Such a system would represent a nirvana for military organisations.

However, such collaboration remains weak across much of NATO Europe.[41] National security cultures characterised by risk aversion, overclassification, and protectionism constrain defence ministries' ability to collaborate meaningfully with cloud providers, AI developers, and cybersecurity firms.[42] Calcara's "NATO's Digital Modernisation: The Case of Cloud Computing" finds that NATO's cloud initiatives highlight this structural tension between the

35 Gilli and Gilli, 'Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward', 5.

36 'The Future of EU Cohesion'.

37 Sweijs, 'Maintaining NATO's Technological Edge', 116.

38 Aagachi, 'In Brief'; Gordon B. "Skip" Davis, 'Threats and Challenges Shaping Nato C4isr', THE FUTURE OF NATO C4ISR (Atlantic Council, 2023), 4, https://www.jstor.org/stable/resrep48478.6; Gordon B. "Skip" Davis, 'Recommendations: Share, Transform, Implement, Modernize, and Invest', THE FUTURE OF NATO C4ISR (Atlantic Council, 2023), 27–30, https://www.jstor.org/stable/resrep48478.9.

39 Mosoiu Ovidiu and Martin Lulian, 'HOW DOES TECHNOLOGY SUPPORT INTELLIGENCE ANALYSTS' TRAINING?', *Conference Proceedings of »ELearning and Software for Education« (ELSE)* 11, no. 01 (2015): 467–75.

40 NATO, 'Science & Technology Trends 2023-2043 Across the Physical, Biological, and Information Domains'.

41 'JOINT WHITE PAPER for European Defence Readiness 2030' (Brussels: European Commission, 19 March 2025), 16–19, https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf.

42 Gilli and Gilli, 'Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward', 5–6.

need for open, modular cloud architectures and political-industrial dynamics that encourage fragmented national solutions. In the absence of "cooperation by design," where interoperability and joint standards are prioritised from the outset, NATO risks replicating past failures in defence industrial integration.[43]

3.4 **Organisational Hurdles**

Organisational culture within many European militaries further complicates C4ISR modernisation. As Gilli's "*Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward*" paper notes, digitalisation challenges traditional military hierarchies by shifting decision-making authority toward data-driven, decentralised models that prioritise agility over rigid chain-of-command structures. Yet many armed forces remain resistant to delegating decision-making authority to junior leaders, embracing rapid feedback loops, or integrating continuous learning processes.[44] However, Bondor's "How Ukraine's War is Reshaping C4ISR for the Modern Battlefield" paper shows that such decisions have been critical to Ukraine's battlefield success against Russia.[45]

Technological divergence, driven by national preferences, industrial policy, and regulatory conflicts, threatens the cohesion of NATO's digital infrastructure.

Technological divergence, driven by national preferences, industrial policy, and regulatory conflicts, threatens the cohesion of NATO's digital infrastructure. Cloud sovereignty debates, conflicting data protection standards, and incompatible national cloud systems risk turning NATO's digital transformation into a collection of connected, yet siloed, systems rather than a unified architecture.[46] Without urgent political leadership to establish common standards for cloud interoperability, secure data exchange, and AI integration, NATO Europe's digital backbone will remain fractured. Such a scenario will undermine its ability to project a coherent operational force.

The Solution: Building a NATO Fit for the Digital Battlefield

Overcoming NATO Europe's C4ISR deficiencies will require a concerted, multi-dimensional effort. As highlighted by the previous section, a C4ISR solution will require simultaneously addressing technological gaps, institutional barriers, and strategic vulnerabilities. The escalating threat landscape and the demonstrated capacity of adversaries, such as China, to exploit digital weaknesses, means that NATO must urgently invest in building a digital backbone. NATO's solution must be capable of supporting high-velocity, MDO. This section outlines the key areas where action is essential, drawing on lessons from recent conflicts, technological developments, NATO's own pilot initiatives, and the need to drive further cooperation with private industry.

43 Calcara, 'NATO's Digital Modernisation The Case of Cloud Computing', 8–9.

44 Gilli and Gilli, 'Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward', 5–6; William A. Denny, 'Senior Military Leadership in Domestic Operations: An Exploratory Study', *Homeland Security Affairs* (blog), 24 April 2021, https://www.hsaj.org/articles/16927.

