Counting on the Cloud?

NATO, Digital Modernisation and Cloud Computing

Daniel Fiott &
Antonio Calcara

CSDS IN-DEPTH PAPER
no. 17

July, 2025

VUB
BRUSSELS SCHOOL OF GOVERNANCE
CENTRE FOR SECURITY, DIPLOMACY AND STRATEGY

CSDS In-Depth Papers provide critical reflections on issues that affect European security and Europe's partners. The Papers are dedicated to providing analytical insights on specific diplomatic, strategic and security challenges.

The **Centre for Security, Diplomacy and Strategy (CSDS)** seeks to contribute to a better understanding of the key contemporary security and diplomatic challenges of the 21st century – and their impact on Europe – while reaching out to the policy community that will ultimately need to handle such challenges. Our expertise in security studies will seek to establish comprehensive theoretical and policy coverage of strategic competition and its impact on Europe, whilst paying particular attention to the Transatlantic relationship and the wider Indo-Pacific region. Diplomacy as a field of study will be treated broadly and comparatively to encompass traditional statecraft and foreign policy analysis, as well as public, economic and cultural diplomacy. CSDS is based at the Brussels School of Governance at the Vrije Universiteit Brussel (VUB).

Centre for Security, Diplomacy and Strategy
5, Pleinlaan
1050 Brussels
Belgium
csds.vub.be

Cover photo credit: Buddy AN, 2024/Unsplash

Abstract

NATO is enhancing its defence and deterrence in the face of grave geopolitical risks. While the major focus in 2025 is on ramping up the manufacturing of ammunition, missiles, tanks, armoured vehicles and more, there is a risk that the digital elements of the Alliance's security and defence are marginalised or neglected. Indeed, the war on Ukraine highlights how traditional capabilities are being enhanced and complemented by disruptive technologies and innovation. This CSDS In-Depth Paper argues that "digital resilience" needs to be at the heart of defence modernisation efforts across the Euro-Atlantic. It is critical that allies have the ability to store, analyse, exploit and protect data and information. In this regard, the In-Depth Paper investigates how far, and in what manner, NATO is developing cloud computing technologies as part of its broader defence modernisation efforts. Based on the case of cloud computing, the In-Depth Paper aims to uncover the successes and challenges associated with developing cloud interoperability and standardisation across NATO.

Acknowledgement

This In-Depth Paper was made possible due to the support of Microsoft. The views in this publication are those of the authors and do not necessarily reflect the official position of Microsoft.

Executive Summary

This In-Depth Paper assesses the potential for the expanded adoption of cloud computing technologies within and across NATO, and it does so by situating the analysis within the broader context of ongoing military modernisation and digital transformation efforts. Following the NATO Hague Summit in 2025, there is increasing urgency to ensure that the Alliance remains technologically competitive amidst the rapid advancement of adversarial technological and industrial capabilities. Central to this challenge is the need for secure, interoperable and resilient digital infrastructure capable of supporting effective defence and deterrence strategies.

The In-Depth Paper demonstrates that NATO has made significant political and financial commitments to emerging and disruptive technologies, with cloud computing identified as a pivotal enabler across operational, strategic and technical domains. The In-Depth Paper evaluates current progress among NATO and its members in integrating cloud solutions into defence architectures, paying particular attention to the role of cloud services in enhancing interoperability, cybersecurity, situational awareness and logistical coordination.

Key barriers to broader cloud adoption are also examined, including procurement constraints, data sovereignty concerns and regulatory complexity. In response, the In-Depth Paper offers a series of targeted policy recommendations to facilitate the implementation of a federated, hybrid multi-cloud architecture within NATO, fully in line with NATO's own stated digitalisation objectives. These include promoting shared standards, streamlining defence procurement processes, leveraging existing instruments such as DIANA and the NATO Innovation Fund and fostering innovation ecosystems that include commercial and start-up actors.

The analysis further highlights the strategic utility of cloud platforms in areas such as AI-enabled intelligence fusion, real-time data analytics, force readiness simulations and multinational information-sharing frameworks. It calls for expanded use of cloud-based environments to support training, war-gaming and multi-domain operations, underpinned by strengthened cybersecurity protocols and shared data governance mechanisms.

Ultimately, this In-Depth Paper argues that the effective uptake of cloud technologies is essential for NATO to maintain a credible defence posture in the digital age. The conclusions and recommendations presented herein are intended to inform policy deliberations following the 2025 Hague Summit, particularly in relation to burden-sharing, technological innovation and collective resilience in an era of accelerating strategic competition.

Contents

Introduction

NATO is enhancing its defence and deterrence in the face of grave geopolitical risks. Conflict and tensions are on the rise and governments and institutions are investing in the defence capabilities and infrastructure needed to support the Alliance's armed forces. The stakes for NATO could not be higher. Strategic technologies have become one of the hallmarks of power in the 2020s, and technology plays a fundamental role in the rising strategic competition between the United States (US) and China. This is an era where military modernisation is as much about adaptation to the digital world as it is about whether cutting-edge military capabilities can be developed in time. Furthermore, undergirding military capabilities is an intricate supply chain of components, technologies, data and information that needs to be secured and utilised effectively. China is moving at breakneck speed to develop and integrate emerging and disruptive technologies (EDTs) such as artificial intelligence (AI) and quantum computing for military purposes, while also instrumentalising critical raw materials and supply chains. Close partners in the Euro-Atlantic region, such as Australia, Japan and the Republic of Korea are also investing in EDTs. Russia continues to pursue a strategy of defence technological modernisation, despite its war effort in Ukraine.

Therefore, while the major focus in 2025 is on ramping up the production of ammunition, missiles, tanks, armoured vehicles and more, the digital elements of the Alliance's security and defence should not be marginalised or neglected. Given resource constraints, it is tempting to prioritise short-term readiness over long-term innovation (and vice-versa), but this form of dichotomy should be rejected as NATO needs readiness and innovation[1]. If anything, the war on Ukraine highlights how traditional capabilities are being enhanced and complemented by disruptive technologies and innovation. Ukraine is a conflict marked by both a "traditional" war including artillery, tanks and jets and a "future" war including AI, cloud computing and hypersonic missiles – the two forms of warfare are being integrated in Ukraine, which is having operational and technological consequences. Fortunately, NATO has a long tradition of integrating and utilising critical technologies for defence. For example, in February 2021 NATO Defence Ministers endorsed a strategy for EDTs such as AI and quantum computing. The NATO Advisory Group's annual reports on EDTs, plus Allied Command Transformation (ACT) and the Science & Technology Organization's (STO) regular assessments, play a continued and critical role in helping NATO mitigate technology risks and utilise innovation to maintain the Alliance's military edge.

[1] Calcara, A., Gilli, A. and Gilli, M., "Short-Term Readiness, Long-Term Innovation: the European Defence Industry in Turbulent Times", Defence Studies, 23(4), 2023: pp. 626-643.

> **In an era where adversaries are rapidly developing electronic warfare capabilities, the idea that NATO forces should be able to securely exchange information and data is a compelling one**

For NATO, a core challenge is being able to keep up with the technological pace set by China and other adversaries. As the NATO Strategic Concept acknowledges, the Alliance 'will promote innovation and increase our investments in emerging and disruptive technologies to retain our interoperability and military edge'[2]. NATO's Digital Transformation Plan also explicitly highlights the need for a secure and scalable cloud environment as the digital backbone of the Alliance[3]. To this end, NATO calls on allies to engage in deeper defence technology cooperation in order to enhance military interoperability and standardisation. The importance of these factors has been reiterated at the Madrid[4], Vilnius[5], Washington[6] and Hague[7]

---

[2] NATO, "NATO 2022 Strategic Concept", 29 June 2022, p. 7. See: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

[3] NATO, "NATO's Digital Transformation Implementation Strategy", 17 October 2024. See: https://www.nato.int/cps/en/natohq/official_texts_229801.htm.

[4] The NATO Madrid Summit declaration of 29 June 2022 recognised that the Alliance is 'confronted by cyber, space and hybrid and other asymmetric threats, and by the malicious use of emerging and disruptive technologies'. See: https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

[5] The NATO Vilnius Summit communiqué of 11 July 2023 underlined that NATO's 'capability development plans will ensure that we maintain our technological edge, recognising the challenges and opportunities presented by emerging and disruptive technologies, while ensuring their timely integration'. See: https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

[6] The NATO Washington Summit declaration of 10 July 2024 stressed that the Alliance is accelerating its 'transformation to meet current and future threats and to maintain our technological edge, including through experimentation and more rapid adoption of emerging technologies, and through digital transformation'. See: https://www.nato.int/cps/en/natohq/official_texts_227678.htm.

[7] The NATO Hague Summit declaration of 25 June 2025 stressed that it is NATO's 'shared commitment to rapidly expand transatlantic defence industrial cooperation and to harness emerging technology and the spirit of innovation to advance our collective security'. See: https://www.nato.int/cps/en/natohq/official_texts_236705.htm.

Summits – thus, NATO has underlined the growing importance of EDTs to the Alliance at every official occasion. We should also acknowledge that the NATO Defence Industry Summit in August 2024 resulted in a Memorandum of Understanding for Allied Software for Cloud and Edge (ACE), which aims to improve communications and data sharing.

Although NATO continues to promote the importance of Allied cooperation on EDTs, there is currently a lack of precision and clarity in how specific EDTs can impact defence modernisation efforts. On the one hand, there is a powerful logic that the use of EDTs to enhance interoperability between NATO's armed forces will pay dividends for the strength of the Alliance. For example, investing in cloud computing, quantum computing or AI-enabled systems can enhance military command and control (C2) functions or improve military communications. NATO initiatives such as the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund (NIF) have been created for such purposes. In an era where adversaries are rapidly developing electronic warfare capabilities, the idea that NATO forces should be able to securely exchange information and data is a compelling one. On the other hand, however, there could be a risk that more connectivity results in greater vulnerability as adversaries look for ways to disrupt the Alliance's electronic warfare capabilities and C2. Absorbing technologies from private or non-traditional defence companies may create additional entry points for vulnerability, even though steps are needed to attract such firms into the defence sector.

