The Hague Centre
for Strategic Studies

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

NATO's Digital Modernisation
The Case of Cloud Computing

Antonio Calcara
May 2025

The Hague Centre
for Strategic Studies

NATO's Digital Modernisation
The Case of Cloud Computing

Author:
Antonio Calcara, Professor at the Vrije Universiteit Brussels and Head of the Geopolitics and Technology Programme at the Centre for Security, Diplomacy and Strategy (CSDS)

Editor:
Tim Sweijs

May 2025

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

Introduction

Recent conflicts in Ukraine and the Middle East, with their many differences, give us a picture of what the current and future battlefield looks like: a multi-domain battlefield where a mix of legacy weapon systems are complemented and integrated by new technologies, especially those related to various types of AI-based weapon systems.[1] Advances in AI in turn depend heavily on the use of high-performance semiconductors, or more specifically, graphics processing units (GPUs) to train algorithms[2], but also on the physical infrastructure of cloud computing to store and analyse this vast amount of data. Cloud computing is, in fact, an enabling technology for the development of AI and in its various forms is already playing a crucial role in recent conflicts. Ukraine has migrated its sensitive data to the cloud in response to Russian destruction of critical infrastructure and persistent cyber-attacks, allowing public access to vital government information and supporting military command and control functions.[3] Several countries are using cloud computing services to manage and analyse data and facilitate AI-driven decision-making in military functions.[4]

Connecting platforms and sensors through distributed and cloud-based computing will provide warfighters with the tools, information and data they need to achieve operational superiority on the battlefield.

Cloud computing is a critical enabler for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). The use of cloud computing in C4ISR allows for joint planning, improved data repositories and communication platforms that can be used for intelligence sharing, reduced data loads for forces, and improved and faster command and control and decision making before and during conflicts. From an operational perspective, the ability to transport and analyse data via cloud computing will be a fundamental requirements as Western countries aim to structurally connect sensors to shooters on the battlefield.[5] Connecting platforms and sensors through distributed and cloud-based computing will provide warfighters with the tools, information and data they need to achieve operational superiority on the battlefield.[6]

Given the importance of cloud computing, this policy brief focuses on NATO's activities in this domain. NATO is at a critical juncture with regard to cloud computing, as it moves from the planning to the implementation phase of its cloud strategy. To make this transition, the policy brief identifies a number of challenges and opportunities, from both a military and an industrial perspective, that need to be addressed in order to effectively implement NATO's cloud ambitions. The policy brief draws an analytical distinction between the military dimension and the industrial and technological dimension, and presents three challenges for each dimension. With regard to the military dimension, the challenges (and possible opportunities) relate to bridging the strategic and tactical levels, the role of end users and the interoperability of military systems. For the industrial dimension, it discusses regulatory harmonisation, the role of the private sector and how to implement a NATO's multi-cloud strategy. It is not easy to find solutions that reconcile the military and industrial dimensions, but this paper proposes a strategy that could help move in that direction, particularly in relation to the concept of cooperation by design, i.e. the joint development of architectures and infrastructures, as opposed to the simple harmonisation, coordination or even integration of existing capabilities.

1 Krepinevich, A. F. (2023). *The origins of victory: How disruptive military innovation determines the fates of great powers*. Yale University Press., Scharre, P. (2023). *Four battlegrounds: Power in the age of artificial intelligence*. WW Norton & Company.

2 Kim, T. (2024). The Nvidia Way: Jensen Huang and the Making of a Tech Giant. W. W. Norton & Company

3 Mitchell, R. (2022). How Amazon put Ukraine's 'government in a box' — and saved its economy from Russia. *Los Angeles Times*, December 15, https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data

4 Borchert, H., Schütz, T., & Verbovszky, J. (2024). *The Very Long Game: 25 Case Studies on the Global State of Defense AI*. Springer Nature.

