INFO FLASH
Finabel
The European Land Force Commanders Organisation

FINABEL - THE EUROPEAN LAND FORCE COMMANDERS ORGANISATION

JULY 2024

# CLOUD COMPUTING IN DEFENCE

**WRITTEN BY**
ISABELLA HEALION

**EDITED BY**
ZOI SOFOLOGI

**SUPERVISED BY**
RICCARDO ANGELO GRASSI

## Introduction

Information superiority is critical to modern combat, and in a changing digital landscape, investment in cloud technology is paramount to maintaining these defence capabilities. During warfare, military forces must gather and analyse extensive data to stay ahead of adversaries. However, warfare has evolved from traditional battles on land, sea and air to encompass various interrelated types of war, including cyberwarfare, information warfare, and space warfare. The evolution of warfare is compounded by the effects of technology, which increase the speed at which war is fought and managed. However, the success of decision-making that modern warfare requires relies on the ability of information technology systems to rapidly process large amounts of data (Defence One, n.d.). New technology is outperforming these older IT systems, and European militaries must adopt new technology, specifically Cloud computing to maintain information superiority which underpins successful warfare. Cloud will likely serve as the backbone of all future digital defence capabilities; thus, investment in this technology is fundamental to maintaining information superiority. Cloud is more than just a storage platform as it can host various computing tools that assist in information superiority through situational awareness, contributing to efficient decision-making during conflict.

In 2019, the European Defence Agency financed a study about cloud computing for the defence sector (European Defence Agency, 2024). The EDA's study, Cloud Intelligence for Decision-Making Support and Analysis (CLAUDIA), ended this January (European Defence Agency, 2024). The study was run in collaboration with GMV, a private capital technology business group (GVM, n.d.), and The Information Processing and Telecommunications Center (IP&T Center) (European Defence Agency, n.d.). This paper explores the notion of cloud computing, and using the case studies of CLAUDIA, NATO and the UK Ministry of Defence (MoD), it delves into three uses of cloud in the defence sector, including source analysis, edge computing and multi-domain operations. Finally, the analysis discusses challenges associated with cloud technology, including digital sovereignty and the need for cultural shifts within the defence sector.

## What is Cloud Computing and Information Superiority?

This section focuses on a brief explanation of cloud computing to preface the analysis of cloud computing applications in defence. Cloud computing refers to "the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale." (Microsoft Azure, n.d.). Cloud computing providers like Microsoft can deliver storage and intelligence, offer a platform for building applications, and analyse data (Microsoft Azure, n.d.). It differs from the traditional approach of owning and maintaining physical data systems installed on premises, which requires significant electricity funds for power and cooling (IBM, 2024). By offloading some or all of this computing to cloud-based infrastructure through an external company or companies, civil companies and even organisations such as the Ministry of Defence can pay-by-use, and save significantly on costs (Microsoft Azure, n.d.).

## What is Cloud Computing and Information Superiority?

This section focuses on a brief explanation of cloud computing to preface the analysis of cloud computing applications in defence. Cloud computing refers to “the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale.” (Microsoft Azure, n.d.). Cloud computing providers like Microsoft can deliver storage and intelligence, offer a platform for building applications, and analyse data (Microsoft Azure, n.d.). It differs from the traditional approach of owning and maintaining physical data systems installed on premises, which requires significant electricity funds for power and cooling (IBM, 2024). By offloading some or all of this computing to cloud-based infrastructure through an external company or companies, civil companies and even organisations such as the Ministry of Defence can pay-by-use, and save significantly on costs (Microsoft Azure, n.d.).

Cloud computing is set to play an increasingly significant role in information superiority, which underpins modern defence capabilities. Conventional European military operations integrate command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) (Defence One, n.d.) with weapons systems and military forces. Defence capabilities hinge on information superiority and precision (Thales, 2019). This demands reliable, accurate and quick delivery of data and intelligence to forces through ‘real-time connectivity’ and ‘precise lethality’ (Thales, 2019). Particularly in urban conflicts, the presence of civilians amplifies the significance of military precession (Thales, 2019). With increased access to technology such as sensors, militaries can receive vast amounts of information. However, outdated approaches hinder the efficient processing of data into actionable intelligence and its timely delivery to the front line (Opiah, 2023).