> **"digital resilience" needs to be at the heart of defence modernisation efforts across the Euro-Atlantic region**

In essence, therefore, NATO's ability to make full use of EDTs such as cloud computing is part of a wider balance between a more "federated" interoperable system and the need to ensure sovereign control over digital assets. To better understand this balance, this CSDS In-Depth Paper looks at the specific case of cloud computing. Cloud computing promises to revolutionise defence by providing enhanced data collection and usage methods to improve Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and enhance logistics, defence management and more. Cloud computing also is an

enabling technology that can help realise the full potential of AI. The cloud's scalability and flexibility make it an ideal platform for running AI algorithms, enabling the analysis and processing of vast amounts of data. Therefore, the paper investigates how far, and in what manner, NATO and its allies are developing cloud computing technologies as part of their overall defence modernisation efforts. The paper aims to uncover the successes and challenges associated with developing cloud interoperability and standardisation across NATO. We propose to address the case of cloud computing because of its relevance to the gathering, storing, analysis and fusion of military-relevant data. Furthermore, cloud computing in many ways highlights the growing importance of multi-domain operations, which presupposes the need for the interoperability of military units (from all military branches) within and between allies.

In this regard, this In-Depth Paper addresses the following four questions based on the case study of cloud computing:

1. What is the relevance and importance of cloud computing for defence and deterrence?

2. What is the current state of NATO's defence modernisation efforts and digital agenda?

3. How are individual allies developing or acquiring cloud computing platforms and services?

4. What are the opportunities and challenges of moving towards a more "federated" or interoperable cloud architecture at the NATO level?

Through this analysis, the In-Depth Paper shows that cloud computing can afford NATO allies a cutting technological edge in situational awareness, military communications and data superiority in wartime. This can serve as an effective element of deterrence. The paper assesses how any Alliance-wide cloud computing initiative can be interoperable with the growing national public cloud initiatives, and that national approaches do not adversely affect interoperability within the Alliance. By focusing on these inter-related questions based on the case of cloud computing, the paper aims to provide insights into how sovereign control over digital assets can be managed in a more interoperable way. The paper also seeks to investigate the possibilities of enhancing flexibility in areas such as data mobility between NATO allies. In this respect, the paper provides an analysis of allies' positions on data exchange within an Allied context, and it scopes out the possibilities for and characteristics of a NATO data mobility standard.

This discussion has wider policy implications for NATO's overall digital defence agenda. In particular, this In-Depth Paper sheds light on the

potential role NATO can play in encouraging its allies to develop further interoperable digital services. Relatedly, given the central role of the private and tech sectors in developing EDTs, the conclusions of this paper consider the challenges and opportunities associated with a greater role for private actors in defence modernisation efforts. Finally, the paper reflects on the implications of the study for NATO's overall defence planning and capability planning processes. Overall, the In-Depth Paper argues that "digital resilience" needs to be at the heart of defence modernisation efforts across the Euro-Atlantic region. Allies must have the ability to store, analyse, exploit and protect data and information.

This In-Depth Paper is organised in four main parts. First, the paper considers the relevance and importance of cloud computing for defence and deterrence. Second, the paper provides a brief overview of NATO's defence modernisation efforts and its digital agenda, and here the paper sets the strategic context for the development of EDTs such as cloud computing. Third, the paper zooms in on the individual cloud computing efforts conducted by NATO allies in order to attain a better understanding of individual sovereign efforts in cloud computing. Fourth, the paper considers the benefits and costs of moving towards a more "federated" or interoperable cloud architecture at the NATO level. The In-Depth Paper ends with conclusions and recommendations for further consideration by policymakers.

Chapter One
Cloud Computing and Defence

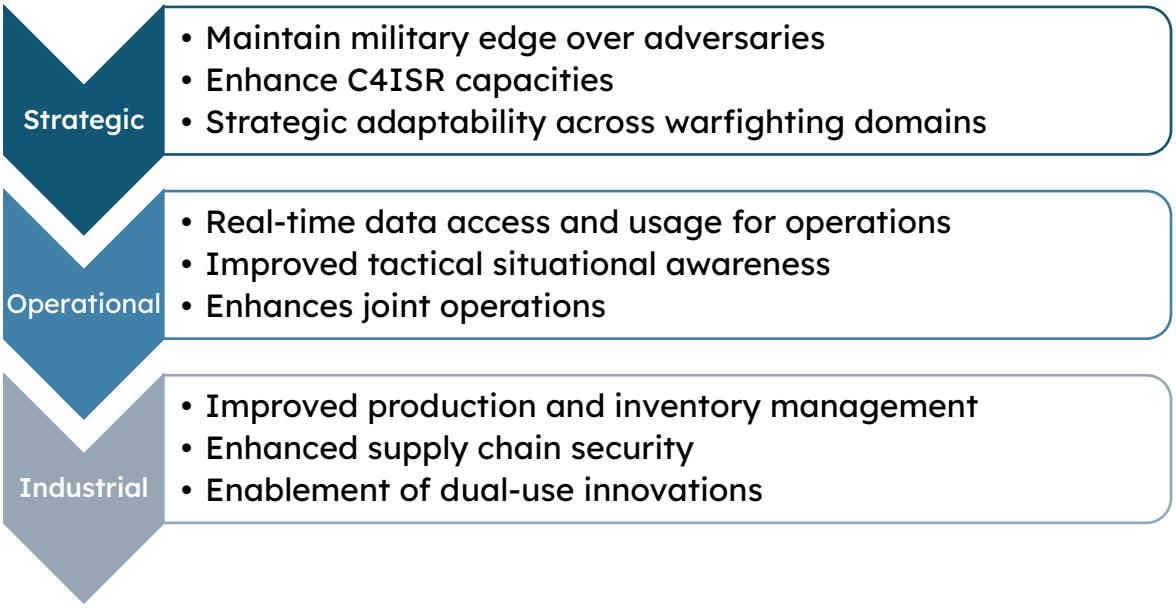
In this first part of the In-Depth Paper we consider the relevance and importance of cloud computing for defence and deterrence. First, however, it is necessary to provide a working definition of the term "cloud computing". In general terms, cloud computing can be defined as a centralised computing service based on the internet to offer users faster and flexible access to data[8]. Cloud computing implies the pooling of information and data that can be accessed on a range of devices such as smartphones or laptops. The benefits of cloud computing include cost-efficiency, scalability, flexibility, accessibility and automation of data storage and usage. Typically, cloud computing services are comprised of servers, storage, databases and networking software and cloud services come in three major forms. First, there are the basic building blocks of cloud services based around an infrastructure (IaaS) of virtual machines, hard drives, networks and data centres. Second, cloud services as a platform (PaaS) include specific tools and platforms for developers to build applications. Third, there is cloud as a software service (SaaS) including ready-to-use software that can be accessed via the web.

For military planners and warfighters, cloud computing can be said to furnish militaries with significant advantages related to 'reliability, commonality, cost, power, scalability, and flexibility of the computing infrastructure over dedicated hardware approaches'[9]. Various parts of the military across Allied nations are already employing cloud computing in vehicles and platforms to help coordinate control and operate systems. For example, the US Joint Warfighting Cloud Capability has in the past awarded contracts to commercial technology companies to furnish the US Department of Defense with commercial cloud services[10]. While these services are largely focused on maintaining efficiencies with logistics, data management, payroll functions, etc., commercial firms have come some distance in providing top secret/classified data management levels of security[11]. For example, Ukrainian forces have been using DELTA as a SaaS system to provide real-

[8] Lele, A., "Cloud Computing", in Lele, A. Disruptive Technologies for Militaries and Security (Springer Nature, 2018): pp. 167-185.
[9] Jedynak, D. "Beyond Victory – Cloud Computing in Military Vehicles", 2013 NIDA Ground Vehicle Systems Engineering and Technology Symposium, 21-22 August 2013. See: http://gvsets.ndia-mich.org/documents/VEA/2013/Beyond%20Victory%20-%20Cloud%20Computing%20in%20Military%20Vehicles.pdf
[10] US Department of Defense, "Contracts for Dec. 7, 2022". See: https://www.defense.gov/News/Contracts/Contract/Article/3239197/.
[11] Microsoft, "Azure Government Top Secret Now Generally Available for US National Security Missions", 16 August 2021. See: https://azure.microsoft.com/en-us/blog/azure-government-top-secret-now-generally-available-for-us-national-security-missions/.

time situational awareness to commands at all levels[12]. We should also recall that in the early stages of the war with Russia, Ukraine used commercial cloud providers to migrate sensitive government data to ensure data continuity while Ukraine's infrastructure was under attack by Russian forces[13].

FIGURE 1: CLOUD COMPUTING – THREE LEVELS



Source: authors' own, 2025

Indeed, based on the existing academic and technical literature, cloud computing can be considered of growing importance for defence and deterrence for strategic, operational and industrial reasons.

Cloud computing: the strategic level

At the strategic level, cloud computing services can help C4ISR and provide militaries with superior detection, information and intelligence abilities. By handling, storing and using data more efficiently through cloud services, militaries can enhance their defence planning, optimise capability development, improve logistics management and develop skills and training. Being able to access and use data in a real-time manner can give militaries a

[12] NATO, "Ukraine showcases battlefield technology at NATO Edge 24", 10 December 2024. See: https://www.ncia.nato.int/newsroom/news/ukraine-showcases-battlefield-technology-at-nato-edge-24.
[13] Microsoft, "How technology helped Ukraine resist during wartime", 20 January 2023. See: https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/.

strategic edge over adversaries through enhanced data fusion, information usage and situational awareness. As one study from the European Defence Agency has implied, the use of a "combat cloud" can also enhance states' ability to operate in kinetic and hybrid environments[14]. What is more, we should not underestimate the cost-saving potential of using cloud services: the enhanced management of logistics and consumables may contribute to cost savings in defence budgets, which could allow additional defence investment in personnel or military capabilities[15].

Cloud computing: the operational level

At the operational level, cloud computing greatly enhance real-time data accessibility and sharing closer to the point of use (e.g. on the battlefield or theatre of operations). Cloud computing allows military personnel across different locations to access and share real-time data, including ISR information[16]. Soldiers operating in contested environments can also use the cloud to process information locally (i.e. at the edge), and therefore increase the chances of making effective tactical decisions. This can be said to help better facilitate collaboration between different branches of the armed forces within and between and Allied nations by supporting unified platforms and data standards. Furthermore, it is important to recognise the "mission adaptability" that can come from the use of cloud computing as it can support a wide range of operations from humanitarian relief, crisis management tasks, rescue and evacuation and high-intensity warfare. The benefit here is that a single cloud platform can be developed and utilised for multiple missions and operations, without the need to replicate or develop new data infrastructures each time.