5 Eversden, A. (2021). How cloud computing makes Joint All-Domain Command and Control Possible. *C4ISR Net*. https://www.c4isrnet.com/smr/cloud/2021/04/26/how-cloud-computing-makes-joint-all-domain-command-and-control-possible/

6 Lindsay, J. R. (2020). *Information technology and military power*. Cornell University Press.

1. Cloud Computing and NATO

Cloud computing is an internet-based technology in which data is stored on servers and made available to customers as a service on demand.[7] Virtualisation allows services from multiple providers to reside on the same physical server and be co-located in a single 'multi-tenant' data centre.[8] Consumers can then use computing services (e.g. web hosting, email, payroll, data archiving) managed by third-party data centres or service providers, which are likely to be located in remote locations. There are three different types of cloud provider: Infrastructure-as-a-Service (IaaS) providers manage the physical infrastructure, such as servers, storage and networks. The IaaS market is currently dominated by three providers, Amazon Web Services (AWS), Microsoft Azure and Google Cloud Computing, which together account for 63% of the global cloud market.[9] Platform as a Service (PaaS) providers sell these pre-built combinations of building blocks in the form of different computing services.[10] They provide a platform for customers to build and deploy applications, and users can start developing applications right away using the providers' programming languages and tools. Software as a Service (SaaS) providers build, run and host applications that are delivered over the Internet and that customers pay to access. Key examples include web-based email (e.g. Gmail), a Salesforce dashboard or a Dropbox folder. PaaS and SaaS typically build on IaaS offerings.

NATO is in the process of creating a classified cloud system where member nations can share classified information.

Cloud computing is an integral part and enabling technology of NATO's Digital Transformation Implementation Strategy, adopted in June 2023, which outlines how the Alliance will transition to a hyper-connected, cloud-based infrastructure that will enable enhanced interoperability, real-time analytics and data-driven decision-making in the context of Multi-Domain Operations (MDO).[11] Cloud computing will then be required to manage vast amounts of data and perform analytics, unlocking the potential of machine learning and AI services. While cloud computing is recognised as central to NATO's digitisation strategy, the Alliance is at a delicate transition point as it moves from planning to implementation. As a senior official at NATO's Communications and Information Agency pointed out, "we already have a cloud-first strategy in NATO. Now we need to live it and adapt it".[12]

There are several lines of effort supporting the implementation of cloud technologies to support NATO's digital transformation. NATO is in the process of creating a classified cloud system where member nations can share classified information. As one NATO executive explained, a classified cloud system is critical to unlocking advances in machine learning

7 The US National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". See https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf p.2

8 Multitenancy refers to the ability of the different resources that make up cloud computing to serve multiple customers (or tenants). See Handler, S., Liu, L., and Herr, T. (2020). Dude, where's my cloud? A guide for wonks and users, *Atlantic Council*. September 28.

9 Data from Synergy research group. Available here: https://www.srgresearch.com/articles/cloud-market-growth-surge-continues-in-q3-growth-rate-increases-for-the-fourth-consecutive-quarter

10 There are also different types of PaaS: some PaaS providers sell software development tools that allow a customer to build and deploy apps on the customer's internal network, while other PaaS sell the software, but require the customer to obtain servers, storage, network connections and other cloud facilities separately (e.g. from an IaaS company or cloud provider).

11 NATO'S Digital Transformation Implementation Strategy https://www.nato.int/cps/en/natohq/official_texts_229801.htm

12 Quoted in Marchi, V. (2021). Cloudy vision: Can NATO's new deployable combat system focus the field?. *DefenseNews*. April 14, https://www.defensenews.com/battlefield-tech/it-networks/2021/04/14/cloudy-vision-can-natos-new-deployable-combat-system-focus-the-field/

and AI: "we need classified cloud as quickly as possible so we can integrate machine learning tools and deliver information at a speed of relevance and allow commands to make decisions. If we can't do that, I think we will fail".[13] There is therefore a shared sense of urgency within the Alliance to build on cloud computing as an enabling technology for the wider digital modernisation of NATO.

