INFO FLASH
Finabel
European Army Interoperability Centre

New Developments in Cloud Initiatives in Land Forces - Advantages and Challenges

WRITTEN BY CATERINA POZZI

Image credits: https://unsplash.com/s/photos/cloud-technologies

We have entered a modern era of warfare, where the battlefield is no longer exclusively physical but also digital. Information is vital to national security. In this context, the storage and process of data become crucial to guarantee mission success (Department of Defense, 2018). An effective ally to do so is represented by cloud technologies that empower the military infrastructures. Cloud technologies or services are defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011). Cloud services are an information technology model that allows information and resources to be available via the Internet (Al-Gharibi, 2019). As a consequence, reliance on the traditional IT model is reduced.

The main differences between conventional IT modes are on-demand, self-service, - broad network access, resource pooling, elasticity, and measured service (Mell & Grance, 2011). Cloud technologies enhance productivity and efficiency by making data and information available to all units situated in different geographical areas. Additionally, they are flexible and reduce costs thanks to on-demand services (Al-Gharibi, 2019). Investing in new Cloud Computing technologies is part of a broader strategy that aims to reach digital sovereignty and reduce dependence on external providers (Pollet, 2021).

Cloud computing is fundamental to ensure national security and the ability to detect and quickly respond to threats, analyse and secure data storage, and ultimately allow armies to make data-driven decisions. Despite being overall beneficial, these technologies also present some challenges to be discussed. Finally, it is interesting to observe the different approaches of European Union (E.U.) member states and the United States (U.S.).

The first advantage of developing cloud space and services is organising and securing information across military sectors and geographical areas. The collaboration entailed in the process enables the joint force to synchronise operations (Spalding, 2009). Thus, adopting the Internet rather than fixed IT infrastructures as the primary network source and rapidly developing processes and procedures is necessary to embrace cloud computing. A web-enabled system will combine ongoing missions and programs into a single interface, with the ultimate goal of bringing significant amounts of data from several sources into a common operating picture (Pomerlau, 2022). This enables all military units' productivity and efficiency by allowing them to access and use easily a well-organised set of data. The same data is reproduced across all the military operations in different geographical areas.

The second advantage of cloud technologies and systems is that they allow the continuity of operation in times of crisis or operational disruption. They are a key instrument in addressing these challenges and ensuring that missions are effectively executed due to their distributed nature. In addition, enterprises providing clouds will offer support for failover during disruption and recovery from the operational cyber incident (Department of Defense, 2018). Most cloud providers achieve this task by using multi-region zone architectures that work hand-in-hand with the use of secure Cloud Access Points (CAPs).

Ultimately, the advantages described above have a significant impact respectively on information superiority and enhanced resiliency. Information superiority is given by enhanced operational flexibility and effectiveness through a web-enabled system that unifies data and information from multiple levels into a common operating picture. The ability to continue operations during crisis and disruption significantly impacts the resilience of states' security and defence. According to E.U. Commission, "Resilience is the ability of an individual, a household, a community, a country or a region to withstand, cope, adapt, and quickly recover from stresses and shocks such as violence, conflict, drought and other natural disasters without compromising long-term development" (European Commission, 2016). In this light, resilience is boosted as cloud services allow to experience less damage or recover quicker, for example, in cases of cyber-attacks on infrastructure.

Governments rely on critical intelligence to make vital security decisions. Even though the advantages of using cloud services in land forces are evident, some challenges need to be addressed. Securing information in the cloud is possibly the biggest concern. Data stored in the cloud is always accessible, making it vulnerable to misuse by anybody who has the resource to exploit the system. Cloud spaces need to be completely safe from mismanagement; data and information should be protected by any cyber-attacks or from being leaked.

Thus, effective use of these technologies in defence and security requires a protected cloud environment and trustworthy and skilled users. Although governments are aware of the security risks, they also know that the advantages exceed the disadvantages and are implementing cloud computing among their IT strategies. To manage the security risks, many governments have developed security guidelines to protect the users' confidentiality, integrity, and availability (Al-Gharibi, 2019). These guiding principles inform future decisions on the use of clouds. First, cloud solutions need to be built so that they never put combatants and their missions at risk. Therefore, it is required that the teams continuously produce assessments during and after the use. Finally, defence departments need to create a culture that is appropriate for adaptability in modern technology, where the workforce can effectively use clouds and that is actively and continuously trained. A guiding strategy will thus help develop an approach for managing the data, the infrastructures, and the applications of cloud spaces. One potentially effective solution might be pooling data, allowing systemic protection against disruption.