Cloud computing: the industrial level

At the industrial level, cloud computing is already playing a significant role in how defence firms adapt and modernise their innovation and productive processes. We should also recall that cloud computing is central to all development in AI, as there is no AI without cloud computing and data centres. There are already indications that the use of cloud services can greatly improve the cost efficiency of aerospace and defence firms, by

[14] European Defence Agency, "Cloud Intelligence for Decision Support and Analysis", 25 January 2024. See: https://eda.europa.eu/news-and-events/news/2024/01/25/combat-cloud-eda-study-shows-benefits-of-cloud-computing-for-eu-militaries.
[15] See, for example, Fiott, D., "Digitalising Defence: Protecting Europe in the Age of Quantum Computing and the Cloud", EU Institute for Security Studies, 11 March 2020. See: https://www.iss.europa.eu/publications/briefs/digitalising-defence.
[16] Riedenstein, C., Echikson, W. and Landrum, L., "Defend in the Cloud: Boost NATO Data Resilience", Center for European Policy Analysis, 30 April 2025. See: https://cepa.org/comprehensive-reports/defend-in-the-cloud-boost-nato-data-resilience/.

reducing management and operational costs[17]. Given that NATO is currently supporting the defence sector across the Euro-Atlantic to produce more vital defence equipment, it makes sense that any cost-reducing technology should be considered. What is more, the use of cloud services in the industrial domain can also support greater civil-defence relations and even improve the development of dual-use technologies. There may also be potential upsides to employing cloud services within defence and aerospace startups and SMEs: here, the application of more efficient data handling and usage services may improve the innovation capacity of smaller industrial actors, especially where labour and capital resources may be scarce. NATO and its allies frequently declare they want to harness the innovation potential of start-ups. However, start-ups need cheap and reliable cloud computing power. A "federated" cloud can help lead to economies of scale.

NATO's Defence Modernisation Efforts and the Digital Agenda

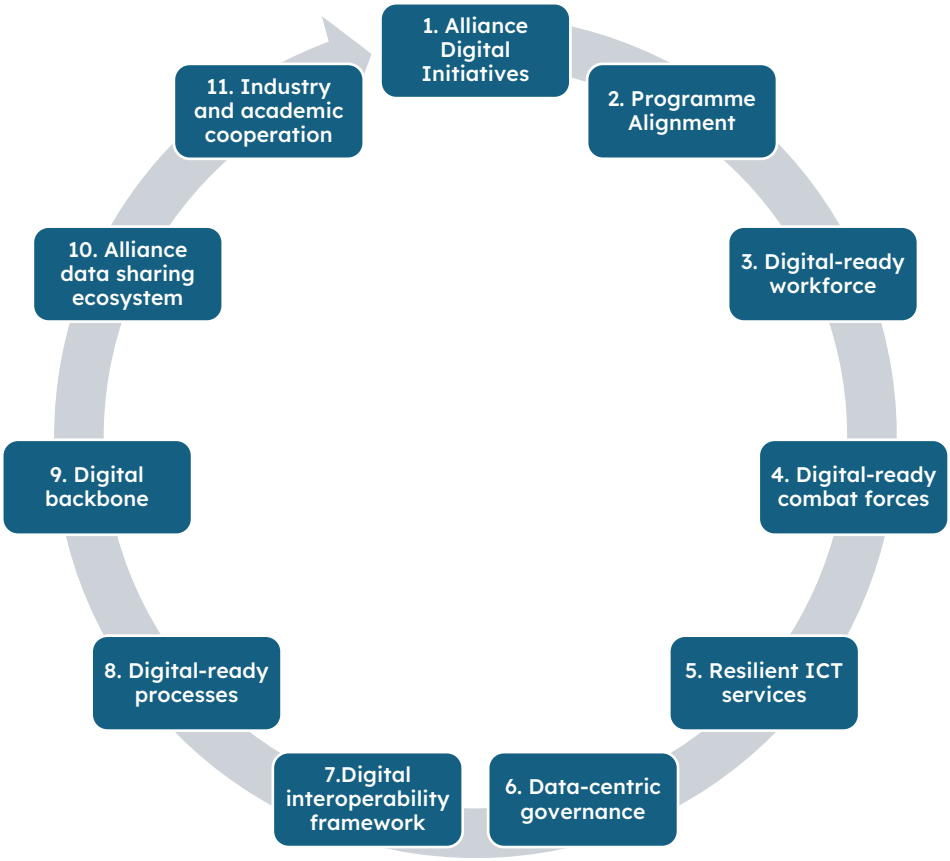
In part two of this paper, we provide a brief overview of NATO's defence modernisation efforts and its digital agenda, and we set out the strategic context for the development of EDTs such as cloud computing. It is argued here that the uptake of cloud computing services is well-suited to NATO's broader defence digitalisation agenda. NATO is undergoing a comprehensive digital transformation to enhance its Multi-Domain Operations (MDO) capabilities by 2030. This transformation aims to ensure interoperability, improve situational awareness and facilitate data-driven decision-making, thereby maintaining NATO's adaptability and readiness in modern warfare. In particular, NATO's 2022 Strategic Concept emphasised the need to maintain the Alliance's technological edge to ensure collective defence and military effectiveness in the information age. To deliver on this objective, NATO produced its "Digital Transformation Vision" in October 2022 and its "Digital Transformation Implementation Strategy" (DTIS), which was approved at the June 2023 NATO Defence Ministers meeting.

The Digital Vision and DTIS outlined the Alliance's path toward adopting technologies to enable MDO, interoperability, enhanced situational awareness and data-driven decision-making[18]. From the outset, the Digital Transformation Vision has sought to leverage modern technologies and close operational gaps, but it recognises that it can only do so over the longer term by bringing together people, processes and technology. This is intended to be an Alliance-wide effort bringing together allies, NATO international staff, industry, innovators and academia. Overall, NATO is embarking on a comprehensive digital transformation in order to remain effective and

[17] Global Data, "The Impact of Cloud Computing on the Defence Industry". See: https://defence.nridigital.com/global_defence_technology_apr23/cloud-computing-impact-defence-industry.
[18] NATO, "Digital Transformation Implementation Strategy", 17 October 2024. See: https://www.nato.int/cps/en/natohq/official_texts_229801.htm.

competitive in future warfare and strategic competition. This will imply a need for greater cooperation between allies, partners and sectors.

FIGURE 2: NATO'S DIGITAL MODERNISATION VISION



Source: authors' own, 2025

To this end, NATO's Digital Transformation Vision seeks to deliver on 11 broad areas of action to: 1) encourage Alliance digital initiatives that are aimed to share national digital innovations (e.g. the Federated Mission Networking (FMN)); 2) align and synchronise NATO capability development initiatives; 3) generate a digital-ready workforce that is skilled and innovation-oriented via training, exchanges and fellowships; 4) create digital-ready and modern NATO forces that can operate effectively in tech-driven, multi-domain environments; 5) ensure that NATO has digital-ready combat forces that can rely on resilient ICT Services, real-time information and analytics; 6) establish robust data management, standards and AI capabilities with proper governance; 7) streamline cross-organisation processes and ensure tech and policy interoperability; 8) reform internal procedures (e.g. procurement, planning) to accelerate technology adoption; 9) create a secure, federated infrastructure (including cloud, AI, edge computing) that integrates all domains; 10) promote secure, responsible and widespread data sharing

across NATO, allies and partners; and, 11) deepen collaboration with external experts in areas like data science, AI, quantum computing, space technology and cybersecurity.

When analysing these 11 broad areas of action, it becomes clear that NATO seeks to use technologies such as cloud computing and other EDTs to achieve operational supremacy across all domains (i.e. land, air, sea, cyber, space)[19]. In particular, NATO recognises that its digital modernisation strategy can only be successful if at least three of the 11 major areas are rapidly and ambitiously pursued: these areas concern the Alliance Data Sharing Ecosystem, the Digital Backbone and the Digital Interoperability Framework.

The Digital Backbone will include federated networks, cloud computing and a service-oriented architecture

The "Digital Backbone" will be developed in line with the Strategic Concept and its key requirement areas. To meet the demands of modern missions and operations – both in peacetime and wartime – the Alliance seeks to develop data-centric, interconnected systems that can integrate securely across organisational and national boundaries. The Digital Backbone hopes to provide the technical infrastructure to ensure seamless connectivity and data exchange, not only across traditional domains (maritime, land and air), but also in emerging domains such as space and cyberspace. By better connecting decision-makers across military and political levels, the Digital Backbone is designed to enhance real-time collaboration and enable users to access and process data securely and efficiently at all levels. It is foreseen that the key components of the Digital Backbone will include federated networks, cloud computing and a service-oriented architecture.

The "Digital Interoperability Framework" is designed to strengthen the governance of Allied digital interoperability. It calls for a unified approach to allow willing allies to provide, federate and manage digital services, while addressing critical areas of shared concern such as security, data governance and protection. NATO hopes that digital interoperability will

[19] NATO Allied Command Transformation, "Empowering NATO's Multi-Domain Operations Through Digital Transformation", 16 October 2023. See: https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/.

extend beyond the adoption of new technologies to also encompass innovation, acquisition, operational integration and the sustainment of legacy systems. NATO believes that implementing a robust Digital Interoperability Framework will enhance the quality of data services, fostering an environment where NATO entities and allies can collaborate effectively and federate services. Moreover, NATO wants to use the interoperability framework to ensure that industry plays a vital role in defining the standards required to achieve full digital interoperability across the Alliance.

The "Alliance Data Sharing Ecosystem" (ADSE) is designed to ensure the systematic and effective sharing of data across the Alliance. NATO seeks to establish interoperable data sharing as a standard practice and a collective responsibility across NATO and Allied nations. Here, NATO seeks to enhance data exchange with industry and academic research partners to foster a broader ecosystem of innovation and collaboration. Specifically, NATO sees a need to overcome organisational silos and build upon the existing culture of cooperation among established communities. NATO also wants to promote the NATO Core Data Framework[20] and data sharing best practices based on NATO's Principles of Responsible Use of Artificial Intelligence and Data[21]. Additionally, NATO seeks to utilise existing initiatives such as DIANA and the NIF to promote innovation in the area of data sharing.