NATO is running several pilot projects. NATO Allied Command Transformation has contracted with IBM to create a digital ecosystem to improve intelligence, surveillance and reconnaissance.[14] The French company Thales has instead been selected to develop the Firefly system in 2021, the first theatre-level deployable defence cloud capability, a compact and fully certified solution for end-to-end management and control of connectivity, applications and data hosting.[15] This is complemented by studies and simulations conducted by the various bodies of the Alliance. The NATO Science and Technology Organisation's IST Panel Research Task Group 168 entitled "Adaptive Information Processing and Distribution to Support Command and Control", has been investigating how best to build an integrated cloud architecture in NATO. The overall objective was to look at cloud computing from a NATO perspective, i.e. as a federation of different national resources, and to investigate how cloud computing resources hosted by different countries can be leveraged in an operational context to make data readily available in a NATO tactical mission context.[16]

There is a shared sense of urgency within the Alliance to build on cloud computing as an enabling technology for the wider digital modernisation of NATO.

At NATO's 2024 Summit in Washington, 22 Allies signed a Memorandum of Understanding (MoU) to acquire the first Alliance-wide classified cloud capability - Allied Software for Cloud and Edge (ACE). With the acquisition process expected to begin later this year, NATO recently hosted a Cloud Conference, attended by more than 25 companies, to kick-start NATO's collaboration with industry.[17] Building on the ACE initiative, the Alliance aims to develop the NATO Digital Backbone (NDBB) to ensure universal connectivity and data transport across all operational domains (maritime, land, air, space and cyberspace).[18] The NDBB will develop a common, standardised architecture that will allow easy sharing of data between different cloud computing resources.

The Alliance is therefore at a very delicate stage in moving from planning to implementation of the cloud-first strategy. This could bring challenges and opportunities, but so far there has been little reflection in the policy debates on what these might be and how solutions might be found to ensure that the cloud strategy becomes a reality and not just an aspiration.

---

13 Quoted in Welch, C. (2024). NATO CIO: Alliance-wide classified cloud system is in the works. *Breaking Defense*, December 3. https://breakingdefense.com/2024/12/nato-cio-alliance-wide-classified-cloud-system-is-in-the-works/

14 IBM (2024), Trusted AI helps enhance NATO's critical multidomain decision making, December 2, https://www.ibm.com/products/blog/trusted-ai-enhances-nato-decision-making

15 Thales (2021), NATO Selects Thales to supply its first defence cloud for the armed forces, 25 January. https://www.thalesgroup.com/en/group/journalist/press-release/nato-selects-thales-supply-its-first-defence-cloud-armed-forces

16 NATO (2024), Adaptive Information Processing and Distribution to Support Command and Control https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=548

17 NATO (2025), NATO Cloud Conference advances innovation and IT security across the Alliance, https://www.nato.int/cps/en/natohq/news_232539.htm

18 NATO (2025), NATO Digital Backbone Architecture, https://www.nato.int/nato_static_fl2014/assets/pdf/2024/12/pdf/241213-DBRA.pdf

2. The Military Dimension

2.1. Bridging the Strategic and the Tactical Level

Adopting cloud computing within a multinational alliance requires a great deal of internal coordination between governments. Such coordination is needed at both the strategic and tactical levels. At the strategic level, Allied nations have already identified cloud computing as one of their priorities for digitising NATO. An initial challenge to cloud adoption at the NATO level is that member nations are adopting different national cloud solutions, so it will be critical to find mechanisms, both at the institutional and the infrastructure level, to integrate these different national systems and to unlock the benefits of cloud computing by integrating data to perform data analytics to support strategic thinking and command and control capabilities.

At the strategic level, Allied nations have already identified cloud computing as one of their priorities for digitising NATO.

At the tactical level, cloud computing could bring great benefits. It would lead to improved sensors and great potential for the collection, processing and analysis of large amounts of data.[19] This would benefit all forces, including those with resource-constrained nodes (e.g. mobile or dismounted soldiers) and communication-constrained nodes (e.g. underwater platforms).[20] However, there is a structural limitation to the use of cloud computing in military operations: unlike cloud services provided over the Internet, where there is high reliability, the tactical cloud must operate in a contested environment with frequent interruptions and limited or intermittent connectivity.[21] Given the difficulties of a direct link between the centralised command and the forces in the field, much of the data should ideally be processed close to where it is generated, so that it can be made available quickly to the end-users.[22] As a result, cloud computing resources need to be provided near the tactical edge or from devices (such as tactical cloudlets hosted on vehicles) on the battlefield itself.[23] By processing data locally, edge computing can reduce latency and bandwidth utilisation.[24]

There is therefore a need for a direct link between the centralised cloud (e.g. at headquarters or operations centres) with the edge and the decentralised cloud in the tactical mission domain. This is definitely an issue that needs to be addressed at the design level or very early in the process of designing NATO's cloud infrastructure, where there is more flexibility compared to the implementation part where the different cloud ecosystems will inevitably be more rigid.[25]

---

19 Magar, A., & Defence, R. (2014). *Assessing the use of tactical clouds to enhance warfighter effectiveness*. Defence Research and Development Canada.

