VAUBAN PAPERS

[CLOUD COMPUTING FOR MILITARY OPERATIONS: CHALLENGES AND OPPORTUNITIES]

SERIES 2

avisa partners

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

The Vauban Papers are a series of publications dedicated to the impact of digital transformation on the Armed Forces and the conduct of operations, published by Avisa Partners in partnership with VMware.

The Papers are both the result and follow-up to the discussions held during the Vauban Sessions, an annual conference organised by Avisa Partners and the Rapid Reaction Corps - France (CRR-FR) in Lille.

The 2021 edition brought together some 120 participants and featured speakers from NATO, European Union institutions, national Armed Forces and defence industry from 23 Allied nations.

The ideas and opinions expressed in this document are those of the authors and do not necessarily reflect the position of Avisa Partners Group or VMware. Avisa Partners retains editorial independence at all times in its work.

ABOUT AVISA PARTNERS

Avisa Partners is a global economic intelligence, international affairs and cybersecurity group. **Avisa Partners' Cybersecurity and Strategy branch** supports its public and private sector clients in decision-making, risk management, impact assessments, digital transformation, outreach and expansion in France, Europe and beyond. Its consultants combine a forward-looking vision with a functional approach with operational knowledge of the sectors in which they operate.

FOR MORE INFORMATION, PLEASE VISIT:
avisa-partners.com

avisa partners

ABOUT VMWARE

VMware software powers the world's complex digital infrastructure. The company's cloud, **app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device**. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact.

FOR MORE INFORMATION, PLEASE VISIT:
vmware.com/company.html

vmware®

COLLECTION

VAUBAN PAPERS

CONTENTS

VAUBAN
SESSIONS

#5 CLOUD SERVICE MODELS FOR DEFENCE

MARCH 2023

avisa partners

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

FOREWORD

The “Vauban Papers” are part of a resolutely operational approach to digital transformation. They are based on the "Vauban Sessions" initiated by the Rapid Reaction Corps - France (RRC-Fr) in Lille, which each year brings together operational commanders, senior representatives from the EU and NATO, industrial players and national decision-makers. The first series of “Vauban Papers” focused on the impact of digital transformation on operations, both at the leadership and the execution level, its benefits and challenges. They also highlighted the need for incremental collaboration between operational staff, expert services and digital technology companies to bring the best of new technologies to the armed forces.

Not surprisingly, it soon became clear that the exploitation of the mass of operational data, whatever its origin, is both the key to and the strategic objective of the digital transformation of our armed forces. This raises the question of where to locate these gigantic databases. To answer this crucial issue, a technical approach alone is not sufficient, but new digital technologies, in particular cloud computing, open up promising horizons. Firstly, one must establish the essential principles to be met in the location, use and dissemination of operational data. A non-exhaustive list will include sovereignty, which does not exclude selective sharing within a collective organisation (EU, NATO, etc.) or a coalition, accessibility and almost instantaneous availability, reliability and its corollary, resilience. Current information systems, highly centralised and specialised by nature, do not meet all of these requirements. Certain developments in tactical data link networks (e.g. Link 16), however, have paved the way to extended connectivity, as a first step towards the operational grail of the “combat Cloud.”

This Vauban Paper makes clear that there is no magical solution today, be in a private, public or even hybrid Cloud, or in the various levels of on-demand services that allow data to be processed, shared and stored: provision of shared applications, Software as a Service (SaaS), IT infrastructures hosted in the Cloud, Infrastructure as a Service (Iaas) or outright complete ready-to-use platforms and Platform as a Service (Paas). Ongoing evolutions in data management will play an important role in these choices, as will the advent of “Edge Computing” which will make it possible to process part of the operational data closer to the combatants. The Cloud, which has now reached a high level of maturity in civilian activities, is now at the heart of operational systems as an essential element in the cognitive battle, the acceleration of decision-making loops, and the optimisation of all the capabilities implemented in the various environments and fields of combat.

This new series of Vauban Papers aims to support operational decision-makers in the definition, in collaboration with the actors of the digital space, of the most appropriate solutions to meet the demanding needs generated by a new geostrategic context. For our armed forces, digital transformation is no longer an option but an imperative to guarantee their freedom of action and operational efficiency.

General (rtd.)
Jean-Paul PALOMÉROS
Former Supreme Allied Commander
NATO Transformation (SACT)
and Senior Advisor at Avisa Partners

CLOUD SERVICE MODELS FOR DEFENCE

CONTRIBUTORS

Axel DYÈVRE
Partner
AVISA PARTNERS

Marie KETTERLIN
Analyst
AVISA PARTNERS

The number of connected devices and terminals (Internet of Things, IoT) has increased significantly since the mid-2000s. Digital transformation, coupled with the increase in network speeds, has resulted in the progressive inclusion of these connected objects in the conduct of operations. This equipment represents a significant operational advantage: the exchange of information at all levels and in "near-real time" makes it possible to shorten the decision-making loop and to deploy a collaborative combat model. The data generated by connected devices (whether by human action or automatically) has led to an explosion in volumes of data exchanged on networks via these connected terminals.

In this context, armed forces are now faced with a two-dimensional **connectivity challenge**. The **volumes of data** produced and used in the field have increased tenfold, making the issue of data exchange - and therefore network access - crucial. The need for "visual discretion" and reduced electromagnetic footprints of radio exchanges are driving the development of networked data exchanges. Moreover, missions generally take place in **degraded conditions**, marked by difficult access to networks, due to adversary actions and/or constraints of the terrain. To avoid dysfunctions linked to network latency, units must be able to work in both "connected" and "disconnected" mode, according to more or less localised connection solutions. This objective is based on three conditions: power requirements, storage capacity and resource allocation.

The framework defined by these different elements no longer favours "local" operations alone: it is no longer possible for armed forces to rely solely on the use of resources stored in terminals deployed in the field. **Cloud-based operations** offer an interesting solution, defined by the **remote hosting** of data and applications.

The use of the Cloud requires accessibility and availability of networks to allow access to data, applications or computing power hosted on remote servers. Connected objects take on the role of **interfaces**, allowing access to content, services and applications stored on these servers more or less remote from the field.

Clouds come in **different architectures** and offer a variety of **services**:

- → **In a public Cloud** architecture, resources are hosted on a provider's server, shared with other users. These resources are available on demand via the Internet to their owners and guests.
- → **A private Cloud** is based on the storage of data on a server reserved for the exclusive use of a single organisation, and can be hosted by the organisation itself - on its network or via the Internet by VPN or tunnel - or by a third party. The private Cloud offers advantages in terms of control, protection and confidentiality of hosted data and applications. This architecture is more costly than a public Cloud and is mainly implemented by very large organisations.
- → **Hybrid Clouds combine** private and public Cloud infrastructures: one part of the Cloud architecture is physically hosted on the organisation's premises, another part by one or more external providers. The data and applications are then distributed according to their sensitivity or the importance of their availability. A hybrid Cloud combines the cost and scalability advantages of a public Cloud with the security of a private Cloud.

A Cloud architecture can also be deployed around **several cloud computing services,** i.e. on-demand access via the Internet to computing resources - such as computing power and storage capacity - from different providers: a **"Multi-Cloud"** structure. Each architecture is based on a unique combination of public and/or private Clouds. Content, data, software and applications are then distributed among the different servers.

To shorten response times and/or save bandwidth, **"Edge Computing"** proposes a distributed computing architecture which brings computing and storage closer to data sources via connected devices or the use of local servers.

CLOUD SERVICE MODELS FOR DEFENCE

These network architectures ultimately make it possible **to distribute** these masses of data, **to rely on "external" applications or computing power** from a local networked device.

The deployment of forces to **distant theatres and at ever shorter intervals** makes it necessary to shorten the information loop in degraded environments and operating contexts. To achieve this, the sharing, processing and storage of information must become an almost "tailor-made" service, on demand, adapted to the procedures and conditions on the ground. The Cloud, which can be deployed at **three levels of intervention,** offers possibilities for communication and information sharing:

- **Application:** Software as a service **(SaaS)** is a software distribution model in which a Cloud provider hosts applications and makes them available to users via the Internet - usually through a browser - on a paid subscription basis. In this "software on demand" model, the provider gives customers network access to a single copy of an application. Customer data can be stored either locally, in the Cloud, or both.
- **Infrastructure:** Infrastructure as a Service **(IaaS)** provides on-demand access to Cloud-hosted IT infrastructure - servers, storage capacity and network resources - that customers can feed, configure and use, while the Cloud service provider hosts, manages and maintains the hardware and IT resources in its own data centres. IaaS users access the hardware via an internet connection and pay for this use on a subscription basis.
- **Platform:** Platform as a service **(PaaS)** provides on-demand access to a complete, ready-to-use platform hosted in the Cloud for developing, running, maintaining and managing applications.
  The Cloud service provider hosts, manages and maintains all the hardware and software included in the platform - servers, operating system, storage, networking, databases - as well as the associated security services.