Following the DTIS, the Alliance was quick to seize the momentum on the digital agenda and, in February 2025, the North Atlantic Council approved NATO's Data Strategy for the Alliance (DASA). The DASA was produced to underline the Alliance's commitment to leveraging data as an 'enduring strategic asset' and to ensure that the Alliance meets its data curation, governance and workforce skills objectives by 2030[22]. Significantly, the DASA is seen as a complementary initiative alongside the ADSE and Digital Backbone and NATO hopes that it will support efforts to 'shift from isolated, private data repositories to shared data spaces and federated data

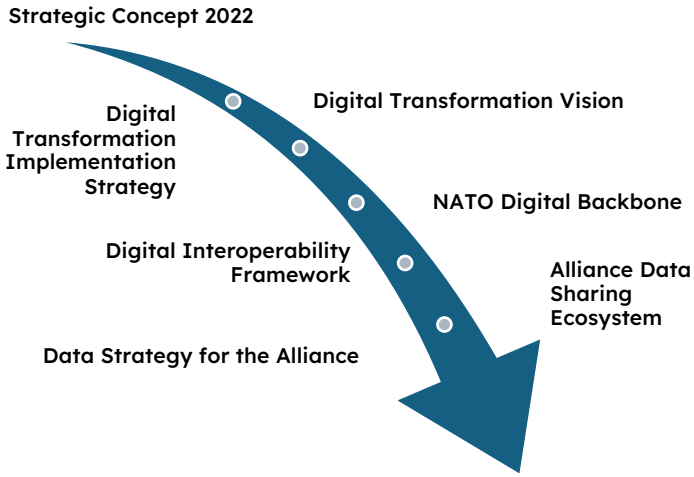
[20] The NATO Core Data Framework aims to enable NATO to leverage data as a strategic resource. The framework aims to enhance awareness on data in the Alliance as well as to improve existing initiatives, policies and programmes with data science processes. The Framework has three strategic goals including: 1) people – to ensure that NATO staff are aware and ready for data usage; 2) processes – ensure coherence between policies across the Alliance for data exploitation; and 3) technology – create a single environment in the Alliance for secure and well-governance data management. See: https://www.nato.int/cps/en/natohq/official_texts_210002.htm.

[21] NATO developed an AI Strategy in 2021 to promote its 6 principles of responsible use for AI including: lawfulness, responsibility and accountability, explainability and traceability, reliability, governability and bias mitigation. NATO released a revised AI Strategy in 2024 to include greater direction for how AI can feature in the NATO Defence Planning Process, how to develop AI capabilities via DIANA and much more. See: https://www.nato.int/cps/en/natohq/official_texts_227237.htm.

[22] NATO, "Data Strategy for the Alliance", 5 May 2025. See: https://www.nato.int/cps/cn/natohq/official_texts_234937.htm.

meshes'[23]. Overall, the DASA contains five main strategic objectives including the need for: 1) clear, coherent and consistent data governance principles; 2) distributable and consumable data products; 3) protected data sources; 4) accessible and relevant data access to drive decision-making; and 5) sharable and exploitable data. The DASA goes on to state that the four major enablers of these objectives are: 1) data governance and frameworks; 2) interoperable data architectures; 3) modern data standards; and 4) data talent and culture.

FIGURE 3: NATO'S CLOUD COMPUTING EFFORTS



Source: authors' own, 2025

In addition to the DTIS and DASA, NATO has also taken concrete steps to help develop Allied cloud capacities. For example, at the July 2024 NATO Summit Defence Industry Forum, 22 NATO Defence Ministers signed a letter of intent on "Allied Software for Cloud and Edge" (ACE). By signing the ACE letter of intent, the 22 allies agreed to step up efforts to integrate Allied software solutions for cloud and edge computing technologies. ACE aims to develop a standardised cloud model to minimise security risks and ensure higher interoperability between the signatories[24]. NATO has sought to complement ACE with regular exchanges such as the 21-22 January 2025 NATO Cloud Conference. This gathering, held in Brussels, brought together 25 European industry leaders and IT service providers with NATO decision-makers to develop strategies for 'secure cloud-based solutions for handling

[23] Op.Cit. "NATO Data Strategy for the Alliance".
[24] NATO, "Allies launch strategic initiatives to enhance capabilities", 9 July 2024. See: https://www.nato.int/cps/en/natohq/news_227472.htm?selectedLocale=en.

highly classified information'[25]. The Cloud Conference was specifically organised to help with the acquisition process under ACE so that allies can start to procure the first Alliance-wide classified cloud capability[26].

Finally, through its Data Centric Reference Architecture for the Alliance[27], NATO has made clear that it seeks to deliver an Alliance secure and scalable cloud environment. Such a course of action is based on 6 major provisions including: 1) cloud-based innovation platforms to create industry capabilities in big data and advanced analytics; 2) federated cloud services that combine edge computing, to form an "Alliance Combat Cloud"; 3) an Alliance data sharing ecosystem to enable the storage, registration and management of quality data; 4) accelerated delivery of cloud solutions to NATO; 5) the exploration and development of trusted Big Data anonymisation technology; and 6) revised regulation[28]. While all of these efforts are ambitious and relatively new, NATO has experience in developing data-related initiatives to improve Allied interoperability.

For example, in the past, NATO has developed interesting initiatives such as the Federated Mission Networking (FMN) capability to build trust between NATO allies and NATO partners. FMN was agreed to by the North Atlantic Council in 2015 to enable an alignment of operational processes, a standardisation of technical and procedural solutions and the development of a shared set of C2 capabilities for NATO-led and/or coalition missions[29]. Efforts like FMN had at their core a need to ensure trust between NATO allies and an insistence upon interoperability. With the introduction of technologies such as cloud computing, it would be wise for NATO allies to consider developing a similar structure to FMN for cloud-computing purposes. In particular, by attempting to enhance the interoperability of cloud systems across NATO allies, an FMN-like structure could enable cloud-based platforms to play a considerably larger role in NATO C2 efforts.

---

[25] NATO, "NATO Cloud Conference advances innovation and IT security across the Alliance", 22 January 2025. See: https://www.nato.int/cps/en/natohq/news_232539.htm?selectedLocale=en.
[26] Ibid.
[27] NATO's Data Centric Reference Architecture (DCRA) provides guidance for developing or enhancing data-centric capabilities by NATO allies in support of NATO's Digital Transformation. Its principles, core functions and federation interfaces are intended for use by NATO allies and industries in order to deploy data-intensive systems and services for NATO's Digital Backbone. See: https://nhqc3s.hq.nato.int/apps/DCRA_Report/id-29d4122b072148f5aaf4882ecc5d963c/elements/id-977df055bb114ad6885e8eb3533b61be.html.
[28] NATO, "Deliver an Alliance Secure and Scalable Cloud Environment". See: https://nhqc3s.hq.nato.int/apps/DCRA_Report/id-29d4122b072148f5aaf4882ecc5d963c/elements/id-e50243cd4f884158aeb9771b9d403d5f.html.
[29] NATO Allied Command Transformation, "Federated Mission Networking", 2015. See: https://www.act.nato.int/activities/federated-mission-networking/.

Chapter Two
NATO Allies and Cloud Computing: The Story So Far

In this part of the paper, we zoom in on the individual cloud computing efforts conducted by NATO allies. This is so we might attain a better understanding of individual sovereign efforts in defence cloud computing enterprises. It should be underlined at the outset that no single cloud infrastructure exists in NATO, and so the policy attention has been squarely focused on how best to create a "federated" or "multi-cloud" architecture among willing NATO allies. What will be clear from the analysis of several NATO allies in this section is that there are various approaches to adopting cloud computing within the Alliance, even though NATO itself has underlined the importance of cloud computing as part of NATO's "Digital Backbone" efforts. In particular, the case of the US military provides a useful insight into how the Pentagon and US military branches are thinking about cloud services in a military context. The US Department of Defence (DoD) has adapted its approach to cloud services over the past two administrations as doubts within the government surfaced over the effectiveness of a federated cloud service for the US military. This is not to imply that the US DoD is sceptical about cloud services in a military context, but rather that greater thought needs to go into where best to apply cloud services in a defence context. We should recognise that the US has faced problems in the past with procuring cloud services from commercial vendors.[30]

As stated earlier, the US military has used its Joint Warfighting Cloud Capability to contract commercial firms to provide limited cloud services. Under the previous Biden administration, the DoD was committed to using cloud services to improve the US military's ability to conduct MDO. The DoD went even further to insist on rapid cloud adoption strategies, whereby individual branches of the US military could contract cloud services as and when needed[31]. Even under the current Trump administration, there are continued efforts at the Pentagon to make use of commercial cloud services – not least because specific elements of the US military, such as Special Forces, are making increasing use of AI and they need to be able to effectively manage the rafts of data they are acquiring through their activities[32]. What is more, the US Department of Defense is also currently

[30] For example, the US government cancelled JEDI in 2021. See: https://www.defense.gov/News/Releases/release/article/2682992/future-of-the-joint-enterprise-defense-infrastructure-cloud-contract/.
[31] See, for example, US Department of Defence, "DOD Makes Headway on Cloud Computing", 29 March 2023. See: https://www.defense.gov/News/News-Stories/Article/Article/3345260/dod-makes-headway-on-cloud-computing/.
[32] US Department of Defence, "Senior Special Ops leadr Highlights AI's Usefulness Beyond Battlefield", 3 June 2025. See: https://www.defense.gov/News/News-

redoubling its efforts to improve network security. Indeed, the DoD is working to ensure that its "Zero Trust" architecture is ready by 2027 in order to ensure that its federated identity, credential and access management system (ICAM) is secure[33], among other things.