Information superiority, critical to defence capabilities, greatly benefits from cloud computings scalability and flexibility in receiving and processing large amounts of data quickly. (IBM, 2024). Cloud computing can increase the speed of critical information processing in conflict. The “tactical edge” refers to personnel or platforms operating on a front line or battlespace close to the adversary (NIST Computer Security Resource Centre, n.d.). They are fully engaged in tactical operations, and highly dependent on the accuracy of information systems (NIST Computer Security Resource Centre, n.d.) Often, the edge does not have enough computation power to process and analyse data as needed. Traditionally, data gathered on the edge, such as from sensors and equipment, is sent to a centralised location to be processed, before being sent back as actionable intelligence. (Opiah, 2023). Consequently, data reliability is reduced when it reaches the edge, hindering real-time decision-making (Opiah, 2023). However, implementing information superiority in the defence sector encounters several challenges due to the sensitive and classified nature of military information and intelligence.

## Cloud and Situational Awareness

The European Defence Agency's CLAUDIA demonstrates that cloud computing can offer robust source analysis, significantly enhancing situational awareness and preventative capabilities in defence.  Hybrid warfare, characterised by a combination of disinformation tactics, conventional warfare, non-conventional warfare and cyberwarfare, is becoming increasingly prevalent (NATO, 2024). Consequently, gathering intelligence from digital sources and discerning between fake and genuine can be vital to combating threats from non-state actors such as insurgents, terrorist organisations and hackers (European Defence Organisation, 2021, 44). The EDA developed SWAN through CLAUDIA, a Software Analysis platform tested on different cloud-based capabilities (European Defence Organisation, 2021, 44). The software was used to detect disinformation from open-source information, such as social media, media newspapers and websites (European Defence Organisation, 2021, 44). Applying of this function across European forces could result in significant security enhancements because using real-time insights leads to proactive measures against hybrid threats.

This pilot project led to several new ideas to be explored in the future, including the capability of the Cloud to prevent cyber-warfare,  "demonstrating how artificial intelligence could exploit the cloud by analysing open-source data and generate intelligence about early signals regarding potential hybrid warfare activity" (European Defence Organisation, 2021, 44). Ignacio Montiel-Sanchez, previous EDA project officer for CLAUDIA, highlighted the potential expansion of this capability to supplement Common Operational Pictures, also known as COP (European Defence Organisation, 2021, 45). COP is a decision-making tool based on up-to-date information from multiple sources merged into a single display (MAG, 2023). COP functions as a go-to piece of information for decision-making in military operations. Sachez noted the SWAN's ability to supplement COPs by generating a map that geo-locates recorded cyberattacks, recognises their nature and calculates the possibility of a cyberattack against "military operations and critical infrastructure" (European Defence Organisation, 2021, 45). Attacks on critical infrastructure include energy systems, transport networks, communication systems or government services and protecting them is essential for the "security of the EU and the well-being of its citizens" (European Commission, n.d.). As the Cloud facilitates easy and quick access to information from various locations, units have better situational awareness when making decisions regarding cyber threats. This information could also be shared with other government agencies.In an increasingly digitised world, the Cloud presents an advanced, fast and adaptable system to analyse information critical to tactical and preventative measures in defence.

## Edge Computing & Information Processing

CLAUDIA has demonstrated that Cloud computing can bring information processing closer to the "edge". After delivering CLAUDIA, the EDA will focus on planning projects that address edge computing planning to help reduce this data lag (European Defence Organisation, 2021, 45). The US Air Force has already tested this concept on its F-35s, using the multifunction advanced data link (MADL) and data sensors onboard each aircraft to share information amongst a squadron (Lee et al., n.d.).This shared information creates a single comprehensive analysis of threats based on the unique vantage points of each aircraft (Lee et al., n.d.). The concept can also be applied to tanks, drones and the "digital soldier", operating as instruments that collect and distribute information on-site (Lee et al., n.d.).  Edge computing improves information superiority, safety and operational efficiency by conducting real-time analysis on the spot.