For the military, these technologies and their uses involve **several issues**, starting with the challenge of **Cloud operation**, to ensure above all a **proper distribution** of computing resources between the different levels in order to guarantee the availability, resilience and possible autonomy of each level. This includes the issue of the physical storage of machines. The physical infrastructure of a Cloud architecture can be hosted within the organisation that uses it (private, public) and deployed through its own networks. This solution is particularly expensive: the Cloud relies on a need for connectivity, availability and redundancy for security, which is both costly and complicated to implement. The hybrid Cloud allows for the management of data and its distribution, between "internal" and "external." A "multi-Cloud" architecture allows data to be distributed with a high level of security, making it virtually impossible to rebuild in the event of an attack. However, any advantage creates a dependence and these architectures (hybrid, multi-Cloud) increase the dependence on networks.

Shortening the decision making loop is the key operational re levance of using cloud computing for the military. The exchange of data and the use of networked data processing services can, in principle, improve networked combat by linking the entities which make up the collaborative combat architecture. Cloud technologies allow a situation to be shared as quickly and accurately as possible, ensuring a better understanding of the environment (situational assessment) and better coordination of fire, ultimately contributing to accelerate a manœuvre.

CLOUD SERVICE MODELS FOR DEFENCE

CONTRIBUTOR

Major General (rtd.) Sully BARBE
Former chief of communication and information systems and cyberdefence division
FRENCH RAPID REACTION CORPS HQ

Information supremacy - defined as the ability to collect, process and disseminate a continuous flow of information or to deprive him of it - enables operational superiority. Information comes from the correlation of data produced by different sources or sensors, texts, figures or a mixture of both, but also from tables and graphs. Converted into knowledge and decision, it provides an advantage to armed forces able to combine its traditional effects with those of the immaterial fields.

Mastering cloud computing, artificial intelligence and big data offers this capacity for transformation. As a set of resources that can be shared according to users' needs and consumed on demand, the Cloud provides greater means and virtually unlimited computing power. It is an essential objective for modern armies. They will thus be able to store, manage and exploit the exponential volume of data produced by their combat platforms, the objects connected to them, and the environment in which they operate. They will benefit from the high-performance tools needed to process this information using algorithms, in a timeframe compatible with the pace of operations at the strategic or tactical level.

Examples of Cloud projects currently underway in the French Armed Forces can be broken down by level:

- → **central** (core, in mainland France), consisting of a private cloud and a public cloud, to host applications and "business" data of the French MoD
- → **local** or "edge", used as relays in mainland France or in theatres of operations, overseas or on French Navy ships. They will be developed with classic hardened Cloud technologies, adapted to the tactical environment (temperature, dust, shocks) and benefiting from sufficient but limited throughput
- → **combat** or "far edge", which requires specific technologies ("fog computing") and capabilities distributed in the weapon systems used in a context of intermittent connectivity.

In line with this concept, the French Army is developing a Land Combat Cloud. A true nervous system and collective memory, it will be able to share and merge information for the benefit of command posts and tactical units, enabling them to share a Common Operational Picture (COP) and to access all the operational data necessary for their mission. The aim is to multiply tactical effects by improving collaborative combat and to improve command agility through planning and decision support. In addition, this technology will be used to provide support to command and operations through "reachback" functions, those requiring, in particular, high-level technical expertise. Finally, Cloud technology will also make it possible to improve the maintenance of equipment (predictive MRO) and, further upstream, the definition of the Army's future capabilities through the ability to analyse large volumes of data.

Ensuring the security of the Cloud is essential for forces' digital security. In the design and implementation phases, a systemic approach[1] and continuous integration of security aspects in projects and programmes is necessary. Efforts must continue to consolidate governance structures, generalise risk analysis and coordinate with relevant authorities to ensure that regulatory compliance takes into account the realities of land-based operations.

From a technical point of view, Cloud security is based on the security of the data, hosted applications and the network. Studies show that data breaches are often related to human configuration errors or targeted attacks.

1. Combined approach according to 3 axes, the static aspect which highlights the structure of the system, its composition, its elements and their structural relations, the dynamic aspect which highlights the evolution of the system in the course of time, and the functional aspect highlights the treatments carried out, the calculations of the system.

The latter is possible when an administrator is given excessive rights to access confidential information or critical data, or when stolen credentials allow attackers to access critical areas of cloud services to steal information.

Poorly managed identities and access can allow an unauthorised user to access internal data and threaten data integrity. A cyber-attacker could also manage to impersonate legitimate users, to read, modify or intercept transactions and send back falsified information or/and redirect users to illegal sites.

A DDOS[2] attack on services can prevent users from accessing their data. A malware infection can cripple or destroy cloud infrastructure, forcing a service to overconsume resources such as processing power or memory. These attacks can also slow dow the use of systems by legitimate users because of bandwith saturation, or even make the system inaccessible.

Finally, an accidental removal of service by the provider, due to a natural disaster or fire, can lead to a permanent loss of data.

The technical architecture of the Cloud is based on virtualisation, micro services and application programming interfaces (APIs)[3]. These APIs are the preferred method for building modern applications, especially for mobile devices and the Internet of Things (IoT), and can be a vector for malicious code if their integrity is not checked.

Finally, a breach of network availability is a significant and likely risk. It can be caused by an attack aimed at saturating bandwidth, jamming communications, or by a hardware failure or poor quality of service management. It is worth noting that "5G", designed in particular for connected objects, defined by software and using common language and Internet protocols, presents an additional risk of attack than previous generations of networks.

Clearly, this list is not exhaustive, and these risks must be adapted to the environment in which the Cloud is used.

To meet these security needs, a "data centric[4]" approach is recommended. It aims to make data more reliable to improve its processing via Cloud services, automate security services in order to reduce staffing requirements and reduce the response time. These actions also aim to facilitate the correlation and aggregation of all data streams to support defence in depth and to generate easily understandable and actionable information for administrators and security operators. In addition, the implementation of a "zero trust" architecture is often advocated. This concept requires secure and authenticated access to all resources, based on the principle of least privilege. It also includes continuous, real-time monitoring of the organisation's information systems, including all connected devices, and regular auditing of stored data.

For Armed Forces, a large part of the security of their cloud must be taken into account in the upstream phases of programmes or projects. Studies and risk analysis to define assets (data, processes, equipment, personnel, etc.) to be protected, detect intrinsic vulnerabilities and general threats, determine the environment of service providers, suppliers and partners, and define potential attack paths will make it possible to remedy the most critical risks. Furthermore, despite a broad attack surface due to the large number of stakeholders in the information system, the occurrence of a common attack is limited due to its low direct exposure to the Internet.

The risk may lie in a complex attack on the support or back-up functions connected to their suppliers and service providers, for which an analysis of cyber maturity is not always possible. It may also be the result of an attack on infrastructure or networks, making Cloud resources unavailable. Other attacks may be carried out by state-sponsored APT[5] groups with the ability to find zero-day vulnerabilities[6] and infiltrate and compromise the most secured systems. The danger also lies in their ability to adapt to security measures, and to move unobtrusively through data centre networks to achieve their objectives.

2. DDOS: A Denial of Service attack is a computer attack aimed at making a service unavailable, preventing legitimate users of a service from using it. At present, the vast majority of these attacks are carried out from several sources, and are referred to as Distributed Denial of Service attacks (DDoS attacks).
3. API: An API is an IT solution that allows applications to communicate with each other and exchange services or data.
4. Data centric approach: unified and integrated view of centrally modelled and managed data for the entire enterprise.
5. APT: Advanced Persistent Threat.
6. Zero-day vulnerability: In the field of computer security, a zero-day vulnerability is a computer vulnerability that has not been published or has no known patch. The existence of such a vulnerability in a computer product implies that no protection exists, either palliative or definitive.