> **No single cloud infrastructure exists in NATO, and so the policy attention has been squarely focused on how best to create a "federated" or "multi-cloud" architecture among willing NATO Allies**

In fact, across recent US administrations, branches of the US military have been keen to adopt cloud services at an early stage. One branch of the US military that has perhaps been on the front foot in this endeavour has been the US Army. In 2014, the US created its enterprise cloud computing reference architecture, which was designed to identify the benefits of cloud services for the US Army enterprise. Overall, the US Army was keen to adopt cloud services in areas such as identity management, network security and operations[34]. Convinced of the benefits of cloud services in specific circumstances, the US Army has been exchanging information on approaches to cloud computing with the US Air Force and US Navy[35]. Each branch of the US military has its own cloud computing agency to help deal with the procurement and uptake of cloud services. The US Army makes use of the "Enterprise Cloud Management Agency" (ECMA), the US Navy relies on

---

Stories/Article/Article/4205349/senior-special-ops-leader-highlights-ais-usefulness-beyond-battlefield/.

[33] US Department of Defence, "'Zero Trust' Architecture Could Prevent Adversary Data Theft, Protect Warfighters", 26 February 2025. See: https://www.defense.gov/News/News-Stories/Article/Article/4078717/zero-trust-architecture-could-prevent-adversary-data-theft-protect-warfighters/.

[34] US Department of the Army, "U.S. Army Enterprise Cloud Computing Reference Architecture", 29 September 2014. See: https://www.dragon1.com/downloads/20140929-us_army_enterprise_cloud_computing_reference_architecture_v1-0.pdf.

[35] Demarest, C., "US Military Services Exchanging Cloud-Computing Wisdom Amid JADC2 Push", 17 January 2023. See: https://www.c4isrnet.com/smr/cloud/2023/01/17/us-military-services-exchanging-cloud-computing-wisdom-amid-jadc2-push/#:~:text=The%20Army%20has%20already%20shifted,%27"&text=Colin%20Demarest%20was%20a%20reporter,also%20an%20award%2Dwinning%20photographer.

"DON Neptune" and the US Air Force offers "Cloud One" as its cloud computing service[36].

Where there has been a shift in the US approach over the past few years is in relation to how useful cloud computing can be from a tactical perspective. In the mid-2010s, the hype around cloud computing services centred on the real-time intelligence advantages that could be had from the development of a "combat cloud"[37]. To this day, there is a compelling logic that cloud services can help warfighters with data gathering, fusion and usage, and that cloud computing can help with tactical decisions as it can fuse data from various tactical capabilities (e.g. drones, satellites, sensors, etc.). Since at least the early 2020s, and since cloud services and applications have had time to further mature, the US Army has reframed its attachment to "tactical clouds" in favour of a multi-cloud, hybrid approach[38]. There have been fears in the US Army that opting for tactical clouds at the edge would present an even bigger burden on warfighters, who are supposed to focus on operations rather than network management. As one senior US Army official has noted, the risk with tactical cloud systems is that it introduces an additional level of complexity for warfighters, when the US military has made a conscious effort to avoid such complexity at the brigade and platoon levels[39]. To this end, the US military is now focusing on how to effectively use edge computing at the tactical level, but this also involves determining how the edge works across theatres, services and government agencies[40].

Such a consideration is of relevance in a NATO context, as there is certainly a need to develop an approach to cloud services that can address the NATO enterprise more generally (i.e. anticipating, scenario testing, data management, industrial and inventory management, etc.) and cloud services in warfighting contexts (i.e. how can cloud services enhance the performance of NATO forces at the tactical level). Furthermore, it is noticeable that the NATO approach to developing multi-cloud architectures reflects the US' cloud strategy, although developing and deploying hybrid clouds in a NATO context is arguably even more complex – the Alliance has to ensure connectivity between different military branches in each NATO ally, whereas

[36] US Department of Defense, "What is the Cloud?", Cloud.mil. See: https://www.cloud.mil/cloud.
[37] See, for example, Wong, W., "The Army Brings the Cloud to the Battlefield", FedTech, 31 July 2013. See: https://fedtechmagazine.com/article/2013/07/army-brings-cloud-battlefield.
[38] Pomerlau, M., "Army's Hybrid Cloud Approach Means Less Emphasis on 'Tactical Cloud' Architecture", Defensescoop, 13 January 2023. See: https://defensescoop.com/2023/01/13/armys-hybrid-cloud-approach-means-less-emphasis-on-tactical-cloud-architecture/.
[39] Pomerlau, M., "Army Experimenting With What the 'Edge' is for Cloud Computing Capabilities", Defensescoop, 17 January 2025. See: https://defensescoop.com/2025/01/17/army-experimenting-with-what-the-edge-is-for-cloud-computing-capabilities/.
[40] Ibid.

the US effort has to deal with inter-service network connections. Perhaps paradoxically, the case for a federated multi-cloud system is even more compelling in a NATO context, given the complexity of the Alliance, even if it is challenging to achieve.

Another NATO ally that has been keen to integrate cloud computing services into its military is the United Kingdom (UK). Under the previous Conservative government, the UK produced a "Cloud Strategic Roadmap for Defence" that not only called for a radical shift in the UK military's perceptions towards cloud computing, but also in how the UK armed forces can exploit data to enhance the UK's approach to digital warfare[41]. Through this strategy, the UK government is hoping to create its own "Digital Backbone" comprised of cloud programmes, digital foundries, cybersecurity capacities and more. It has created a "CIRRUS" delivery model within the UK defence enterprise to ensure that all strands related to governance, security and technology are brought together in a single digital approach to defence. Such an approach was taken further in the UK Strategic Defence Review (SDR) 2025, which highlighted the critical need to develop a "Digital Targeting Web" to improve UK defence's ability to connect sensors, deciders and effectors across all military domains[42]. What is more, the SDR promises a £1 billion investment in this endeavour including an ambition to produce a "Defence-wide Secret Cloud" by at least 2026-2027[43].

Still, at the heart of the UK's defence cloud efforts rest familiar technological and personnel challenges. As one study makes clear, the UK has possession of advanced digital capabilities and it already makes use of them in a defence context, but the major challenges in enhancing the UK's digital backbone related to a lack of digital skills, cumbersome procurement processes and being able to effectively network new digital capabilities with legacy analogue systems[44]. Indeed, the British Army had already identified a need to upskill its workforce and enhance its digital services by 2025, but the continued need to deliver the UK's digital backbone in defence shows that ambitious timelines are difficult to adhere to, given the sheer breadth of

[41] UK Government, "Cloud Strategic Roadmap for Defence", 2 February 2025. See: https://www.gov.uk/government/publications/cloud-strategic-roadmap-for-defence/cloud-strategic-roadmap-for-defence.
[42] Barrie, D., Barry, B., Childs, N., Hackett, J. and Williams, H., "Strategic Defence Review 2025: UK Outlines Ambitious Vision for Defence Amid Fiscal Challenges", International Institute for Strategic Studies, 4 June 2025. See: https://www.iiss.org/online-analysis/military-balance/2025/06/sdr-2025-uk-outlines-ambitious-vision-for-defence-amid-fiscal-challenges/.
[43] Ibid.
[44] Sylvia, N., "European Digital Defence Priorities in an Uncertain World", Royal United Services Institute, 25 March 2025. See: https://www.rusi.org/explore-our-research/publications/emerging-insights/european-digital-defence-priorities-uncertain-world.

modernisation efforts[45]. One of the major challenges identified by the British Army is to ensure that the UK's digital backbone in defence is fully interoperable with NATO, and that force commanders and field armies can share data in real-time with allies[46].

FIGURE 4: "COMBAT CLOUDS" AND NATO ALLIES

Country	Cloud system
Albania	Albania has established a Military Cyber Security Unit, that utilises cloud services and is supported by the United States.
Belgium	Belgium is developing a military cloud system, which should be ready by 2026. It is undertaking national defence digitalisation and supports NATO efforts.
Bulgaria	There is no evidence of a military cloud as yet, but Bulgaria supports wider NATO digitalisation efforts.
Canada	Canada makes use of cloud services in the area of air defence, and it is experimenting with cloud technologies in the area of C2.
Croatia	There is no evidence of a military cloud as yet, but Croatia supports wider NATO digitalisation efforts.
Czechia	There is no evidence of a military cloud as yet, but Czechia is seeking commercial cloud services and supports wider NATO digitalisation efforts.
Denmark	Denmark makes use of cloud services in the area of military communications, is undertaking a digital modernisation strategy and supports NATO efforts.
Estonia	Estonia makes use of cloud services in the area of air surveillance, is undertaking a digital modernisation strategy and supports NATO efforts.
Finland	Finland makes use of cloud services in the area of C4ISR, is undertaking a digital modernisation strategy and supports NATO efforts.
France	France makes use of cloud services in the area of C4ISR and cyberdefence, is undertaking a digital modernisation strategy and supports NATO efforts.
Germany	Germany makes use of "pCloudBw" for defence information systems, is undertaking a digital modernisation strategy and supports NATO efforts.
Greece	Greece makes use of cloud services in the area of air surveillance, is undertaking a digital modernisation strategy and supports NATO efforts.
Hungary	There is no evidence of a military cloud as yet, but Hungary supports wider NATO digitalisation efforts.

[45] British Army, "The Army Digital and Data Plan, 2023-2025: A Guide to Help you Deliver the Army's Digital Transformation", UK Government, 2022. See: https://www.army.mod.uk/media/21608/2_295200-mod_addp_review-file_05.pdf.
[46] Ibid.

Iceland	Iceland is seeking to become the first “cloud nation”, but has no single military cloud as yet. Iceland uses cloud services for maritime surveillance and air and missile defence and supports NATO’s digital defence efforts.
Italy	Italy is developing a “Military Space Cloud Architecture (MILSCA)”, which will be a single-vendor system.
Latvia	There is no evidence of a military cloud as yet, but Latvia makes use of cloud services in the area of C4ISR, is undertaking a digital modernisation strategy and supports NATO efforts.
Lithuania	There is no evidence of a military cloud as yet, but Lithuania makes use of cloud services in the area of C4ISR, is undertaking a digital modernisation strategy and supports NATO efforts.
Luxembourg	Luxembourg is currently developing a “Cyber Defence Cloud”, is undertaking a digital modernisation strategy and supports NATO efforts.
Montenegro	There is no evidence of a military cloud as yet, but Montenegro supports wider NATO digitalisation efforts.
Netherlands	There is no evidence of a military cloud as yet, but the Netherlands makes use of cloud services in the area of C4ISR, is undertaking a digital modernisation strategy and supports NATO efforts.
North Macedonia	There is no evidence of a military cloud as yet, but North Macedonia supports wider NATO digitalisation efforts.
Norway	There is no evidence of a military cloud as yet, but Norway makes use of cloud services in the area of C4ISR, is undertaking a digital modernisation strategy and supports NATO efforts.
Poland	There is no evidence of a military cloud as yet, but Poland makes use of cloud services in the area of C4ISR, defence inventories and cybersecurity, is undertaking a digital modernisation strategy and supports NATO efforts.
Portugal	Portugal is developing a military cloud system, which should be ready by 2027. It is undertaking national defence digitalisation and supports NATO efforts.
Romania	No military cloud as yet in Romania, but the country is undertaking a digital modernisation strategy and supports NATO efforts.
Slovakia	There is no evidence of a military cloud as yet, but Slovakia supports wider NATO digitalisation efforts.
Slovenia	There is no evidence of a military cloud as yet, but Slovenia supports wider NATO digitalisation efforts.
Spain	There is no evidence of a military cloud as yet, but Spain makes use of cloud services in the area of C4ISR and is planning to boost cloud service usage as part of the FCAS fighter project. Spain is undertaking a defence digital modernisation strategy and supports NATO efforts.