While the Western world is aware of the advantages and the challenges of cloud services and actively planning to make significant steps forward, there are some disparities in approaching the topic in the E.U. and U.S. For the current year, bringing new cloud and data capabilities to the tactical sector is a top priority for the U.S. Army following last year's Digital Transformation Strategy. Firstly, the U.S. will actively work on merging all the current missions in a single operating picture while also modernising the platform (Pomerlau, 2022). Some units are already being trained to this aim. Furthermore, Maj. Gen. Robert Collins, who leads the Program Executive Office for Command, Control, Communications-Tactical, stresses the importance of having precise and flexible data fabric to allow information to move from the enterprise level to the tactical and collaborating with machine learning and artificial intelligence (AI) (Pomerlau, 2022). The U.S. will soon implement the first experiment of Army's cloud outside the U.S., in the Indo-pacific region.

The E.U. is also planning to become an attractive and secure data economy by joining forces in cloud capacities by 2025 and is planning to invest €4-6 billion on data spaces and cloud services (European Commission, 2020). Furthermore, the Commission has welcomed the member state's proposal on E.U. cloud federation by combining private, national and E.U. investment efforts (European Commission, 2020).

In the defence industry, around €100 million of the European Defence Fund (EDF) will be dedicated to critical technologies, including artificial intelligence and clouds for military operations (European Commission, 2021). Nonetheless, there is one limitation to consider: Since cloud computing is already present in the private commercial sector and enterprises, member states already rely on this technology. However, there is an apparent discrepancy in capacities among them. Data shows that cloud computing services of medium-high sophistication are prevalent in the Nordic countries, with more than 60% of Finnish enterprises purchasing them, followed by Sweden and Denmark. Bulgaria, at the bottom, counts only 10%; hence the gap between the top and low performances is notably high (European Commission, 2021). To conclude, to effectively transfer this valuable technology to the defence sector and ensure interoperability among European armies, member states first need to homogenise their critical technology capabilities.

In conclusion, cloud technologies are a precious instrument to succeed in modern warfare, where information and data are a crucial part of the military. As observed, clouds have a series of advantages, such as storing and making data available to all the units and geographical areas, allowing the continuity of operations in times of disruption, ultimately enhancing information superiority and resilience. The security of cloud services represents the main challenge, and steps need to be taken to provide guidelines to manage the security risks. While the U.S. and the E.U. have acknowledged the importance of cloud services for the countries' security and allocated resources and funds to this aim, the E.U. member states still experience discrepancies in the homogenisation of cloud capabilities. These differences should be first solved to effectively use critical technologies for defence purposes and ensure interoperability between national armies.

Bibliography

Al-Gharibi, M. (2019). Government Cloud Computing Security Guidelines: Similarities, Differences, and Gaps Related to Cyber Warfare. Deakin University Centre for Cyber Security Research and Innovation, 46-52. Retrieved from https://www.researchgate.net/publication/346970281_Government_Cloud_Computing_Security_Guidelines_Similarities_Differences_and_Gaps_Related_to_Cyber_Warfare

Department of Defense. (2018). DoD Cloud Strategy. Department of Defense. Retrieved from https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF

European Commission. (2016). Building Resilience: The EU's approach. Retrieved from European Commission: https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/EU_building_resilience_en.pdf

European Commission. (2020, February 19). A European strategy for data. Retrieved from European Commission: https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf

European Commission. (2020, October 15). Towards a next generation cloud for Europe. Retrieved from European Commission: https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe

European Commission. (2021, June 30). Defence Industry: the Commission kick-starts the European Defence Fund with €1.2 billion and awards 26 new industrial cooperation projects for more than €158 million. Retrieved from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3325

European Commission. (2021). Digital Economy and Society Index (DESI) 2021. Retrieved from European Commission: https://digital-strategy.ec.europa.eu/en/policies/desi

Bibliography

Mell , P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute for Standard and Technology, 2, 3. Retrieved from http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

Pollet, M. (2021, December 15). European Commission launches new data and cloud alliance. Euractiv. Retrieved from https://www.euractiv.com/section/digital/news/european-commission-launches-new-data-and-cloud-alliance/

Pomerlau, M. (2022, January 13). US Army plans to make big advances in cloud initiatives this year. Defense News. Retrieved from https://www.defensenews.com/it-networks/2022/01/13/us-army-plans-to-make-big-advances-in-cloud-initiatives-this-year/

Spalding, N. S. (2009). Net-Centric Warfare 2.0: Cloud Computing and the New Age of War. Air war College, Air University. Retrieved from https://www.researchgate.net/publication/235082301_Net-Centric_Warfare_20_Cloud_Computing_and_the_New_Age_of_War