In the context of a coalition operation, partners' cyber maturity must be assessed. For interoperability purposes, their access to the cloud(s) which centralise data must be studied, taking into account security requirements and longer-term sovereignty imperatives.

Cloud security requires a high level of expertise from external and internal cloud operators. They must be able to master areas such as identity and access management, connected object security, data security, or the implementation of resilience plans. Otherwise, the risk of losing control of the information system is high, making it difficult to gain informational superiority on the battlefield.

For effective digital security in operations, the Cloud may imply a simplification of technical architectures, to facilitate their protection. It does not mean however to fundamentally modify the approach to be adopted. The technical security mechanisms of the platforms must be complemented by appropriate operational security structures. They must be able to monitor the evolution of threats and take measures to correct residual vulnerabilities, protect the forces deployed, anticipate and detect attacks, and react if necessary. Similarly, cyber risk awareness among users of these modern combat systems must be increased. The basic security measures of the soldier using the weapon systems must remain easy to implement. Finally, resilience to cyber attacks must be developed through training in cyber crisis management and in the continuation of operations in a degraded service mode, pending their restoration by the competent units.

THE INTEGRATED BATTLEFIELD

PLANNING FOR BILLIONS OF THINGS

CONTRIBUTOR

Joe BAGULEY
Vice-president & Chief Technology Officer EMEA
VMWARE

"Be prepared" is the motto of every Boy Scout, but it remains applicable in all walks of life long after childhood has passed. Nowhere more so than in the military where situations and circumstance can vary quickly and dramatically and because Armed Forces are in a never-ending race to remain one step ahead of adversaries. I am reminded of the "P's" I was taught as a young officer – "Prior Preparation & Planning Prevents Poor Performance."

Armed Forces need to embrace what is at the bleeding edge now to adequately prepare for years in the future when today's emerging innovations, processes and technologies will be mainstream. Nowhere is this more aptly demonstrated than with the Internet of Things (IoT).

Speed of change

This particular area of technology is a real example of the speed of change and how militaries can act and mobilise or get left behind. The reason IoT is such a pertinent concept, is that the underlying technology is not new. In 2016, the U.S. Army lab (ARL) created the Internet of Battlefield Things (IoBT) project. This was in response to the U.S. Army's operational outline for 2020 to 2040, titled "Winning during a Complex World", which focused on keeping up with technological advances of potential adversaries. There are similar examples in nations around the world.

We're now seeing the theory brought to life. Israel's Ministry of Defence recently announced that it will begin trials of an unmanned robotic combat vehicle – dubbed the Medium Robotic Combat Vehicle (M-RCV) – in 2023.

Clearly, the concept of connectivity is already well established. But the reason it must remain the focus for Armed Forces is the speed of change and scale which it can potentially reach - the global Military IoT market size is projected to reach USD 16080 million by 2026, from USD 10620 million in 2019 according to Industry research.

A globally connected battlefield

If you feel that IoT and connectivity has permeated into a military setting, you simply, ain't seen nothing yet. The number of IoT devices in use is growing rapidly and will continue to rise. Cyber-physical systems - larger, algorithm-controlled embedded systems, such as autonomous vehicles and digital twins - are proliferating and we're entering into an era of total connectivity.

This won't simply involve singular tools or equipment, but every element of combat. Rifles will be connected to the individuals brandishing them, who will be connected to weapons depots and overall health monitoring stations and so on. It will move the dial from managing hundreds or thousands of endpoints to potentially billions in a globally interconnected battlefield.

If there is any doubt that this future is coming quickly, you need only turn your attention to what is happening in Ukraine. It has been a war fought on communications and networks, demonstrated by the effectiveness of Starlink, a satellite communication system owned by Musk's SpaceX. This has become an information lifeline, keeping battered hospitals connected and serving as a link to drones targeting artillery strikes against Russian forces. Ukraine's aerial reconnaissance force has used Starlink to connect directly to drones that have knocked out numerous Russian tanks, mobile command centers, and other military vehicles.

Unleashing tomorrow's innovative applications

Today's Internet is optimised for server-to-server communication between data centers or Clouds, which are usually located in remote areas where land and power were most inexpensive and easy to acquire. The problem with this architecture is that it doesn't effectively support the edge, where users and things are. For the Armed Forces, applications need to be able to intelligently place app instances and data in the right places to optimise performance, experience, and cost.

Unfortunately, today's networks just can't do some of the things we need to do to unleash tomorrow's most innovative applications. The boundaries between networks, Cloud providers, manufacturers, telecoms and storage are relatively clear now, but that's all going to change as connectivity becomes ubiquitous – the overlap will become larger, and you will not be able to tell the difference between a network, Cloud or IT provider. Military leaders must start planning for this now so that, as more and more elements become connected, they do not encounter restrictions in terms of what can be done or how systems are architected. This is where embracing 6G now is critical.

A future realised with 6G

Some experts believe 6G networks could one day allow us to hit max speeds of one terabit per second (Tbps) on an Internet device. That's a thousand times faster than 1 Gbps, the fastest speed available on most home Internet networks today. In a military context, it will be the foundation for applications including edge devices, autonomous vehicles, holographic communication and the connected soldier.

Realising these visions is what will happen when connectivity becomes as common, plentiful and unobtrusive as the air we breathe. It is why VMware is a founding partner of the Open Grid Alliance (OGA). This is a collection of the industry's best and brightest to advance a manifesto and a set of guiding principles for the formation of an Open Grid that stretches across the globe to support multi-Cloud services via fungible resources employed when and where they are needed, on demand. It combines many technologies and vendors working together in a neutral framework where all participants can benefit from their contributions, while individual stakeholders can innovate in unique and differentiated ways. It's looking at a more democratised, decentralised view of future architectures.

The "I's" in team

Regardless of these exciting developments, there is no magic formula for militaries. The world is changing so quickly that even the most ardent technologist can only speculate as to what future interoperability standards will be. This is both the opportunity and the challenge - making sure everything is going to work with everything.

For a sector that is predicated on teamwork, the future of the Armed Forces is faced with many "I's": Interoperability, interconnectivity and instantly available information. But to win tomorrow requires preparing now. If the Armed Forces do not start planning for building architectures capable of managing billions of things, they will fail in the future.

VAUBAN
SESSIONS

#6 TAKING TO THE CLOUD: CHALLENGES TO MILITARY USES OF CLOUD COMPUTING

MARCH 2023

avisa partners

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

FOREWORD

The digital transformation of the Armed Forces is an essential challenge for their adaptation to the ever-evolving and changing geostrategic environment, risks and threats, as well as the forms of use of the forces. The "Vauban Papers" published to date have made it possible to establish the founding principles of this operational digital transformation and its underlying issues. From these reflections, it is clear that this evolution will mark an important step in the modernisation of the Armed Forces who manage to conduct it with vision and pragmatism by making the most of the exceptional potential of the digital world and technologies. Those who also master its limitations and risks to define robust and resilient concepts of employment.

At the heart of this transformation is data, the true DNA of this new space. The interests, advantages and limitations of exploiting the vast flows of data that irrigate the operational chains from the strategic level to the soldiers have been examined in the previous "Vauban Papers". From these reflections, it became clear that the potential of cloud computing technologies[1] lends itself perfectly to the needs for access to these precious databases expressed by military commanders and executors alike, in their various operational domains, thus creating "Combat clouds". In order to create these "dynamic memories", many options are available to decision-makers who must be able to assess their relevance, resilience, dependence on third-party suppliers, security, access conditions, including in a highly degraded environment, and confidentiality. This last point is of particular interest because it requires a review of the rigid classifications that have hitherto governed operational information in order to adapt them to a dynamic management of confidentiality criteria.

This is one of the keys to the "Federated Mission Networking" concept advocated by NATO to develop new information systems that are agile, interoperable, reliable and secure. Virtualisation technologies lend themselves particularly well to this objective. They form the basis of the founding concept for the development of the new British Common Combat System (CCS). CSS establishes different levels of security that correspond to the level of confidentiality required by operations, whether they are purely national (Secret), open to work within NATO or coalitions of the willing (Mission Secret) or finally "Official" exchanges that can satisfy a lighter classification. It is thus possible, depending on the need and circumstances, to pass information dynamically from one level to another by defining access rights. This methodological analysis is a prerequisite for establishing an efficient, resilient and secure "Combat Cloud". It also enables the most suitable structure to be chosen according to the missions and the environment and to define the terms of collaboration with trusted third parties in order to make the most of the new information technologies.