Sweden	There is no evidence of a military cloud as yet, but Sweden makes use of cloud services in the area of C4ISR. Sweden is undertaking a defence digital modernisation strategy and supports NATO efforts.
Türkiye	The armed forces are developing a "TAF Cloud Computing System Project", which will be a single-vendor cloud service.
United Kingdom	The UK uses "MoDCloud", which is a single-vendor cloud system for use by the Ministry of Defence.
United States	Joint Warfighting Cloud Capability is a multi-cloud and multi-vendor cloud system for all branches of the US military and Pentagon.

Source: authors' own, 2025

Canada has also started to rely on cloud technologies for C4ISR and the tasks of intelligence sharing and data storage. Indeed, in January 2024, the Royal Canadian Air Force carried out a demonstration of a cloud-based C2 software integrator to enhance response times within the North American Aerospace Defense Command (NORAD)[47]. During this same time, the Canadian Army experimented with a cloud-based tactical network during the military exercise Maple Resolve 23. This saw Canadian Army units use cloud-based systems for tasks such as troop manoeuvres, enhanced communication and more effective tactical geospatial intelligence. Most importantly, one of the major conclusions from Maple Resolve 23 was that cloud-based tactical systems allowed military units to move more freely without the need for lengthy congregations of forces on the battlefield, which would have exposed forces to enemy, red team, attacks[48].

Italy has also made an early bid to produce its own combat cloud called the "Military Space Cloud Architecture" (MILSCA). Entrusting the development of MILSCA to a national firm, Leonardo, Italy wants to seize on the potential of cloud services in defence and allow the Italian armed forces to be able to benefit from strategic data: this would effectively see the fusion of data for navigation, earth observation and communications. And here, Leonardo is cooperating with national champions in Italy such as Telecom Italia, to develop a cloud for the public administration and thereby to stimulate civil-military interactions in Italy[49]. Italy has proclaimed that it wants to be the

[47] Canadian Government, "Canadian Air Defence Sector introduces new cloud-based command-and-control system", 26 January 2024. See: https://www.canada.ca/en/department-national-defence/maple-leaf/rcaf/2024/01/canadian-air-defence-sector-introduces-new-cloud-based-command-and-control-system.html.
[48] Ibid.
[49] Leonardo, "Al via il Polo Strategico Nazionale, la nuova infrastruttura cloud per la Pubblica Amministrazione", 6 October 2022. See: https://www.leonardo.com/it/news-and-stories-detail/-/detail/polo-strategico-nazionale.

first country in NATO to have a "space-cloud" system, which would see the development of a supercomputer and archive system in space to 'guarantee users access to strategic data such as communication, earth observation and navigation data, anywhere, even in the most remote places, and at any time'[50]. MILSCA is currently in the study phase of the project with a duration of 24 months, which, if successful, 'will involve the deployment in orbit of a demonstrative constellation of satellites'[51]. Finally, we should also not neglect that Italy, Japan and the UK are developing the Global Combat Aircraft Programme (GCAP), and Leonardo has already partnered with Microsoft and Accenture to roll out a cloud platform across its UK business[52].

Germany has also been experimenting with cloud services in defence, and it already makes use of cloud computing for military tasks related to C4ISR, logistics and defence administration. More broadly, Germany has been quick to integrate cloud services across its government, with the adoption of the German Government Cloud (Deutsche Verwaltungscloud, DVC) in 2025[53]. For the Bundeswehr, Germany has also sought to develop a private cloud infrastructure under its pCloudBw architecture. The German armed forces are adopting cloud services as part of their broader digitalisation efforts, and the aim is to develop a private and secure cloud by the end of 2027[54]. As part of these efforts, the German Federal Ministry of Defence has already invested in new data centres and IT infrastructure to support the introduction of pCloudBw, with the aim to ensure that all new data centres are in place in 2026[55]. It is believed that pCloudBw will enable the Bundeswehr to engage in MDO and to ensure that Germany's growing military forces and capabilities remain interoperable[56].

---

[50] Leonardo, "Leonardo: Kick off for the project of the first Space Cloud System for defense", 19 February 2024. See: https://www.leonardo.com/en/press-release-detail/-/detail/19-02-2024-leonardo-kick-off-for-the-project-of-the-first-space-cloud-system-for-defense.
[51] Ibid.
[52] Leonardo, "Leonardo is first major defence company in the UK to move to the secure cloud", 20 April 2023. See: https://www.leonardo.com/en/press-release-detail/-/detail/20-04-2023-leonardo-is-first-major-defence-company-in-the-uk-to-move-to-the-secure-cloud.
[53] German Federal Ministry of the Interior, "Germany launches government cloud", 27 March 2025. See: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2025/03/dvc.html.
[54] Knop, D., "Bundeswehr relies on Google Cloud", Heise, 26 May 2025. See: https://www.heise.de/en/news/Bundeswehr-relies-on-Google-Cloud-10397526.html.
[55] "Ministry of Defence receives new data centre network", Marine Forum, 27 December 2024. See: https://marineforum.online/en/ministry-of-defence-receives-new-data-centre-network/
[56] "The pCloudBw and its Importance for the Bundeswehr", BWI Deutschland, 21 January 2025. See: https://www.bwi.de/magazin/artikel/die-pcloudbw-und-ihre-bedeutung-fuer-die-bundeswehr.

> **The German armed forces are adopting cloud services as part of its broader digitalisation efforts, and the aim is to develop a private and secure cloud by the end of 2027**

For France, cloud computing in defence is seen of growing importance for national strategic autonomy. The government has been supportive of French efforts to digitalise the French armed forces, but there have been concerns about how to ensure that any French combat cloud is sovereign. Here, there are concerns about ensuring national sovereignty over algorithms and there is an identified need 'to invest in designing and configuring algorithm chains' in defence[57]. France has taken a similar route to Italy in relying on a national defence prime, in this case Thales, to develop its military cloud. Paris does not seem to be insisting on French-only companies or services, however, but it does insist that any non-French elements to Thales' cloud architecture are located in France (e.g. ensuring that data centres are located in France)[58]. Again, France is interested in utilising cloud services to ensure its ability to conduct MDO and to boost interoperability; however, France is also investing in cloud services in anticipation of major weapons programmes development such as the FCAS fighter jet[59].

Poland, like many other NATO nations, is also investing in cloud services in defence[60]. Not only is the Polish Ministry of Defence utilising cloud services as part of its overall integrated IT system, but it also makes use of cloud

[57] French Ministry of the Armed Forces, "Artificial Intelligence in Support of Defence", Report of the AI Task Force, September 2019: p. 5. See: https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf.
[58] Rosemain, M., "France's Thales creates cloud services company powered by Google", Reuters, 30 June 2022. See: https://www.reuters.com/technology/frances-thales-creates-cloud-services-company-powered-by-google-2022-06-30/
[59] Gros, P., "The 'Tactical Cloud', A Key Element of the Future Combat Air System", Note de la FRS, No.19, 2019. See: https://www.frstrategie.org/en/publications/notes/tactical-cloud-key-element-future-combat-air-system-2019.
[60] CEPA, "Polish Military Modernisation", 30 September 2015. See: https://cepa.org/article/polish-military-modernization/.

computing for its logistics networks[61]. Poland has been keen to invest in cloud computing services and, in February 2025, the Polish government signed a $700 million investment in Microsoft's cloud services to boost cybersecurity and help Poland adapt to AI and cloud economies and technologies[62]. For Poland, the potential of cloud computing in defence is a natural part of its overall national "Military AI Strategy 2024-2039", which sets out to ensure that Poland has a material technological advantage over potential and actual rivals[63]. Part of this drive has already seen Poland launch an AI Implementation Centre to enhance the country's cyberdefences and to ensure that Poland's military networks are secure from cyberattacks[64].

Many other allies are also seeking to adopt cloud services in defence, although they are at various stages of adoption and there remain concerns about how best to furnish their armed forces with cloud services. Among these concerns is, first, a recognised need to fully assess the financial costs involved in adopting cloud services. This is combined with the fact that defence budgets are increasing across Europe, meaning that there is additional financial leeway to modernise defence forces in NATO. For example, Greece has the potential to develop innovation within the Greek armed forces, but it has not always seized on the potential of its defence technological and industrial base[65]. Nevertheless, Greece has recently announced a 12-year modernisation plan for its military, which will include a €28 billion injection of support until 2037. This modernisation will be felt mainly in the areas of fifth-generation fighter jets, new frigates, an air and missile defence system (named Achilles' Shield), satellite communications and a suite of sensors for underwater threat detection[66]. Interestingly, at the time of writing, Greece does not make use of a dedicated military cloud system, even though it aims to modernise its defence forces.