20 Baastiaansen, H., van der Geest, J., van den Broek, C., Kudla, T., Isenor, A., Webb, S., ... & Sliwa, J. (2020). Federated control of distributed multi-partner cloud resources for adaptive c2 in disadvantaged networks. *IEEE Communications Magazine*, *58*(8), 21-27.

21 Johnsen, F. (2019). Towards Big Data in the Tactical Domain. *NATO Science and Technology Organization*.

22 Fogli, M., Kudla, T., Pingen, G., Watson, S., Bastiaansen, H., Sanchez, P., & Suri, N. A Coalition Perspective on Federated and Adaptive Clouds for Disadvantaged Tactical Networks.

23 Johnsen, F. (2019). Towards Big Data in the Tactical Domain. *NATO Science and Technology Organization*.

24 Latency is the time it takes for data or a signal to travel between two points of a system. It combines a number of delays – Response times, transmission, and processing time.

25 Wolf, W. H. (2002). Hardware-software co-design of embedded systems. *Proceedings of the IEEE*, *82*(7), 967-989.

2.2. **The Role of End-Users**

A key role in the adoption of the cloud computing strategy will be played by the end-users, in this case the armed forces themselves, who will use cloud services, particularly at the tactical level. The literature on digital innovation indicates that users are at the centre of defining and solving problems in the digital age, sometimes actively contributing to the development of new solutions.[26] This is particularly true in the military, where end-users must constantly make sense of the information they have, but also generate new information, which is then analysed and sent back by integrating it with other types of information. Creating virtuous feedback loops between the central cloud infrastructure and the forces on the ground is therefore key to stimulating innovation and increasing efficiency in NATO's adoption of cloud computing. End-users, i.e. those who use the cloud in the field, are not just passive recipients or users, but active contributors to a more efficient and innovative use of cloud computing at NATO level. It is therefore essential that the cloud strategy and the strengthening of NATO's digital infrastructure be accompanied by a parallel effort to equip forces with digital literacy and the ability to understand and use information in multiple formats from a variety of sources when presented via distributed or centralised cloud computing. Conducting this training at the multinational level could contribute to the collaboration at the design level or very early in the process that, as noted in the previous sub-section, will be critical in moving from planning to implementation of NATO's cloud strategy.

Creating virtuous feedback loops between the central cloud infrastructure and the forces on the ground is therefore key to stimulating innovation and increasing efficiency in NATO's adoption of cloud computing.

2.3. **Systems Interoperability**

Another challenge could be related on how to coordinate communication between different weapon systems, with the most advanced systems already having their own cloud computing system. In the past, communication between different weapon systems has proven to be extremely difficult. For example, Soare and her co-authors found that the F22A and F35 fighter jets have incompatible data link protocols and struggle to share information with each other. There are many other such examples.[27] This must be taken into account as the US and several European nations are developing separate combat systems, including new sixth-generation fighter projects such as the Global Combat Air Programme (GCAP) or Future Combat Air Systems (FCAS). These platforms are considered 'systems of systems' and focus on connectivity and the ability to share information between the different weapon systems that will make up these systems. They will therefore have their own cloud infrastructure. General Breton, who heads the FCAS programme, explains that "an important aspect of innovation in FCAS will be networking: currently on the Rafale [in its present configuration] the pilot mainly uses his own sensors and some information provided by the network".[28] These different systems must become integrated into the NATO cloud infrastructure so that they are interoperable. The issue of system interoperability is not only a technical one, but also a political one, and recent transatlantic friction, for example over the lack of control by some allies over F-35 software, could further complicate matters.[29] Instead, there is an urgent need for top-down guidance that prioritises interoperability and leaves parochial political or industrial interests in the background.