In conclusion, the development of the various solutions that can make the most of the data flows in modern operations cannot be the result of purely technical choices. It requires, above all, an in-depth reflection on the organisation of the command, the delegations granted at the execution level, the operation in degraded mode and, as shown above, a new and more dynamic definition of the confidentiality criteria attached to these data, which, without altering the needs of sovereignty, authorises exchanges within NATO or any other coalition of circumstances. The success of this undertaking and thus of the operational digital transformation depends on the collaboration of all public and private actors in a "win/win" partnership, to experiment with the potential of new information technologies for the benefit of the military.

General (rtd.)
Jean-Paul PALOMÉROS
Former Supreme Allied Commander
NATO Transformation (SACT)
and Senior Advisor at Avisa Partners

1. Cf. Vauban Paper n°5.

TAKING TO THE CLOUD: CHALLENGES TO MILITARY USES OF CLOUD COMPUTING

CONTRIBUTORS

Axel DYÈVRE
Partner
AVISA PARTNERS

Martin DE MAUPEOU
Director
AVISA PARTNERS

Marin MESSY
Analyst
AVISA PARTNERS

Armed Forces have over the last decade worked on the doctrine and capabilities for collaborative combat across domains (land, air, sea). Collaborative combat relies on the use of systems, terminals and connected devices constantly exchanging data from the field towards the C2 and vice versa. It relies, as a result, on the ability of units involved to reliably access the network and with sufficient speed.

Measuring and integrating the connectivity challenge

Cloud technologies can provide an effective solution to the challenges of storing and processing the volumes of data generated by the digital transformation of Armed Forces. They also make it possible to increase the power of terminals (cloud computing) and the online use of applications (Software as a Service - SaaS). Whatever the uses of the Cloud, they imply certain constraints. The main one - logical for remote uses - is to ensure a sufficiently fast, responsive (latency) and secure connection between the servers where the data or applications are stored and the users and resources deployed on the ground (vehicles, drones, computers, effectors, vectors, etc.). This need for connectivity, which does not pose any particular problems in the majority of civilian and commercial applications, is a major constraint for use by Armed Forces in operations. These cannot always rely on a quality cable network, and rely on radio or satellite for data transmission as well as for vocal communications. In addition, the environment in which they operate and the conditions of unit deployments in theatres of operation strongly influence the availability of a connection with sufficient speed and latency. Maintaining a constant connection cannot be guaranteed in all circumstances due to the physical constraints imposed by the environment, the mobility of units or adversary action:

- **Geophysical constraints** such as topography, but also simply the rotundity of the Earth, can hinder the propagation of waves and therefore the information they carry, whether voice or data. In 2013, during Operation Serval in Mali, the units involved were at times stretched over an area of operation of more than 700 km and radio links sometimes proved difficult. The natural environment is another form of constraint, as waves do not propagate in the same way in the air as in water. A underwater vessel must be closer to the surface to transmit and receive data, thus risking its main asset, its stealth. The weather is another factor - by nature unpredictable in the long term - which affects wave propagation.

- **Encryption of data contributes to increasing the volume to be transported:** encrypted data weighs its own weight plus that of the encryption. If the network is encrypted, its throughput is reduced for the same reasons: it "carries" its encryption at all times. The necessary security of transmissions is therefore a factor which impacts connectivity. If the network is available, it limits the speed at which data is transmitted ("narrowing the pipe") and increases the volume (encrypted data, therefore heavier) to be transmitted.

- **Digital technologies are energy-consuming by nature:** processors, storage and networks all require electricity. Present everywhere from the overpowered server to the soldier's connected device, components constantly increase the need for energy. Because a connected device without energy cannot function, the need for connectivity also requires energy production, storage and even recharging throughout the chain, whether for servers or forces in the field.

- Finally, the connectivity chain necessary for the proper functioning of a cloud system is a complex set of resources. It is exposed to technical failures and malfunctions, as well as to human error. Permanent monitoring, an alert system and means of analysing the operation are therefore necessary.

Prioritising data and information needs

These issues of connectivity, availability and security of networks and data are very familiar to the military. They are amplified and made more complex by the intrinsically connected nature of cloud computing. This makes it necessary to think about, right from the design of a military cloud, the conditions for deployment and use of these technologies "in degraded mode", i.e. situation of reduced available bandwidth or even total loss of connection, whether as a result of technical constraints or enemy action. The US Army's Asymmetric Warfare Group (AWG) assessed that units' increasing dependence on technology increases their exposure to threats and requires the ability to operate in a simplified technological environment. For cloud computing, reflections on uses in degraded mode require both technical answers such as the use of Edge computing and the definition of doctrines of use. Combined, these will make it possible to optimise the use of data, the resilience of the connected systems and ultimately the control of information.

In a constrained environment, the main consequence of a reduction in available bandwidth will be to limit the flow of data which can be transmitted in a given time. In other words, the more data one seeks to transmit, the longer it will take. It is thus essential to prioritise data according to its use, by asking questions such as: What data is needed for the mission? What information is required for the next level? Which software needs to be deployed at which level? In the case of an armoured fighting vehicle which is constantly transmitting information to its tactical HQ, some information is more critical than others. It is conceivable that in the case of limited throughput, there will be a tendency to transmit tactical data on the location of friendly and enemy forces and to wait before transmitting data on the technical status of a vehicle or other less urgent information. In more critical cases, it is conceivable that some vehicle functions requiring connection even cease to operate, requiring thorough advance planning to ensure the best possible resilience in a highly degraded mode. Ensuring the availability data types according to their level of criticality for each connected system will make it possible to prioritise their transmission.

This will simplify and reduce data flows while avoiding the heavy deployment of infrastructure, CIS resources, connections, etc.

The almost certain prospect of a network disconnection - whether accidental or intentional - therefore requires preparation for the consequences of a total cut-off of upstream or downstream data flows for an indefinite period. To ensure the operational continuity of combat units and platforms, it is essential to decide ahead of time which capabilities and tools that must remain operational locally at all costs, i.e. independently of their network access.

Deploying suitable data storage solutions and relevant military doctrines

Questions around the impact of reduced or lost bandwidth implies thinking about a scenario to restore communications. Especially since it may be necessary for a unit to cut off then restore its data transmissions depending on the situation, for example to reduce the risk of detection by the enemy. Slowing down or stopping the flow of data does not necessarily mean slowing down the capture of information, which entails a probable risk of conflict between different versions of the same data when links are re- established. For example, the progress of an enemy armoured convoy is monitored by several sensors which transmit information on its composition and position to a C2. If one of the sensors loses the connection for a few minutes and suddenly starts transmitting data that has become "old", the problem of "reconciling" this data arises and therefore of how the system will arbitrate to keep only the most up-to-date data. This is all the more true as one can reasonably imagine that several units could disconnect and reconnect simultaneously. In order to prevent this risk, it is therefore necessary to design technical solutions and protocols which allow for data reconciliation. This problem has also been encountered - for different reasons - by many civilian sectors over the years, especially in the field of mobile applications, but solutions have been developed to allow the synchronisation of information when a terminal regains connectivity. As is often the case in the digital domain, developments from the civilian sector can therefore feed into developments for the military and their specific needs.

Optimised transmissions and connectivity in a constrained war environment may also make it necessary to have "tactical data warehouses" with highly decentralised processing capabilities. These warehouses may be the sensor itself, which concentrates the functions of collection, storage, processing and transmission. One relevant avenue to explore is Edge computing, a method which consists in processing data at the edge of the network, i.e. as close as possible to the data source. By doing so, the necessary computing power is distributed and the focus is only on the transmission of processed data, the initial volume of which is therefore in principle reduced. In addition, this method of distributing the computing load between the different units increases the resilience of the system: the impact of the loss, or temporary incapacity, of part of the network or resources is thus reduced. Here again, the challenge is to arbitrate between the computing power and storage capacities to be embedded (Edge) in the units or platforms and the number (and nature) of operations to be processed by remote capacities (Cloud) at higher levels. It therefore comes down to deciding which capacities must absolutely remain available to the units in the field in degraded mode. This is the case, for example, for mapping and location tools.