45 Bondar, 'How Ukraine's War Is Reshaping C4ISR for the Modern Battlefield'.

46 Clara Riedenstein Landrum William Echikson, Lance, 'Defend in the Cloud: Boost NATO Data Resilience', 30 April 2025, 1–10, https://cepa.org/comprehensive-reports/defend-in-the-cloud-boost-nato-data-resilience/; Vivienne Machi, 'Cloudy Vision: Can NATO's New Deployable Combat System Focus the Field?', Defense News, 14 April 2021, https://www.defensenews.com/battlefield-tech/it-networks/2021/04/14/cloudy-vision-can-natos-new-deployable-combat-system-focus-the-field/.

4.1 Technological Modernisation: Investing in the Digital Backbone

First and foremost, NATO Europe must prioritise comprehensive investment in next-generation C4ISR capabilities. This necessitates upgrading sensors, communication nodes, and surveillance platforms.[47] However, it also requires that these assets be seamlessly integrated through resilient, federated cloud infrastructures. As highlighted by Calcara's findings, cloud computing is a critical enabler for real-time data collection, processing, and dissemination across multiple domains. NATO's Allied Software for Cloud and Edge (ACE) initiative and the broader NATO Digital Backbone initiative represent crucial steps forward.[48] Nevertheless, successful implementation demands full commitment by European members to guarantee interoperability by streamlining standards and implementing a holistic security model to embed scalability and redundancy from the outset.

First and foremost, NATO Europe must prioritise comprehensive investment in next-generation C4ISR capabilities.

In addition to this, adopting a multi-cloud strategy is critical.[49] Entrusting NATO's digital infrastructure to a single provider or national cloud heightens the risk of technical vulnerabilities and/or political tensions hindering NATO's interoperability. As the NATO Cloud Conference and pilot projects have suggested, the Alliance should pursue a modular, open architecture built on interoperable APIs. This would enable multiple providers to contribute while maintaining system resilience.[50] This modular approach would also allow rapid integration of innovative civilian technologies, an area where Ukraine's wartime adaptations have proven highly effective.[51]

Meanwhile, NATO Europe must also accelerate AI integration into C4ISR processes to further ensure it maintains an operational advantage over strategic rivals. Indeed, AI-enabled decision support, autonomous ISR processing, and predictive analytics can significantly enhance the alliance's operational speed and accuracy.[52] However, the development of AI applications must be grounded in ethical principles and maintain stringent human oversight.[53] These protocols would avoid vulnerabilities such as AI-related false flags that lead to unnecessary conflict escalations or AI-enabled cyber exploitation by foreign hacking groups.

4.2 Institutional Reform: Bridging the Public-Private Divide

Despite the necessity of this improvement, technological investment alone will not suffice. NATO must fundamentally reform its institutional approach to digital transformation, namely by strengthening its public-private cooperation.[54] Traditional procurement protocols and rigid security cultures within the public sector have proven too slow to keep pace with the

47 Gilli and Gilli, 'Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward', 2–7.

48 Calcara, 'NATO's Digital Modernisation The Case of Cloud Computing', 4; NATO, 'NATO DIGITAL BACKBONE & NATO DIGITAL BACKBONE REFERENCE ARCHITECTURE'.

49 NATO, 'NATO Cloud Conference Advances Innovation and IT Security across the Alliance', NATO, 21 January 2025, https://www.nato.int/cps/en/natohq/news_232539.htm.

50 Calcara, 'NATO's Digital Modernisation The Case of Cloud Computing', 5–7.

51 Calcara, 4.

52 Jeffrey Erickson, 'The Role and Benefits of AI in Cloud Computing', OCI, 21 June 2024, https://www.oracle.com/artificial-intelligence/ai-cloud-computing/.

53 J. Eaton and D.F. Reding, 'Science & Technology Trends 2020-2040 Exploring the S&T Edge', NATO, March 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

54 NATO, 'NATO-Private Sector Dialogues Focus on NATO 2030 Initiative', NATO, 6 February 2021, https://www.nato.int/cps/en/natohq/news_184601.htm.

commercial technology sector's innovation progress. As underscored by Kateryna Bondar's "How Ukraine's War is Reshaping C4ISR for the Modern Battlefield" paper vis-à-vis Ukraine's experience, agile partnerships with the private sector and civil society can deliver operational advantages even under extreme conditions.[55]

As such, NATO and its European members should establish more agile acquisition models, incentivise experimentation with emerging technologies, and create protected innovation pathways. These mechanisms should not only fund cutting-edge developments but also ensure rapid field-testing and adaptation, bridging the gap between promised theoretical concepts and practical solutions that can be deployed on the battlefield.

The Alliance's digital transformation must be treated as a core strategic tenet, not a procedural byproduct.