---

26 Chesbrough, H. (2017). The future of open innovation: The future of open innovation is more extensive, more collaborative, and more engaged with a wider variety of participants. *Research-Technology Management*, *60*(1), 35-38.

27 Soare, S. R., Singh, P., & Nouwens, M. (2023). Software-defined defence: Algorithms at war. *The International Institute for Strategic Studies*.

28 Quoted here: Gros, P. (2019). *The'tactical Cloud", a Key Element of the Future Combat Air System*. Fondation pour la Recherche Stratégique.

29 https://theaviationist.com/2025/03/10/f-35-kill-switch-myth/

3. The Industrial and Technological Dimension

3.1. Regulatory Harmonization

Implementing a cloud computing strategy means, first and foremost, harmonising data infrastructure and data sharing between the different members of the Atlantic Alliance. This means that different national governments need to develop cloud solutions that can communicate and interface with each other. Governments use different cloud computing solutions, typically choosing a combination of a 'sovereign' and secure cloud to store the most sensitive data and another cloud system for less sensitive data.[30] Different vendors, but also different rules on how to store, analyse and protect data in different countries, can pose a challenge to the adoption of an integrated NATO cloud strategy. Indeed, cloud computing has been at the centre of a transatlantic dispute. In 2018, the US Cloud Act gave US law enforcement the ability to request data stored in the US and abroad from cloud providers.[31] This was a problem because European countries were starting to become completely dependent on the big American cloud providers but saw the US Cloud Act as being at odds with European data protection rules. It was the US Cloud Act that provided the impetus for the creation of pan-European cloud initiatives, such as Gaia-X or the European Alliance for Industrial Data, to try to find a European solution to the adoption of cloud computing. Transatlantic disputes over technology regulation, as well as the recently published US Framework for the Diffusion of Artificial Intelligence, which seeks to restrict the export of computing power for use in data centres and places some European countries in Tier 1 and others in Tier 2, with different levels of restriction, could have an impact, albeit indirect, on NATO's cloud strategy.[32]

Different vendors, but also different rules on how to store, analyse and protect data in different countries, can pose a challenge to the adoption of an integrated NATO cloud strategy.

Regulatory harmonization is inextricably linked to the need to ensure technical interoperability between the different cloud solutions adopted by NATO members. The adoption of common standards can help the Alliance to have a cloud strategy where services managed by different providers can coexist. It will therefore be crucial to understand how to design API infrastructures and allow a classified cloud to coexist with the possibility of different countries and developers contributing with the repository, but also with data analysis. This is an issue, moreover, that has been highlighted by the same companies running NATO's cloud computing pilot projects. As highlighted by Thales industry executives: "When you work with NATO, in terms of IP [intellectual property], it has to be very open and it has to be as standard as possible," he said. "For me and for my company, the point is to make sure this solution will be the cornerstone of the coalition. I don't want that at the end of the day we have a jigsaw [of systems]."[33]

3.2. The Role of the Private Sector

Implementing a cloud computing adoption strategy also requires a different relationship between NATO members and the private sector. The proliferation and ever-increasing use of cloud computing resources in the commercial sector has been greatly facilitated by the reduction in cost per computing capacity and the ability of large cloud providers to scale up

30 Herr, T. (2020). Four myths about the cloud: the geopolitics of cloud computing.

31 US Cloud Act

32 Heim, L. (2024). Understanding the Artificial Intelligence Diffusion Framework. *RAND Corporation*.

33 Marchi, V. (2021). Cloudy vision: Can NATO's new deployable combat system focus the field?. DefenseNews. April 14, https://www.defensenews.com/battlefield-tech/it-networks/2021/04/14/cloudy-vision-can-natos-new-deployable-combat-system-focus-the-field/

or down as organisations' needs evolve. As the largest cloud service providers continue to expand their operations and data centre locations around the globe, data can be replicated in multiple locations to serve as backups and applications can be placed as close to users as possible to reduce latency and improve performance.[34] It is difficult, and probably unnecessary, to build a cloud infrastructure without using what is already available from the major cloud providers.