These different scenarios underline the need to define and implement operational standards to adapt cloud computing technologies for use in a military context. This means that from the design of combat systems and tactics, it is necessary to take into account these scenarios and to ensure that the use of networks is not essential to manœuvre and combat: units must be able to maintain their operational capacity in the event of loss of connection. The operational benefits of cloud computing for armed forces no longer need proving. Collaborative combat however requires further thinking about modes of deployment and uses of this technology, taking into account technical risks and operational constraints, and placing the issue of connectivity (or, more precisely, the loss thereof) at the heart of the reflection. This work will make it possible to prioritise, rationalise and organise data processing and information transmission capacities between all those involved in theatres of operation.

Because the adoption of cloud computing cannot be the result of technical choices only, it is also necessary to consider the implications of cloud computing in terms of sovereignty in the context of coalition engagements. Indeed, in the military domain, sovereignty is paramount, but interoperability is also essential. Within a NATO framework in particular, ensuring interoperability between Allies is therefore a central issue, especially in view of the multiplication and even systematisation of operations conducted in coalition. Once the will to share data has been secured at the political level, the definition and design of a cloud infrastructure must ensure the difficult balance between confidentiality and flexibility to create the conditions for instantaneous sharing by defining the confidentiality criteria attached to the data, the appropriate authorisation levels and the technical gateways.

TAKING TO THE CLOUD: CHALLENGES TO MILITARY USES OF CLOUD COMPUTING

CONTRIBUTOR

Brigadier General (rtd.) Olivier KEMPF
Director of La Vigie strategic consultancy
Associate researcher at the Federation for Strategic Research
Author of Guerre d'Ukraine (Economica, 2022)

The Cloud is fashionable, and seen by many as inescapable: the question is not whether to move to the Cloud, but when. What is valid for civilian organisations however presents some difficulties for the military: whether for routine activities on one's own territory, where network security constraints exist but are not insurmountable, or in operations where the challenges are of another scale.

Reasons behind the development of Cloud computing in the private sector

Cloud computing refers to the delivery of resources and services on demand over the Internet. In other words, where applications and data used to be stored on the user's terminal or server (on a hard drive), they are now stored remotely, on a cloud using server farms. The expansion of the Cloud therefore depends on improved access to the Internet, both in quantity and quality. The increase in bandwidth, but also its geographical spread, has facilitated this transition. The Cloud also benefits from both the considerable increase in server power (the operating frequency of servers increased by a factor of 10 between 1998 and 2008, with processors having between four and ten cores) and the fall in storage costs (for the price of a 1.2 GB hard disk in 2000, in 2013 we have a 1,000 GB disk).

This development has favoured two major elements: mobility and permanence. The development of Cloud computing allows companies of all sizes to purchase computing resources as a service. In other words, rather than buying networks, servers, appropriate software, storage capacity and the corresponding electricity on site, the company rents them. What it used to own locally, it now rents from a remote player.

This has several advantages: one, this variable rental allows for economies of scale, since large infrastructure is shared by all "tenants". Instead of having several cooling installations, for example, only one is necessary for a server or data farm. Two, this allows for better skills management: instead of an IT manager who must know about networks, servers, storage and keep up with the technology, this function is decentralised to a Cloud specialist. Last but not least, renting services on the Cloud allow for a much more refined management of resources, since only what is really needed is consumed, according to the company's production needs. The company is therefore no longer constrained either by unused excess capacity or by capacity that is too low to support growth. The IT manager transfers responsibility for service continuity to the subcontractor.

In other words, cloud computing allows for self-service on demand, elasticity and pay-per-use.

There are several disadvantages. Local storage allows quick and easy access due to the proximity of the storage. There is no need to fear service interruption due to network unavailability. And many consider local storage to be more secure than remote storage. In other words, data availability and security are the two major objections to cloud computing.

The advent of Cloud computing: a paradigm shift

Previously, the individual computer (whether of a private user or a company employee) was at the centre of the network. Today, this computer is part of a network, of the Cloud, which itself has become the heart of the system. The network is now a system, not just an interconnection.

This leads to a kind of paradox: the network is central, even if it is decentralised. The peripheral component is local, it allows autonomous action, but on condition that it has access to the network. Basically, every computer becomes a connected object: it only provides all its benefits if it is connected to the Internet (or to the network) or within the framework of certain very precise configurations (for example, private networks). In the world of cloud computing, we speak of public, hybrid or private clouds, depending on user's access to the Cloud.

TAKING TO THE CLOUD: CHALLENGES TO MILITARY USES OF CLOUD COMPUTING

While the French armed forces have organised a certain number of their internal information systems in Cloud configurations, these are obviously very "private" *("Cloud défense" implemented by the DIRISI - Direction interarmées des réseaux d'infrastructure et des systèmes d'information).* But this is about the management of organic activities, taking place on national territory for everyday service. The real challenge of cloud computing concerns operations.

Soldiers and weapon systems are increasingly interconnected, a trend which will continue (e.g. Armed Forces Information System programme - SIA, or the Scorpion programme of the French Army and the associated SICS). These operational information and communication systems (SIOC) will face the same constraints as large civilian organisations: increasing volumes of information, networking of staff, equipment and infrastructure, mobility and reactivity of armed forces. This is what collaborative combat is all about. Storing and exchanging huge masses of data raises technical challenges which cloud computing can answer, at least in part.

The idea is to deploy military units, each of which would be automatically linked to the whole and able to transmit and receive tactical data. A tank would automatically report its fuel use for instance, while the tank commander would automatically receive the order from his direct commander, which would be displayed directly on his map screen. This would be the case between peers or between one level and the one immediately above, but information should also be able to go up the chain of command, aggregated and simplified where necessary, across the whole hierarchical chain. The position of the tank should thus indicate that of the platoon, squadron, regiment, brigade, division, etc. Information about the enemy follows the same circuit, with the added challenge of relevance: what is of interest to a tank commander (eg enemy armoured vehicle within firing range in a specific direction) is not relevant to the colonel commanding the regiment, who wonders instead if said armoured vehicle is isolated, or is at the enemy's vanguard. It is not enough to transmit enormous volumes of data, it must be processed to give each person the information (i.e. qualified data) of interest.

Technically, Cloud technology makes this possible, since it aims to take advantage of the effects of computing scale to carry out analytics using Big Data and artificial intelligence.

Obstacles and challenges

Unfortunately, this model also faces technical obstacles: first, that of data transmission, which requires robust and constant bandwidth; second, that of computing power, with computers requiring both storage space and sufficient computing power to process data. This is in addition to challenges of confidentiality, synchronisation, traceability and integrity, not to mention energy sources, a key element in operation.

Building a private cloud in a foreign operation, for example in the middle of the desert, thus entails serious challenges, especially if control is to be maintained, a French reflex. Are several cloud layers necessary? Should both a local data farm and one back home be deployed? Should asynchronous systems be organised, allowing for operation in the absence of a connection? These are all questions which remain open.

The war in Ukraine raises other questions. The Ukrainian military is demonstrating that it is possible to wage war without using proprietary information systems with defence classification and dedicated encryption. The use of civilian means is widespread, such as the Starlink satellite system or the development of applications for drone to observe and guide their own firepower. The Ukrainian army thus uses a mix of private clouds while concentrating its own resources on dedicated but simplified uses. This hybridisation of military and civilian assets (with associated uses and procedures) could challenge our conception of military cloud computing.

Collaborative combat was intended for small numbers. The return of high intensity in Europe, with its need for mass and volume, could challenge this expeditionary model. A combat cloud designed for usual operations of the French army for example (maximum 5,000 troops) risks being unsuited to future conflicts, if mass becomes the norm.

There are this significant constraints associated with the combat cloud. They may not be unsurmountable, but will require complex technical considerations for commanders to factor into their decisions.

DATA AND APPLICATIONS IN THE FIELD

CONTRIBUTOR

Joe BAGULEY
Vice-president & Chief Technology Officer EMEA
VMWARE

When people picture the armed forces they think of soldiers, guns, machinery and vehicles. And while these features will always be a staple element of any campaign, there are some equally critical components that can't be captured in pictures. Namely, communication, information and agility.

Indeed, in an era of widely dispersed forces, hybrid fighting and the increasing regularity of both attack and defense in the cyber realm, the ability to deploy innovation and applications in the field on a real time basis has become the defining feature of success.