## Interoperability: Multi Domain Operations and Data Sharing

Cloud is essential for supporting multi-domain operations, as demonstrated by the NATO Allied Command Transformation. Within the NATO structure, are five distinct operational areas: Maritime, Land, Air, Space and Cyberspace, which traditionally function as separate entities (NATO, 2023 -a). However, multi-domain interoperability becomes increasingly important as warfare and the digital landscape evolve. NATO states that integrating these military domains with "instruments of power and external stakeholders" is also crucial (NATO, 2023 -a). Unlike joint operations, multi-domain operations prioritise military collaboration with non-military assets. These non-military assets refer to member states' various departments or agencies, such as the Ministry of Foreign Affairs. In NATO,  "a secure and scalable Cloud environment [will] serve as the foundation of the Digital Backbone and to enable Multi-Domain Operation" (NATO, 2023 -b). At the same time, stakeholders are external groups such as academia and private industries with whom NATO maintains business partnerships. Cloud-enabled data sharing also supports interoperability between different classification levels (Microsoft, 2021). In 2021, the US Government enabled Microsoft Azure Top Secret to simplify data segregation amongst different classification levels (Microsoft, 2021). Initiatives like these offer a seamless approach to data sharing, but outdated legacy systems still threaten the competitiveness of defence organisations such as NATO (NATO, 2023). As warfare evolves and technology advances, the demand for interoperability is escalating. Cloud computing is highly beneficial in facilitating data sharing across various defence classifications levels and with the civil sector.

## Championing the adoption of Cloud & Recruitment

A culture shift and recruitment expansion are needed to transition to cloud-native operations in defence. Cloud implementation will be achieved most effectively through close collaboration between teams, avoiding the traditional siloed approach. The UK Government's Ministry of Defence (MoD) has suggested that the implementation of its Cloud program should rely on a sector-wide vision of Cloud as a "pan-Defence priority" (UK Ministry of Defence, 2023). UK Mod views the Cloud as the "digital backbone" of powerful systems, including Artificial Intelligence, the Internet of Things and Big Data Analytics (UK Ministry of Defence, 2023). Therefore, leaders within the defence sector should champion its uptake as a 'campaign' rather than a project (UK Ministry of Defence, 2023). Senior defence leadership explicitly stated a need to recruit talent with "the cloud skills and capabilities" required to support this transition (UK Ministry of Defence, 2023). While the Cloud will facilitatean increasingly automated defence sector, it is critical to build an adaptive culture and support highly skilled IT recruits to assist in this transition.

## Data Sovereignty & Data Security

A prevailing challenge with the Cloud in defence applications is data sovereignty. Europe lags behind the United States, which leads the Cloud infrastructure market (McKinsey, 2024). There is still a significant gap between the EU and the US in adopting Cloud technology for military use, raising concerns about Europe's geopolitical influence (Deloitte, 2023). The US Cloud Act, established in 2018, alarmed European authorities, denoting the US can access data stored by US companies inside or outside the US to conduct criminal investigations (Wood & Lewis, 2023). In 2022, it was reported that US Cloud providers, mainly Amazon, Google and Microsoft, dominated the global Cloud market by 75% (Wood & Lewis, 2023). Consequentially, European member states are limited in their choice of Cloud providers, resulting in "costs and...gaps in capacity for European industry" (Wood & Lewis, 2023). The Cloud Act was incompatible with Article 48 of the EU's General Data Protection Regulation, as data can only be transferred to foreign authorities if authorised by an existing international agreement (Wood & Lewis, 2023; European Union, 2016, Article 48).