However, the strategy for cloud adoption, particularly in terms of private and commercial sector procurement, is not an easy one. The US experience in developing a general-purpose IaaS/PaaS-type cloud, the Joint Enterprise Defense Infrastructure (JEDI), has run into several intra-industry disagreements and has been challenged by the US Congress, and subsequently replaced by the Joint Warfighter Cloud Capability (JWCC).[35] It would be a mistake to think of large cloud providers as the only key players in the cloud, as the market is very diverse and diversified, especially in the PaaS and SaaS segments. In particular, on the software side, large cloud providers are creating and capturing value through co-creation with open-source communities and end users to meet their evolving needs. Software development today is increasingly driven by the day-to-day relationships between big tech companies and the best practices developed by the commercially driven open-source software community. Platforms such as the Linux Foundation, GitHub and Open Stack Foundations are central to supporting innovation in cloud computing.[36] The use of open-source groups is not without risk, but as the Ukrainian case shows, it can bring great benefits in terms of spreading technological innovation capacity or, more simply but no less importantly, sharing information.[37]

The best strategy may therefore be to adopt a multi-cloud strategy, relying on multiple providers.

3.3. **A Multi-Cloud Strategy**

Entrusting the entire cloud to a single supplier, or allowing a single supplier to manage the main infrastructure and then open the system to other participants (e.g. those managing national defence clouds), may be a good idea to optimise services and costs, as the large cloud providers offer consolidated and technologically advanced services. There would be a cybersecurity risk, not new to the cloud, as a malfunction or malicious intrusion into the main supplier's servers could cripple the alliance. This is mitigated by the fact that the major cloud providers have long had excellent cybersecurity systems in place.[38] The best strategy may therefore be to adopt a multi-cloud strategy, relying on multiple providers. This is possible and desirable, and the major cloud providers have already equipped themselves with standardised commodities (e.g. kubernets) and advanced multi-cloud strategies[39], but it should be done by design and very early in the cloud development and procurement strategy. In the case of the cloud, moving data from one provider to another is not a simple task. Once data or applications are deployed on a particular cloud infrastructure, they are often inherently tied to that infrastructure through technology ties and lock-ins. A well-know example is the difficult migration of Instagram data from AWS data centres to Meta.

34 Handler, S., Liu, L., & Herr, T. (2020) DUDE, WHERE'S MY CLOUD?, Atlantic Couuncil, https://www.atlanticcouncil.org/wp-content/uploads/2020/09/DUDE-WHERES-MY-CLOUD.pdf

35 For a critical view see Roaten, M. (2021). Death of the JEDI. *National Defense*, *106*(814), 32-33.

36 Berk, G., & Saxenian, A. (2022). Architectures of participation. *Issues in Science and Technology*, *38*(4), 62-69.

37 Cronin, A. (2023), Open Source Technology and Public-Private Innovation are the Key to Ukraine' Strategic Resilience, *War on the Rocks,* August 25, https://warontherocks.com/2023/08/open-source-technology-and-public-private-innovation-are-the-key-to-ukraines-strategic-resilience/

38 Arce, D. G. (2020). Cybersecurity and platform competition in the cloud. *Computers & Security*, *93*, 101774.

39 Oracle Expands Multicloud Capabilities with AWS, Google Cloud, and Microsoft Azure https://www.oracle.com/be/news/announcement/ocw24-oracle-expands-multicloud-capabilities-with-aws-google-cloud-and-microsoft-azure-2024-09-11/

The development of a multi-cloud strategy is inextricably linked to the development of a modular structure that can hold together different providers in the IaaS, Paas, SaaS segments. There are already models in the digital industry that could be followed and adapted to the context of a multinational alliance such as NATO. Advances in software engineering and architecture allow the creation of a central cloud architecture and the development of Application Programming Interfaces (APIs), i.e. interfaces that allow the creation of software (or an ecosystem) on which external software developers can build on top of other applications (usually through Software Development Kits), but create boundaries between one application and another. This provides a good balance between centralisation and decentralisation, between the need to protect the central infrastructure (especially in the IaaS part) and the need to open up to the contribution of various external inputs (especially in the PaaS and SaaS part). On the one hand, much research has shown how the 'opening' of a platform interface triggers innovation by complementors.[40] On the other hand, a modular architecture has also a "security" function, allowing a form of control over the strategic components of the platform (e.g. through licences that define what is allowed and what is not)[41]. The design of the API and digital interface is therefore intended to resolve the recurring tension between stimulating complementary third-party applications and maintaining platform control.