Separating the best from the rest

Yet it is for precisely this reason that achieving it is such a challenge - if it was easy, everybody would be doing it. This is because forces in the field have to adapt to ever evolving situations, with new innovations and in constantly changing landscapes. At the same time, they're battling adversaries who tend to be smaller and more nimble outfits that have access to the same tools and technologies.

It is not unfair to compare defense teams to long established corporations or public sector organizations that have a long history of legacy systems. These types of business have been using solutions and processes that have passed through rounds of procurement or are in long-standing agreements that may no longer be suitable but are difficult to reverse out of. The cycle of change is such that innovation moves quicker than they do.

In such cases there are layers of complexity and communications silos that restrict the flow of information and innovation to precisely where it is required and in real time. The military is no different and today, how this challenge is being addressed, is what separates the best from the rest.

Information flow from back end to front line

We are seeing some examples of defense organizations that are deploying and developing applications, systems and processes that aid the flow of information from backend to the front line and from minor developments to Majors commanding troops. It is because these examples are so different and are actively achieving what many are not, that by proxy, they stand out considerably.

Kessel Run Division, which supports the U.S. Air Force operations by building a scalable software factory to architect, manufacture and operate Wing and Operational level Command and Control systems, amongst other things, is one such example. Another is the US Army Futures Command - a program of continuous transformation of army modernization to provide future warfighters with the concepts and capabilities for future warfare.

Of course, in the armed forces, we also have to deal with coalition groups where members need to work together - something business organizations do not. It's a scenario that adds an additional layer of complexity because it requires members to be able to integrate with each other, use each other's resources and share best practices. Something that isn't working well today.

Circle of Trust

The main reason this is failing is because defense forces have their own SaaS (System as a Service), which creates demarcation between one nation and another. This has historically made sense for sovereignty and security but in an interconnected world, it's a legacy environment that means members cannot have connected software. This is where trust becomes more than vital. It is essential to ensuring no compromise of information in the system.

The solution is a circle of trust. One that incorporates the defense cloud at HQ or in the home nation, the combat tactical cloud at the edge and all connections with all devices and terminals that gather information or process information in between. The obvious challenge is ensuring coalition members have the same level of security and understanding of information processing as well a degree of standardization of information and data so that they can be incorporated and relied upon.

This is perhaps the definition of something that is easy to say and difficult to do but, coalitions must work in a circle of trust otherwise failure is inevitable.

The evolving command post

There is the added challenge of moving different pieces of the organization in the field. Traditionally, a tactical command post will take about a week to deploy is full of cables and computing hardware - all giving off heat. In the military vernacular, this is what is known as a sitting duck for the enemy. Though here too we're seeing innovations like Project Lelantos. This is a software defined data center (or software defined command post). It can be deployed and moved in days, which dramatically reduces the level of vulnerability of the command post.

Fixing the architecture of information

Despite these, and many other innovations, the objective of having effective and real- time information flow from source to where is required remains unresolved. Data is still being lost and the system is wholly inefficient. And something has to change. Key nations must get together to fix the architecture of information. This is where a multi-cloud strategy makes a lot of sense. It provides agility because its a way to implement interoperability, without relying on a single technology provider - something that will never be the case.

This is where the defense organizations need to reflect and they have to do that together and with a common goal. They need to define information standards and format, but also have a common understanding of classified and unclassified data. While understandable issues remain, it is also clear that the challenge we are facing at a communication and information level is not a technology issue but an organizational and a people one. And while solutions are abundant, none will be realized until armed forces can leverage technology and change the doctrine of the organization.

VAUBAN
SESSIONS

#7 HOW CLOUD COMPUTING SUPPORTS C2: BALANCING COLLABORATIVE TECHNOLOGY AND COMMAND PERFORMANCE?

APRIL 2023

avisa partners

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

FOREWORD

The art of command in its main principles has not fundamentally changed since Sun Tzu expressed it clearly in his "Art of War". Thus, anticipation, preparation and training, knowledge and intelligence, distribution of responsibilities and delegation of authority, and resilience, to name but a few of his commands, remain particularly relevant in crisis management, the conduct of modern operations, and especially in the context of the war in Ukraine. Today, in each of these fields, man holds more than ever an essential place, even if the rapid evolution of the technical means at his disposal, in particular in the digital domain, can give the illusion of a possible automation of the decision-making and even execution processes.

On the contrary, the digital transformation of the armed forces, in order to bring all its benefits, must intimately involve all the players in the operational chain, as the series of "Vauban Papers" published to date has emphasised. The Command and Control (C2) functions, which constitute the real nervous system of this chain, are at the heart of this operational digital transformation. They can now benefit from massive and continuous data flows that need to be managed, filtered, classified, exploited, exchanged and stored. Thanks to its potential for remote access and processing, cloud computing is a solution that has already been tried and tested in the civilian world and in companies, and some armies have already adopted it, adapting it to their needs. In this area, the sharing of experience and best practices constitutes both an axis of progress and interoperability. Indeed, the adoption of cloud computing within operational chains offers a remarkable potential for accelerating the decision/action loop by allowing access to relevant data at each level, from decision to execution, and by offering everyone a common vision of the operational situation. Cloud computing is therefore an integral part of the multi-domain collaborative battle. The implementation of the cloud in Command and Control structures must first of all lead to a comprehensive analysis of the pre-existing processes of exchange and storage of operational data. This must lead in particular to a new approach to the levels of confidentiality of these data, as mentioned in the "Vauban Paper 6: Taking to the Cloud: challenges to military uses of cloud computing" to ensure the best possible fluidity of exchanges throughout the chain of operations, whether purely national, inter-allied (NATO, EU) or within an ad hoc coalition. The adoption of the Cloud should in fact open the way to a new dynamic in the Command and Control of operations. This is not to question the need for a centralised level of command capable of implementing coherent and effective military strategies. On the contrary, the objective is to enable operational decision-makers to delegate the authority to engage to the most appropriate level in the chain, ensuring that the latter has the most relevant information to assume this responsibility. Thus, while accelerating the Observe-Orient-Decide-Act (OODA) decision loop, the combat cloud also aims to make all the data that contributes to its effectiveness reliable and organised in real time.

The control of operational data is more than ever a strategic, operational and tactical issue. The Cloud has an exceptional potential in this field, but it should not replace the experience and competence of the different actors of the operational chain. On the contrary, it should enable the art of command and execution to be enhanced in a very dynamic vision of modern operations, which is the whole point of this 7th "Vauban Paper".

Général (rtd.)
Jean-Paul PALOMÉROS
Former Supreme Allied Commander
NATO Transformation (SACT)
and Senior Advisor at Avisa Partners

HOW CLOUD COMPUTING SUPPORTS C2: BALANCING COLLABORATIVE TECHNOLOGY AND COMMAND PERFORMANCE?

CONTRIBUTORS

Axel DYÈVRE
Partner
AVISA PARTNERS

Martin DE MAUPEOU
Director
AVISA PARTNERS

Marin MESSY
Analyst
AVISA PARTNERS

NATO defines Command and Control (C2) as "the functions of commanders, staffs, and other Command and Control bodies in maintaining the combat readiness of their forces, preparing operations, and directing troops in the performance of their tasks". C2 designates the decision-making process, the ability to lead, and information and communication systems. It enables the planning, programming and conduct of operations from the strategic to the tactical level, taking into account developments in the theatre.

Developments in communications greatly influence on C2. The military's ongoing digitalisation generates a massive volume of operational and technical data. In this context, the performance of C2 depends on the permanent capacity to acquire, communicate, process and synthesise information at the relevant level. This capacity is itself based on the means to produce, receive, store and transmit information and orders faster than the adversary.

The operational benefits of a digitalised C2 - which can be summarised as a condensation of the decision-making loop or OODA (Observe-Orient-Decide-Act) - are widely recognised and identified, from increased intelligence capacities to decision support, giving the commander greater freedom of action and manœuvre.

A horizontal tool to serve the verticality of command

By offering increased means of storage, access and remote processing of data, cloud computing serves the performance of C2. In concrete terms, cloud computing translates into the command and control of operations through:

- An infrastructure which allows all units and staffs to access information remotely, thus limiting the volume of communication and information systems (CIS) in command posts and allowing, for example, mobility gains.
- The sharing of a common operational picture at all levels, based on improved information sharing. This common picture is no longer only centralised at the highest C2 level, but information can be shared across all echelons, which can increase autonomy and initiative at the lowest tactical levels.
- Data replication and synchronisation capabilities with an architecture comprising "mini-Clouds" in theatre interacting with a more central Cloud at the strategic level. This allows for greater resilience of the chain of command in the event of loss of contact with one of the echelons.