Furthermore, these solutions and reforms must address cultural or internal political barriers within military organisations. Most notably, data literacy, digitally enabled collaborative decision-making authority, and iterative learning processes must be institutionalised across NATO's European forces. Command structures should empower junior leaders to exploit dynamic ISR capabilities and operationalise AI insights to adapt and adjust tactics in real time vis-à-vis geopolitical flashpoints.[56]

4.3 **Shifting Cultural Attitudes**

The Alliance's digital transformation must be treated as a core strategic tenet, not a procedural byproduct. Indeed, NATO Europe must embed "cooperation by design" into all major capability development programmes. This will entail early alignment of national investments in the Alliance's transformation. Moreover, it will require coordinated strategic planning among allies, as well as military staff and defence planners in Brussels, to ensure joint implementation of C4ISR technology and the establishment of joint standards for cloud computing, AI governance, cybersecurity, and ISR integration. One area that could help bring such systems to reality is increased public-private collaboration, as it is essential for keeping pace with the speed of commercial technological innovation.

In addition, the roles of the NCIA and NSPA in digital operations, cloud interoperability, procurement, and AI ethics could drive continuous Alliance-wide innovation, testing, and standardisation. However, this could potentially require a move away from consensus-based governance. Nevertheless, European states must mitigate nationalistic fragmentation in their investments in combat cloud, ISR, and AI.[65] These efforts will ensure that NATO's strategic advantage in the digital age emerges from its collective capabilities, rather than being unilaterally held by a single ally.

4.4 **Strategic Integration: Building an Interoperable System**

To ensure holistic integration, NATO Europe must treat digital transformation as a collective venture, not a series of separate, uncoordinated national projects. As Gilli's paper "Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward" stresses, uncoordinated national strategies and capabilities threaten to fragment the Alliance's digital architecture unless interoperability is prioritised from the outset.[57]

55 Bondar, 'How Ukraine's War Is Reshaping C4ISR for the Modern Battlefield', 5–6.

56 Gilli and Gilli, 'Appraising the State of Play of C4ISR Infrastructure within NATO: Gaps, Deficiencies and Steps Forward', 7.

57 Gilli and Gilli, 2.

Standardised data formats, cybersecurity protocols, and cloud frameworks must be developed, maintained, and enforced collectively across all member states.

This means embedding cooperation among allies into the design of all digital modernisation efforts within the Alliance. Indeed, interoperability must be treated as a strategic imperative, not an afterthought. This embedded cooperation will be critical for aspects ranging from cloud procurement and ISR platform upgrades to AI model training and battlefield communications systems. Indeed, this approach would mitigate the potential of technical fragmentation and enhance collective resilience within the Alliance. In addition, this approach will severely mitigate the risk of an attack on one node or national system disabling the broader Alliance's ability to operate.[58]

This means embedding cooperation among allies into the design of all digital modernisation efforts within the Alliance. Interoperability must be treated as a strategic imperative, not an afterthought.

NATO should also establish standing bodies to ensure that these processes are conducted promptly and in a coordinated manner. These bodies would be focused on continuous digital interoperability testing, AI governance, and cyber-resilience stress-testing. To achieve this, these bodies would run regular exercises on newly integrated technologies (e.g., EDTs) and cloud architecture into operational plans. This would ensure that Alliance-wide standards evolve dynamically as technology advances.

In addition to embedding cooperation among allies into the design of all digitalisation modernisation efforts, it is equally important to sync these efforts with increased cooperation with private industry (including commercial providers, defence integrators, and SMEs). Indeed, the aforementioned long procurement cycles and governments' risk-averse nature towards research and development (R&D) mean that they are always behind the latest cutting-edge innovations. In contrast, public firms' less bureaucratic nature always allows for a more agile approach to innovation, making this an ideal partnership for ensuring Alliance-wide technological advances. This partnership, with the government taking on an advisory type of role, would allow the Alliance to tailor-make their C4ISR requirements but at a cheaper cost and create secure-by-design, plug-and-play solutions.[59]

58 Peter Andrysiak and Bryan Quinn, 'Empowering the Combatant Commands Is Critical for the Future Fight', War on the Rocks, 10 December 2024, https://warontherocks.com/2024/12/empowering-the-combatant-commands-is-critical-for-the-future-fight/; Calcara, 'NATO's Digital Modernisation The Case of Cloud Computing', 5–7.

59 Whitney M. McNamara, Peter Modigliani, and Tate Nurkin, 'Commission on Software Defined Warfare', Final (Atlantic Council, March 2025), https://www.atlanticcouncil.org/wp-content/uploads/2025/03/Commission-on-Software-Defined-Warfare-Final-Report.pdf.

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