---

[61] Sendek, R. and Kowalska-Sendek, M., "Logistic Network", 2 December 2021. See: https://www.polska-zbrojna.pl/home/articleshow/35927?t=Logistic-Network.
[62] Zulhusni, M., "Poland sees €700m investment in cloud infrastructure and security", T_HQ, 19 February 2025. See: https://techhq.com/2025/02/poland-to-see-usd-700-million-investment-into-cloud-infrastructure-and-security/.
[63] Polish Government, "Department Artificial Intelligence Strategy until 2039", 11 October 2024. See: https://www.gov.pl/web/obrona-narodowa/resortowa-strategia-sztucznej-inteligencji-do-roku-2039.
[64] "Poland Launches Artificial Intelligence Center to Boost Military Power", Defense Mirror, 11 October 2024. See: https://www.defensemirror.com/news/38978.
[65] Kamaras, A., "Innovation and the Greek Armed Forces", ELIAMEP Policy Paper, No. 163, 2024. See: https://www.eliamep.gr/wp-content/uploads/2024/05/Policy-paper-163-EN-final.pdf
[66] "On Maple Resolve 23, the enemy was armed with a cloud-based tactical network", Canadian Army Today, 18 January 2024. See: https://canadianarmytoday.com/on-maple-resolve-23-the-enemy-was-armed-with-a-cloud-based-tactical-network/.

> **Nordic states have experimented with cloud services in a defence context during military exercises such as Joint Viking, where technologies such as 5G networks were used to enhance tactical communications and situation awareness**

Türkiye is seeking to develop a combat cloud for its armed forces within the "Steel Dome" concept of air and missile defence. The Turkish Armed Forces (TAF) have made clear their intention to develop cloud infrastructure as part of their C4ISR and for specific tasks such as drone surveillance missions. In the case of Türkiye, however, the government has taken the decision to create a fully sovereign cloud system called the "TAF Cloud Computing System Project". To this end, the government in Ankara has entrusted Turkish firm Havelsan to oversee the development of the cloud platform. In particular, Havelsan has already indicated that the cloud project would help the TAF with logistics tasks, protect against cyber threats and enhance simulation and training by utilising AI and Big Data[67]. While the development status of the cloud computing project is unclear, it is clear that the project is a major government commitment that should be completed by 2028.[68]

Several Nordic NATO members have also sought to enhance the digitalisation of their defence forces, including with cloud services. Finland, Iceland, Norway and Sweden do not have central combat clouds for their militaries, but they do already make use of cloud services for specific military tasks such as Command, Control, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR). Sweden, for example, is investing in its wider government AI strategies in defence, and it can rely on commercial innovations to help with the transition to cloud-based

[67] Havelsan, "HAVELSAN Takes Another Historic Step for the Turkish Defense Industry", 9 December 2024. See: https://www.havelsan.com/en/news/havelsan-taf-cloud-computing#:~:text=The%20Turkish%20Armed%20Forces%27%20(TAF,under%20the%20leadership%20of%20HAVELSAN.

[68] Turkish Government, "Türkiye Strategic Plan, 2024-2028": p. 81. See: https://www.ssb.gov.tr/Images/Uploads/MyContents/V_20240405145902497059.pdf.

platforms[69]. When it comes to the adoption of cloud technologies, however, Sweden has experimented with cloud services in the domain of C2, especially with naval military communications[70]. Finland and Norway are also seeking to take up cloud services in the area of C4ISR, especially in terms of modernising satellite communications and cyberdefence[71]. It is also noteworthy that Nordic states have experimented with cloud services in a defence context during military exercises such as Joint Viking, where technologies such as 5G networks were used to enhance tactical communications and situation awareness[72]. Finally, Iceland is perhaps one of the more advanced Nordic NATO nations, as it uses cloud services for its coast guard and its air surveillance radar sites, which play a critical role in NATO's Integrated Air and Missile Defence System (IAMD). Keeping in mind that Iceland took a relatively early decision to become a "cloud first nation", Iceland does not need convincing of the importance of the cloud in defence[73].

[69] Finlan, A., "A Fertile Soil for AI? Defence AI in Sweden", in Borchert, H., Schütz, T. and Verbovsky, J. (eds.) The Very Long Game: 25 Case Studies on the Global State of Defense AI (Springer: 2024): pp. 107-126.
[70] "Sweden and NATO: Unlocking SitaWare Advantage", Systematic, 7 May 2024. See: https://systematic.com/int/industries/defence/news-knowledge/blog/sweden-and-nato-unlocking-the-sitaware-advantage/.
[71] See, for example, Lund, K., "Military Use of Cloud Services – Possibilities and Challenges", Norwegian Defence Research Establishment FFI, 2021. See: https://www.ffi.no/en/publications-archive/bruk-av-skytjenester-i-forsvaret-muligheter-og-utfordringer; Casimiro, C., "ICEYE Leads Consortium to Enhance Finland's Space-Enabled ISR Capabilities", TheDefensePost, 22 November 2024. See: https://thedefensepost.com/2024/11/22/iceye-consortium-finland-isr-f35/; and O'Halloran, J., "Norway's ICE offers slice of 5G for military communications", Computer Weekly, 9 October 2024. See: https://www.computerweekly.com/news/366613113/Norways-ice-offers-slice-of-5G-for-military-communications.
[72] Nokia, "Nokia trials 5G technology during Joint Viking military exercise in Norway", 20 May 2025. See: https://www.nokia.com/newsroom/nokia-trials-5g-technology-during-joint-viking-military-exercise-in-norway/.
[73] See, for example, Barney, D., "The Power of Iceland: RMS and Verne Global Take to the Cloud", TMCnet, 3 January 2014. See: https://cloud-computing.tmcnet.com/features/articles/365250-power-iceland-rms-verne-global-take-the-cloud.htm; and Microsoft, "Iceland to become the first 'cloud-first-nation'", 19 September 2018. See: https://news.microsoft.com/europe/features/iceland-to-become-the-first-cloud-first-nation/.

Chapter Three
NATO and the Challenges of Cloud Computing Uptake

Following our analysis of the current state of cloud service uptake in NATO allies, the paper now considers the benefits and costs of moving towards a more "federated" or interoperable cloud architecture at the NATO level. One of the obvious benefits of utilising cloud services within defence is its ability to enhance the interoperability of military units and systems, as well as to improve data usage in the battlefield for ISR and logistics. Even away from the battlefield, one of the areas of NATO policy and planning that could be improved by the greater uptake of cloud services is in the area of personnel training, healthcare and logistics[74]. We should also acknowledge that cloud computing services can give NATO allies a technological cutting-edge in warfare and defence[75]. For example, fifth generation fighters – either in use of under development – make use of cloud computing services already. Such aircraft are able to make use of cloud computing in order to enhance operational autonomy. This is particularly the case as Big Data can be used to substitute operational dependencies on space-based technologies, which may be disrupted in times of war, as well as increase the ability to manage a distributed network of weapons systems such as Unmanned Aerial Vehicles.

Several challenges do, however, present themselves. Based on the analysis in the previous chapter, it is clear that NATO nations are at different stages of developing or adopting cloud computing in their militaries. Allies can, essentially, be divided into two main camps: 1) those that want to develop sovereign combat clouds; and 2) those that are more open to vendors and commercial providers. This very fact complicates NATO's efforts to digitalise the Alliance and the ambition to create a federated, multi-cloud architecture will take some time and additional investments. The potentially good news for NATO is that defence budgets are increasing across the Alliance. Measures designed to increase NATO allies' defence spending from 2% of GDP to 5% of GDP should, in theory, lead to greater financial bandwidth to invest in EDTs such as cloud computing and services. The other positive development is that commercial cloud computing services are expanding globally. Such trends can have positive outcomes for the adoption of commercial cloud services in defence. As shown in the previous chapter, several NATO allies already procure cloud computing services from commercial firms.

---

[74] Saha, S., Low, W. and Di Martino, B., "Sustainment of Military Operations by 5G and Cloud/Edge Technologies", Advanced Information Networking and Applications, 2023: pp. 70-79. See: https://link.springer.com/chapter/10.1007/978-3-031-28694-0_7.
[75] Op.Cit., "Defence in the Cloud". See also Op.Cit. "NATO's Digital Modernisation: The Case of Cloud Computing".

So, creating a federated cloud architecture across the NATO Alliance is an ambitious but complex endeavour. One of the major challenges related to cloud computing is sovereignty and security. As each NATO nation has different legal and military requirements, there appears to be a preference for sovereign cloud architectures. States are hesitant about sharing sensitive data through clouds and maintaining data privacy and sovereignty is seen as a key attribute of military power and security interests. Ensuring secure communication and data exchange among nations with varying threat models, security postures and intelligence-sharing protocols is very challenging. The fact that there are no fully agreed-upon NATO standards for sharing sensitive data hampers the ability of allies to exchange classified or sensitive data via cloud platforms. Without common NATO standards for data, it is more difficult to effect cross-border cloud services and to ensure safe identity and access management protocols across the Alliance.

Creating a federated cloud architecture across the NATO Alliance is an ambitious but complex endeavour

The interoperability and governance of cloud services within NATO is another major challenge. Aligning disparate IT systems, software stacks and cloud service models (e.g., IaaS, PaaS) is not easy. NATO nations use a host of commercial cloud services and national sovereign clouds, and there are difficulties in integrating Application Programming Interfaces (API), which allow different cloud services and applications to communicate and exchange data. What is more, deciding how shared data resources are governed, who makes policy decisions at the NATO level for data usage and how conflicts are resolved between allies are critical governance factors. Without strong governance, any NATO federated cloud system may fragment or become underutilised. Here, differing strategic priorities, trust levels and domestic political pressures may conspire to reduce usage in a federated NATO cloud system. Here, it would be recommended for NATO allies to share best practices when it comes to the procurement of cloud services on a national level, as this may allow the Alliance to better position the adoption of cloud technologies in line with NATO allies' diverse budget cycles, procurement regulations and acquisition strategies.

Another challenge facing NATO relates to latency and network resilience. Ensuring that the constituent parts of a cloud architecture are geographically and strategically located is important. As we saw in the case of the US, there are discussions with the US military about how to distribute networks and to gauge the risks associated with edge computing resources. For the Alliance, there is a major question about how to ensure the cyber and physical resilience of data centres and associated computing infrastructure. However, deploying edge computing resources in remote or vulnerable tactical theatres is a consideration for all military planners seeking to deploy cloud services in a combat or strategic situation. And here, there is also a need for the Alliance to better understand the operational limitations that come with the deployment of cloud services in the field, including how different legal regulations in various jurisdictions may hamper data transfers. We must be cautious, for example, of "data swamping" platforms, vehicles and devices, which may inadvertently overburden communications systems. Today's communications and smart devices still suffer from computing power and there remains a lag between Big Data processes and mobile devices[76]. Such limitations continue to weigh on the minds of defence planners, who may be reluctant to invest in technologies that have not matured enough for the battlefield.