Cloud computing will therefore contribute to a strengthening and acceleration of decision-making by improving access to information (upward flow from the tactical to the strategic level) and the transmission and coordination of orders (downward flow from the strategic to the theatre level). In theatre, orders reach subordinate units more quickly and can even go directly to the weapon systems without human intermediaries (automatic fire control, missile guidance, etc.).

HOW CLOUD COMPUTING SUPPORTS C2: BALANCING COLLABORATIVE TECHNOLOGY AND COMMAND PERFORMANCE?

An increased risk of weakening the chain of command

By its very nature, cloud-based operation generates a great deal of information exchange between different levels of decision-making and results in a certain horizontality between C2 players, as expressed by the term "collaborative combat." These developments amplify certain challenges and constraints impacting the verticality of the chain of command, where each level must have the right and necessary information quality to guarantee its freedom of decision and action. For example, in the case of a tank squadron, a generalised access to the squadron's network "allows each of the tank commanders to understand his place in the system. It does not mean that the network is no longer directed and that the links of subordination between elements are not clearly established."[1]

For commanders, at the operative or even strategic level, access to a massive amount of information in real time can lead to micro-management, a term borrowed from the business world. The opportunity to follow the live evolution of a section or even a combat group, with great precision can lead to a "tunnel effect", locking in the decision- maker. This perception bias may be detrimental to the distance required to command large combat units. The hierarchical chain is broken by the upper level, which bypasses or crushes the intermediate echelons. Mirroring the concept of the "strategic corporal", i.e. how individual action of tactical significance can lead to a real strategic turnaround, this would lead to a "tactical general." Initial feedback from the war in Ukraine shows the operational consequences of reduced room for initiative at tactical level, due to an overly strict control by the higher echelons. The Russian army's highly vertical chain of command, which includes few non-commissioned officers, grants little autonomy to tactical units; the latter tends to be reduced to reaction only. In contrast, Ukrainian doctrine encourages tactical initiative, leading to unpredictability and much more reactive attitudes.

Facilitated by cloud computing, the potential abundance of information, sometimes accessible in real-time and remotely, can also interfere with the decision-making process by exposing the decision-maker to:

→ An **"information avalanche"** which can lead to an **information overload**[2] where the data feedback is too dense to be processed efficiently. This overload can be explained by technical faults on the one hand, when the computing capacity is not sufficient to exploit the mass of data that is fed back and stored; and by human limitations on the other hand, when operators are exposed to cognitive overload and unable to extract useful information from the mass of data available. In April 2012, this led Regional Command East in Afghanistan to ban video feeds from Predator UAVs to Joint Operations Command, as these distracted operators from their missions[3]. This "infobesity" can divert attention from information which is essential to the conduct of operations.

→ **The blocking of the chain of command by the permanent expectation of additional information**. The appropriate response to overabundance of data could be to voluntarily limit the flow of incoming data. Instead, individuals often seek to have increasing amounts of information to make better-informed choices. However, a decision can only be considered appropriate in a specific context and according to the time frame in which it is made. By constantly trying to reduce uncertainty, decision- making becomes paralysed. For military leaders, the risk is to reduce their capacity for initiative and to place themselves in a reactive position. Maintaining the capacity to decide in conditions of uncertainty is essential as information will always be incomplete and imperfect: enemy action or theatre conditions may lead to a loss of connection with certain units.

1. CES Martin Pinel, "*La subsidiarité au combat : de quoi s'agit-il ?*", Fondation Maréchal Leclerc, 18/12/2020, URL: https://www.fondation-marechal-leclerc.fr/wp-content/uploads/2017/08/CES-PINEL_Subsidiarite-au-combat.pdf
2. Caroline Sauvajol-Rialland, "*La surcharge d'emails, nouveau vecteur de la souffrance au travail*", Huffington Post, 31/08/2012, URL: https://www.huffingtonpost.fr/actualites/article/la-surcharge-d-emails-nouveau-vecteur-de-la-souffrance-au-travail_8843.html
3. Serge Caplain, "*Les 10 pièges de la numérisation des forces terrestres*", Linkedin, 15/01/2018 URL: https://www.linkedin.com/pulse/les-10-pièges-de-la-numérisation-des-forces-serge-caplain/?originalSubdomain=fr

HOW CLOUD COMPUTING SUPPORTS C2: BALANCING COLLABORATIVE TECHNOLOGY AND COMMAND PERFORMANCE?

In a context of increased dependence of the C2 on networks, these risks to the chain of command highlight the importance of:

- Strictly maintaining the principle of subsidiarity of command;
- Maintaining the responsiveness of decision-making, especially in a degraded environment where access to data may be limited or even cut off;
- Managing the growing influx of data at the various levels of the chain of command while avoiding paralysis of decision-making;
- Facilitating the processing of heterogeneous data from multiple sources;
- Making information more accessible at all levels through ergonomic tools and interfaces.

These requirements are met first and foremost by managing information feedback and orders via each link in the chain, adapted to instantaneous data flows for all the players connected to the network. This implies that there be a progressive upwards processing of information, but also an adjustment of the orders given downwards at each hierarchical level. Cloud computing can contribute to this organisation by enabling optimal distribution of data between "local storage" (up to the combatant level) and "network storage" (up to the strategic level). Its corollary for the distribution of computing capacity (Edge Computing) also allows data to be processed "locally" on platforms and terminals. Artificial intelligence, another technology closely linked to cloud computing, enables the automation of data processing and the extraction of useful information from the mass of data to guide - rather than automate or replace - decision-making.

Combined, these tools reduce the flow of data and therefore of information between the various levels of the chain of command. Once the data has been stored and processed at the relevant level, only useful information is transmitted onwards. In addition to reducing the volume of data flowing through the networks - and thus meeting the constraints of limited connectivity - they improve decision-making by on the one hand storing, and on the other transmitting

HOW CLOUD COMPUTING SUPPORTS C2: BALANCING COLLABORATIVE TECHNOLOGY AND COMMAND PERFORMANCE?

CONTRIBUTOR

Lieutenant General (rtd.) Hervé GOMART
Former Deputy Chief of Staff of the French Army

Evolution of command with the emergence of "collaborative" technologies

As Asma Mhalla[4], a specialist in political and geopolitical issues of Tech, points out, the year 2022 will have been marked by the entry of cyberspace into the public debate. Whether through cyberattacks, disinformation campaigns on social networks, or the destruction or takeover of network infrastructures, cyberspace offers states new tools for power, subversion and coercion.

The year 2022 will also have been marked by the Russian invasion of Ukraine and the war that has been going on there ever since. Against all odds, the Russian army failed to achieve its main strategic or operational objectives, as it came up against a well-prepared, well-organised and highly resistant Ukrainian army. One of the notable differences between the two armies at war was in C2 (Command and Control). Where the Russian army remained organised according to the Soviet model based on excessive centralisation of command, the Ukrainian army has been able to evolve since 2014 and the loss of Crimea and part of the Donbass by making an effort on a decentralised C2 relying on small, mobile and underground command posts.

As C2 is recognised as the main factor of superiority, it is therefore vital for armies to take a determined look at so-called collaborative digital technologies to evolve their command in terms of its organisation and implementation and thus remain capable of winning the war.

On the one hand, one of the challenges of cloud computing lies in the ability to acquire more and more information, to be able to analyse, store, exploit, transmit and monitor it. The army that is able to do this will retain its freedom of action in the digital and data fields. It will be able to gain the upper hand over its competitors or adversaries by being one step ahead and by anticipating thanks to more powerful and more efficient decision support tools.