Consequently, the European Commission is advocating for the EUCUS (European Cloud Services Scheme), which would place regulations for data sovereignty to prevent EU data from being accessed by non-EU actors (Voci et al., 2022). Supported by Spain, Italy and France but rejected by the Netherlands, Denmark, Estonia, Greece, Ireland, Lithuania, Poland and Sweden - the issue is proving contentious (Voci et al., 2022). These nations are concerned that although the scheme seeks to champion European companies, it claims it is politically motivated rather than based on "sound technical standards"(Voci et al., 2022). EUCUS poses potential risks to European competitiveness by threatening partnerships with established and advanced companies from allied nations (Voci et al., 2022).

Establishing trust in Cloud computing in the civil sector could lead to the widespread adoption of Cloud technology across Europe in the defence sector. In 2021, Peter Altamaier, German Federal Minister of Economic Affairs and Energy, alongside Bruno Le Maire, French Minister of Economy, established a privately funded Cloud project, Gaia-X, to secure European Digital Sovereignty (EURACTIV, 2020).The project aims to create a secure data infrastructure for Europe, bringing together technology researchers, users, and providers while boosting EU competitiveness in the market (Gaia-X, 2023). Gaia-X also claims that Cloud is the backbone of global economies; however, the adoption of Cloud technology in Europe is less than 25% in the civil sector, reflecting a lack of trust (Gaia-X, 2023). Despite these data sovereignty concerns, European countries like the UK have contracts with American Cloud providers, namely Amazon Web Services for its Ministry of Defence (Amazon Web Services, n.d.). Therefore, data sovereignty is a prevailing concern hindering the uptake of highly advantageous Cloud services in the European defence sector.

## Conclusion

As the backbone of diverse digital capabilities, Cloud computing can provide a crucial edge in maintaining informational superiority in modern warfare. Tools such as SWAN can revolutionise data analysis to counter disinformation and prevent cyberwarfare, essential in combating hybrid warfare. Moving forward, the EDA will explore the Cloud's ability to enhance information processing and decision-making, already demonstrated by the U.S. Air Force's F-35 MADL system (European Defence Organisation 2021; Lee et al., n.d.). Cloud computing could also facilitates interoperability across various defence classification levels and with the civil sector. However, transitioning to a cloud-native necessitates the recruitment of highly skilled IT specialists in Cloud technology and leadership to champion its implementation (UK Ministry of Defence, 2023). Another key concern is data sovereignty and the global dominance of US companies in the Cloud technology sector. While initiatives like the European Cloud Services Scheme and Gaia-X are being promoted, there is disagreement over the best possible strategy and a clear need to balance European innovation with international partnerships and data security. European military organisations must recognise the associated risks and develop mitigation strategies. Ultimately, the defence sector may witness Cloud technology becoming the backbone of digital capabilities in the future. In conclusion, strategic and proactive investment in Cloud infrastructure is critical to enhancing information superiority, situational awareness, information processing and interoperability in the digital age of evolving warfare.

## Bibliography

Amazon Web Services. (n.d.). AWS for UK National Security and Defence. AWS Amazon. https://aws.amazon.com/government-education/worldwide/uk/national-security-and-defence/?wwps-cards.sort-by=item.additionalFields.sortDate&wwps-cards.sort-order=desc.

Barocca, J. G., Batista, S. B. & Ferrer, B. A. (2023, October 26). Cloud sovereignty in Europe. Deloitte Insights. https://www2.deloitte.com/us/en/insights/technology-management/cloud-sovereignty-three-imperatives-for-the-european-public-sector.html.

Betley, B., Dip, H., Jensen, B. & Mühlreiter, B.. (2024, April 2). The state of cloud computing in Europe: Increasing adoption, low returns, huge potential. McKinsey. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-state-of-cloud-computing-in-europe-increasing-adoption-low-returns-huge-potential.

Brüls, H. (Ed.). (2021). Innovation Corner: Modern Computing for Armed Forces: Reaching fro the Cloud. European Defence Matters (21), 44-45. https://eda.europa.eu/docs/default-source/eda-magazine/edm21-single-1-48-web.pdf.

European Commission. (n.d.). Critical infrastructure protection. EU Science Hub. https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en.

European Defence Agency. (2024, January 25). 'Combat cloud': EDA study shows benefits of cloud computing for EU militaries. European Defence Agency https://eda.europa.eu/news-and-events/news/2024/01/25/combat-cloud-eda-study-shows-benefits-of-cloud-computing-for-eu-militaries.