One of the major concerns with the deployment of cloud services in a NATO context is related to potential supply chain vulnerabilities and cybersecurity breaches. Therefore, one of the ways to build greater trust within NATO about cloud services and platforms is to enhance the Alliance's overall cybersecurity. The key aim with any cybersecurity architecture in cloud services and platforms is to ensure that cyber breaches are detected in a timely fashion, and that they can be adequately isolated to ensure that any system-wide cloud is not compromised. This is not a simple affair, but it is well within the ability of NATO to ensure cybersecurity for any future multi-national cloud systems. For example, the Alliance would need to ensure the physical security of data centres where cloud servers are stored. This will require physical protection in the form of onsite security, air defence, detection sensors and systems, etc. It will also require that the Alliance ensure network security in the form of intrusion detection, prevention and response, as well as ensuring data and system integrity.[77] Cloud security should not be taken for granted, and there is a need to ensure adequate resources for response and prevention to cyber critical incidents: one study

[76] Soyata, T. et al. "COMBAT: Mobile-Cloud-Based Compute/Communications Infrastructure for Battlefield Applications", Proceedings of the SPIE. See: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/8403/84030K/COMBAT--mobile-Cloud-based-cOmpute-coMmunications-infrastructure-for-BATtlefield/10.1117/12.919146.short.

[77] Nimi, T., "Safeguarding the Cloud: The Imperative of Defense in Depth", Medium, 25 January 2024. See: https://medium.com/@tolubanji/safeguarding-the-cloud-the-imperative-of-defense-in-depth-928ec0d8b14e.

has argued that 58% of cybersecurity teams are busy responding to incidents, rather than engaging in preventive measures[78].

There is evidence to suggest that larger cloud firms tend to be more structurally attentive to cybersecurity than smaller firms, which is also a consideration when planning for secure architectures

There are major improvements in the development of secure cloud computing environments. Indeed, the rapid development of so-called "zero-trust" architectures are being deployed to ensure that computing systems are constantly authenticating and authorising access and usage[79]. Such "zero-trust" architectures are based on a "never trust, always verify" model that presumes that threats could emerge inside or outside a network. There are multiple ways to develop a "zero-trust" architecture including via enhanced identity and access management (IAM) based on strong user authentication (e.g. multi-factor authentication); network segmentation (i.e. dividing networks into smaller zones that can be isolated to contain threats); encryption; and constant surveillance and monitoring[80]. There is evidence to suggest that larger cloud firms tend to be more structurally attentive to cybersecurity than smaller firms, which is also a consideration when planning for secure architectures[81].

---

[78] Law, M., "Cloud Security: The New Frontier of Enterprise Defence", Technology Magazine, 27 November 2024. See: https://technologymagazine.com/articles/cloud-security-the-new-frontier-of-enterprise-defence.

[79] "The Silver Lining of Military Cloud Computing", Systematic, 25 March 2025. See: https://systematic.com/int/industries/defence/news-knowledge/blog/the-silver-lining-to-military-cloud-computing/.

[80] Kamble, T. et al., "Secure Data Transmission in Cloud Computing Using a Cyber-Security Trust Model with Multi-Risk Protection Scheme in Smart IOT Application", Cluster Computing, Vol. 28, No 79, 2025. See: https://link.springer.com/article/10.1007/s10586-024-04847-z.

[81] Acre, D.G., "Cybersecurity and Platform Competition in the Cloud", Computers & Security, 93, June 2020: pp. 1-9.

Finally, we cannot escape the overall transatlantic political context when thinking about the adoption of cloud services in a NATO context. Deteriorating transatlantic relations through trade tariffs and questions of burden-sharing have raised questions about security of supply and technology dependencies. Even in past years, 'European countries were starting to become completely dependent on the big American cloud providers' and this fear has not disappeared[82]. Europeans are indeed becoming more sensitive about technology control and supply chains, and there are cases where national parliaments in Europe have called for less dependency on non-European cloud service providers[83]. In this respect, there appears to be a contradiction between the "technological sovereignty" agenda in Europe and the need to rapidly integrate cloud services in Europe, even if from a non-European supplier[84]. However, it is also the case that there is no set European approach to the integration of non-European cloud service providers, and there is even evidence to suggest that European states are attempting to secure stronger bilateral deals with non-European cloud providers, rather than to exclude such providers from the European market[85]. As the previous chapter revealed, many combat clouds being developed in Europe do so in partnership with large American technology firms such as Microsoft, Google, Amazon and more.

[82] Op.Cit., "NATO's Digital Modernisation: The Case of Cloud Computing": p. 6.
[83] Desmarais, A., "'A threat to autonomy': Dutch parliament urges government to move away from US cloud services", Euronews, 20 March 2025. See: https://www.euronews.com/next/2025/03/20/a-threat-to-autonomy-dutch-parliament-urges-government-to-move-away-from-us-cloud-services.
[84] See, for example, Blancato, F. and Carr, M., "The Trust Deficit: EU Bargaining for Access and Control Over Cloud Infrastructures", Journal of European Public Policy, Early Online View. See: https://www.tandfonline.com/doi/full/10.1080/13501763.2024.2441418?src=recsys.
[85] Calcara, A., "European Cloud Computing Policy: Failing in Europe to Succeed Nationally?", West European Politics, Early Online View. See: https://www.tandfonline.com/doi/full/10.1080/01402382.2025.2491962#abstract

Conclusion and Recommendations

This In-Depth Paper has analysed the potential for the greater uptake of cloud computing and services within a NATO context. We have shown that NATO is heavily invested – politically and financially – in ensuring that the Alliance can seize on the benefits of emerging and disruptive technologies. Following the Hague Summit in 2025, military modernisation and digitalisation are highly likely to remain NATO priority issues. Indeed, the core challenge for NATO is ensuring that it does not fall behind in critical technologies that can enable and enhance its defence and deterrence efforts. In an era where adversaries are rapidly developing electronic warfare capabilities, NATO forces must be able to securely exchange information and data. To this end, this paper investigated how far, and in what manner, NATO and its allies are developing cloud computing technologies as part of their overall defence modernisation efforts. We also set out this analysis by looking for the main obstacles to the greater uptake of cloud service in defence, and we paid attention to critical issues such as how cloud services may advance interoperability, security and a military cutting-edge. To this end, we provided our understanding of cloud computing in defence, while also outlining the steps already taken by individual NATO allies and some of the challenges hampering greater adoption of cloud services.

Cognisant of NATO's ongoing efforts to create a "Digital Backbone" and promote a federated, multi-cloud architecture, we conclude this In-Depth Paper with some specific conclusions for policymakers to consider. The authors believe that these recommendations can also inform debates about military technology, burden-sharing and innovation that will long continue after the 2025 Hague Summit. Overall, the paper has shown that NATO and NATO allies can leverage cloud computing and services to significantly enhance the Alliance's defence and deterrence capabilities across operational, strategic and technical domains. To achieve this, the Alliance could consider the following recommendations:

- Ideally, NATO would move towards a more **hybrid multi-cloud architecture** that integrates Allied and NATO-level cloud services. Such an architecture would need to respect national sovereignty and compliance requirements (e.g. GDPR and national data regulations). It is recommended that NATO allies learn from past initiatives such as the FMN capability to build trust, interoperability and support in the area of cloud computing.

- NATO should use existing instruments to **streamline the involvement of commercial cloud providers in its operations**. Smaller players (e.g. start-ups) can be supported and integrated into NATO structures through preferential access to venture capital to scale up their capabilities (which NATO can already do through the NATO Innovation Fund) and through incentives to partner with large infrastructure providers (which NATO can already do through DIANA).

- NATO needs to assess current **defence procurement regulations and processes**, which can add unnecessary time and cost to cloud uptake in the Alliance. The Alliance as a whole is seeking to modernise its defence planning process, not least by making it easier for allies to cooperate with the commercial sector. Current procurement procedures are not always optimised for the uptake of EDTs.

- Cloud platforms can greatly aid **real-time situational awareness** through real-time data fusion, AI analytics and decision support. The ability for rapid ingestion and processing of data from ISR assets can drastically enhance early warning and operational adaptability.

- Cloud-based platforms can **enhance cybersecurity and resilience** by building in automated threat and risk detection systems. The NATO Cyber Operations Centre already utilises cloud, AI and machine learning capacities for situational awareness, coordination and resilience. Yet, NATO can seek to mainstream these measures across all allies.

- Cloud-based applications can be developed to enhance and optimise the Alliance's **force deployment and logistics needs**. Cloud-based systems could help optimise troop and equipment tracking, as well as enhance supply chain security and management. Cloud computing tools could also potentially be used for predictive analytics in case of a need to urgently re-route supplies.

- NATO must aid allies in developing **common cloud security and data-sharing standards**. NATO will be unable to conduct successful multi-domain operations in the future without secure data exchange. To this end, STANAGS should be leveraged and extended to cloud data formats.

- Cloud-based "data lakes" and secure enclaves can be used for **multinational intelligence exchange**. There is the potential to improve multi-domain planning and operations by using cloud-based systems to enhance and fuse HUMINT, SIGINT and GEOINT in near real-time. Here, an emphasis is needed on secure data environments and greater efforts are required to ensure that different levels of security classification are maintained and respected.

- NATO can spearhead efforts to **develop cloud-based training environments** for allies through joint simulations and war-gaming. Simulated environments could be hosted on clouds for various military and hybrid exercises and scenarios. The Alliance could experiment with cloud-based virtual environments to develop war-gaming and tabletop exercises.

Authors

Prof. Dr. **Daniel Fiott** is Head, Defence & Statecraft, at the Centre for Security, Diplomacy and Strategy (CSDS) at the Vrije Universiteit Brussel (VUB). Daniel is an Assistant Professor at the VUB and he is also a Non-Resident Fellow at the Madrid-based Real Instituto Elcano.

Prof. Dr. **Antonio Calcara** is Head, Geopolitics and Technology, at the Centre for Security, Diplomacy and Strategy (CSDS) at the Vrije Universiteit Brussel (VUB). Antonio is a Research Professor at CSDS, where he leads the European Research Council project Competition in the Digital Era (CODE): Geopolitics and Technology in the 21st Century.

ISSN print version: 2983-4678
ISSN online version: 2983-4686