Cloud computing is therefore a key technology for enabling and facilitating the digitisation of the transatlantic alliance, and for unlocking advances in machine learning and AI.

4. Moving Forward: Cooperation by Design

Cloud computing is therefore a key technology for enabling and facilitating the digitisation of the transatlantic alliance, and for unlocking advances in machine learning and AI. This paper seeks to advance the debate by identifying some possible challenges and opportunities for NATO, from a military, industrial and technological perspective, as it moves from planning to implementing a cloud strategy. Many of the problems encountered in implementing NATO's cloud strategy are related to the need to integrate different clouds infrastructures at the national level, provided by a wide range of private actors operating in the IaaS, PaaS and SaaS segments. There is no one-size-fits-all solution, but cooperation by design or initiated very early in the process, can help solve some of the problems of defining the Alliance's cloud architecture before they become too rigid and intractable.

This applies to the military dimension, where decisions on the design of NATO's cloud infrastructure need to be taken urgently. The use of modular, open architectures, common standards and APIs across the Alliance, both on the hardware and software side, will enable different Allies to jointly develop, feed and update common infrastructures. This will simultaneously provide a connectivity layer between the central cloud and the edge cloud (thus bridging the strategic and tactical levels), structurally integrate end users into the cloud infrastructure, and enable interoperability of systems and platforms.

40 Baldwin, C., & Von Hippel, E. (2011). Modeling a paradigm shift: From producer innovation to user and open collaborative innovation. *Organization science*, *22*(6), 1399-1417.

41 Foerderer, J., Kude, T., Schuetz, S. W., & Heinzl, A. (2019). Knowledge boundaries in enterprise software platform development: Antecedents and consequences for platform governance. *Information Systems Journal*, *29*(1), 119-144.

Cooperation by design, inspired by the concept of modularity, could also foster greater connectivity between public actors (e.g. governments or armed forces) and the private sector, which is the largest producer of cloud solutions. Cloud computing is indeed an area where it is crucial to stimulate feedback loops between different types of actors in different segments of the cloud, starting with large players that own the infrastructure (IaaS) and other actors specialised at the platform or software level (Paas and SaaS). On the specific question of how to involve the private sector, NATO would do well to incentivise the supply chain practices of large players to effectively absorb and integrate innovation from SMEs, start-ups and open source groups.[42] Smaller players 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).

Finally, and this is an issue that will affect both the military and industrial dimensions, potential disputes over regulation and data protection will need to be resolved by establishing common standards that would facilitate communication and data sharing within the Alliance. This is a politically sensitive issue at the moment, especially as it ties in with Europe's broader regulatory policy and pressure from the current US administration and its private actors to relax these rules.[43] Overcoming these differences could be a good starting point for reinvigorating the EU-NATO relationship, starting with common standards on cybersecurity and cyber defence, and eventually extending to data protection. An effective NATO digital infrastructure revolves around the creation of a modular cloud architecture based on the principle of cooperation by design. It will not be easy to overcome several military and industrial challenges, but this policy brief aims to propose some pragmatic solutions as a first step in this direction.

An effective NATO digital infrastructure revolves around the creation of a modular cloud architecture based on the principle of cooperation by design.

42 Calcara, A. (2023) One Step Back, Two Steps Forward: the EU, NATO and Emerging and Disruptive Technologies. *Centre for Security, Diplomacy and Strategy* https://csds.vub.be/publication/one-step-back-two-steps-forward-the-eu-nato-and-emerging-and-disruptive-technologies/

43 Mariniello, M. (2025). On tech regulation, the European Union should be bolder. *Bruegel*, February 20, https://www.bruegel.org/first-glance/tech-regulation-european-union-should-be-bolder

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

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