European Defence Agency. (n.d.). CLAUDIA - CLOUD INTELLIGENCE FOR DECISION MAKING SUPPORT AND ANALYSIS. In European Defence Agency. Retrieved July 11, 2024, from https://eda.europa.eu/docs/default-source/posters/7---claudia---cloud-intelligence-for-decision-making-support-and-analysis.pdf.

Gaia-X. (2023, February 15). Creating Trusted Data Infrastructure, Gaia-X. https://gaia-x.eu/news-press/gaia-x-creating-trusted-data-infrastructure/.

Lee, K., Dupier, G., & Pisano, J. (n.d.). How the U.S. Military Is Using Edge Computing. Booz Allen. https://www.boozallen.com/s/insight/blog/how-the-us-military-is-using-edge-computing.html.

MAG Aerospace. (2023, July 12). Unlocking the Benefits of a Common Operating Picture. MAG Aerospace. https://www.magaero.com/unlocking-the-benefits-of-a-common-operating-picture/.

Microsoft Azure. (2021, August 16). Azure Government Top Secret now generally available for US national security missions. Microsoft Azure. https://azure.microsoft.com/en-us/blog/azure-government-top-secret-now-generally-available-for-us-national-security-missions/.

Microsoft Azure. (n.d.). What Is Cloud Computing? A beginner's guide Microsoft Azure. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/.

NATO ALLIED COMMAND TRANSFORMATION. (2023, October 5 -a). Multi-Domain Operations in NATO - Explained – NATO's ACT. NATO ACT. https://www.act.nato.int/article/mdo-in-nato-explained/.

NATO ALLIED COMMAND TRANSFORMATION. (2023, October 16 -b ). Empowering NATO's Multi-Domain Operations Through Digital Transformation. NATO ACT. https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/.

NATO. (2024, May 7). Countering hybrid threats. NATO.https://www.nato.int/cps/en/natohq/topics_156338.htm.

NIST Computer Security Resource Centre. (n.d.). tactical edge – Glossary. CSRC. NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/tactical_edge.

Opiah, A. (2023, September 19). Tactical edge cloud computing: Enhancing military battlefield efficiency. Edge Industry Review. https://www.edgeir.com/tactical-edge-cloud-computing-enhancing-military-battlefield-efficiency-20230919.

Perry, W., Signori, D., Boon, J., & National Defense Research Institute. (2004). Exploring Information Superiority: A methodology for measuring the quality of information and its impact on shared awareness. In Prepared for the Office of the Secretary of Defense. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1467.pdf.

Susnjara, S. & Smalley, I.. (2024, February 14). What Is Cloud Computing? IBM. https://www.ibm.com/topics/cloud-computing.

Stolton, S. (2020, June 4). Digital Brief: The Gaia-X generation.EURACTIV. https://www.euractiv.com/section/digital/news/digital-brief-the-gaia-x-generation/.

UK Ministry of Defence. (2023, February 2). Cloud Strategic Roadmap for Defence. GOV.UK. https://www.gov.uk/government/publications/cloud-strategic-roadmap-for-defence/cloud-strategic-roadmap-for-defence#addressing-some-practical-issues.

Thales. (2019, March 18). For today's fighting forces, information superiority means battlefield superiority. Thales. Retrieved July 11, 2024, from https://www.thalesgroup.com/en/worldwide-defence/land-forces/magazine/todays-fighting-forces-information-superiority-means.

Voci, V., Workman, G., & Muñoz, D. (2022, December 5). Issue Briefing: The European Union’s Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS). U.S. Chamber of Commerce https://www.uschamber.com/security/cybersecurity/issue-briefing-the-european-unions-proposed-cybersecurity-certification-scheme-for-cloud-services-eucs.

Wood, G., & Lewis, A. (2023, March 29). The CLOUD Act and Transatlantic Trust. Center for Strategic and International Studies.https://www.csis.org/analysis/cloud-act-and-transatlantic-trust.