On the other hand, technologies in the fields of space, satellite, imagery, robotics, etc., contribute directly to the transparency of the battlefield, which is a particularly important factor in today's conflicts. Even if it is not absolute, it must be taken into account in the different operational phases of the strategic campaign. The direct consequence of this transparency applies to C2, which can hardly remain established on an organisation based on plethoric, sedentary staffs weighed down by ever more cumbersome digital tools. Today, a chain of command must be based on an organisation offering reactivity and pragmatism. It is therefore necessary for each level (strategic, operational and tactical) to know how to operate on small, agile and mobile HQs or CPs. A modular organisation in distributed PCs is already a relevant response. Furthermore, the principle of subsidiarity is an imperative. It is more applicable with access to the cloud. Any command entity must be able to connect to it and find the common operational picture (COP). Such an organisation allows for autonomy of the CPs down to the lowest level, which should not be seen as a permanent command, but as an opportunity to be exploited according to the manœuvre and the situation of the moment.

4. Asma Mhalla teaches at Sciences-Po Paris and Ecole Polytechnique

However, although they represent a major technological development, cloud computing, with its various applications (storage, messaging, collaborative tools, etc.), should not be considered as a panacea in the field of information exchange. Indeed, although it can bring real added value in terms of speed in the collection of information, data processing cannot be fully exploited without the contribution of artificial intelligence. Given the ever-increasing massification of information, whether operational or technical, humans are already no longer able to see everything, analyse everything and exploit the right data at the right time. Information overload will only increase in the operation of cloud computing, developing real cognitive risks.

Yes, and this is a reality, the difficulties and even risks associated with the emergence of new collaborative technologies exist, but given the challenges of cognitive superiority, of accelerating the decision-making process through decision support tools capable of automated or predictive analysis, militaries have little choice but to pursue with determination their understanding of a constantly evolving C2 and to consolidate the resilience of the chain of command. Therefore, not only will the chain of command need to be protected from cyber threats and jamming of all kinds, but it will also need to work continuously to increase its stealth, reduce its electromagnetic signature and thermal footprint, while promoting an operational level organisation based on a system of replicating parts of the strategic cloud.

The digital transformation of our armies has been underway for many years. Collaborative technologies will become increasingly important, as will virtual reality and other immersive solutions. It is therefore vital that we continue to keep up with the advances in high-tech and continue to evolve our chains of command. The complexity of the battlefield or the fog of war will not disappear, but it can be more understandable. The country that does not make the necessary efforts and investments has already lost the war.

HOW CLOUD COMPUTING SUPPORTS C2: BALANCING COLLABORATIVE TECHNOLOGY AND COMMAND PERFORMANCE?

CONTRIBUTOR

Michael CROWLEY
EMEA Director Public Sector
VMWARE

Adopting agile to avert becoming fragile

Modern warfare is the embodiment of variety. It is conducted in the multi-domains of land, sea, air and cyber - often simultaneously. While it often involves several nations acting in a coalition with troops operating with various equipment, using multiple languages and conducting operations in all conceivable types of environments. The potential scenarios are almost limitless.

It means that the basis of success for all armed forces is agility. But given the size and scope of the work militaries are faced with, the difference between wanting to be agile and actually being so, is vast.

No singular road map to agile

The obvious question is, "what is required to enable forces to be more agile" ? For all the bullets fired in this sector, there is no silver one. It is precisely because of the variations involved that no singular road map to agile exists. Yet there is a common denominator that differentiates the forces that are agile and those that are not. That is infrastructure.

The best and most agile militaries have the necessary infrastructure to allow coordination across coalition members, regardless of mission objective or geography. It is the backbone that supports data propagation to all the different command levels and is the key to delivering the right information, at the right tempo to the right individual so that initiative can be taken in the field by the mission commanders.

Changing chain of command

The dispersal of forces in the field are evidence enough that a monolithic chain of command no longer works. The requirement to enable initiatives in the field at a commander-level has not just fractured the traditional chain but obliterated it entirely. This is the 21st Century, Western approach to warfare and something we're seeing today in the conflict in Ukraine.

The Ukrainians, supported by leaders of other European states, are adopting this approach. It is a key strategy in aiding the fluidity of their operations both in attack and defense and why we continually hear reports of mission successes, no matter how small. The reason this is brought into such sharp focus, is because the Russian forces continue to operate with a very rigid command structure, which does not allow for flexibility or the agility to respond or prepare in enough time. This piece[6] of detailed analysis on the subject makes for interesting reading.

Federation of clouds

The next question is, 'what is infrastructure'? What do we mean and what is involved? To be clear, we're talking about a federation of clouds. That is a collection of clouds coming together to create a multi-cloud architecture. This ensures the right data is hosted, stored and shared in the appropriate place, capitalizing on the unique benefits of public, private or edge, without an over-reliance on one particular option. Aside from that, it allows for interoperability between nations and coalition members.

5. Major General (rtd.) Mick Ryan "*A tale of three generals - how the Ukrainian military turned the tide*", Engelsberg Ideas, 14/10/2022, URL: https://engelsbergideas.com/essays/a-tale-of-two-generals-how-the-ukrainian-military-turned-the-tide/

This type of cloud architecture enables nations or forces to plug into the overall scheme or command infrastructure for information and data while offering the autonomy to scale activity up or down accordingly. This is where multi-cloud architecture is bringing value. It is cycle of processing information from the backend to the front in a federated mode and the basis for agility in the armed forces.

Multi-cloud in a coalition

Take, for instance, a coalition between Portugal, Spain and the UK. The UK would be the lead country with its own cloud architecture. But this same architecture would enable Portugal to plug-in with its own cloud and Spain to do likewise. This is a multi-cloud and it allows information to flow from the Portuguese or Spanish source into the UK control and command system as the lead country. This information can be processed at the back-end and delivered into actionable intelligence in the field almost in real-time. At the end of the operation, Portugal and Spain can disconnect with their security, intelligence and information intact.

Bringing multi-cloud to life

We only need to look back a few weeks to see an example of how this journey to multi- cloud is being brought to life. In December 2022, the U.S. The Defense Department (DOD) awarded the Joint Warfighting Cloud Capability[7] (JWCC) contract - the Department's enterprise-level acquisition vehicle - which allows the DOD to directly acquire commercial cloud offerings at all classification levels to serve missions from headquarters to the tactical edge.

The JWCC contract allows the DOD to have direct access to the four main cloud providers - AWS, Google, Microsoft and Oracle - of which VMware is the glue that binds them together. It means that warfighters will have the opportunity to, under one contract, acquire capabilities such as global accessibility; available and resilient services; centralized management and distributed control; ease of use; commercial parity; elastic computing, storage and network infrastructure; advanced data analytics; fortified security; and tactical edge devices.

Military leaders need not be afraid of integrating legacy systems or embracing multi- cloud architecture. The best and most agile forces are already doing this successfully. Without embracing this approach, there is no doubt that, in time, military operations will become fragile and unwittingly restrict progress. Or, even worse, put missions and lives at risk.

6. AUS Department of Defense "*Department of Defense Announces Joint Warfighting Cloud Capability Procurement*", 07/12/2022, URL: https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/

VAUBAN
SESSIONS

#8 CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

MAY 2023

avisa partners

VAUBAN-SESSIONS.ORG

vmware

COLLECTION

VAUBAN PAPERS

FOREWORD

If proof were needed, the war in Ukraine shows how much the training, initiative and creativity of combatants close to the action make up the strength that any modern army must capitalise upon. To make the most of this precious asset, it is necessary to conceive the collaboration of actors at all levels of command and execution within a dynamic, efficient and reliable information network. The previous Vauban Paper, "How cloud computing supports C2: Balancing collaborative technology and command performance?", highlights the added value and conditions of use of cloud computing within the operational chain. In short, it is a question of making the most of data flows from various sensors, organising them and thus enabling decision-makers to gain an informational advantage. In order to exploit and even amplify this advantage in the various combat areas, the use of cloud computing within a genuine tactical network is an attractive option. Thus, each combat unit could both permanently contribute to and benefit from an updated tactical situational assessment. Like certain specific current networks (use of UAVs, air support, tactical data links, etc.), information sharing within the tactical Cloud would make it possible to optimise the use of the means available at a given time and place and to maximise the effects produced. The dynamic management of data enabled by cloud computing is not limited to the use of resources, but can also improve the identification of forces involved, reduce the risk of friendly fire, and contribute to the medical support of combatants and operational logistics.

In order to move from theory to practice, to deploy and implement these tactical combat networks, numerous challenges must be met and experiments in demanding operational conditions must be conducted. The availability of efficient means of communication at any point in operation is obviously a prerequisite that can be solved at least partly by new information technologies, provided that they are protected against the most modern jamming techniques. This highlights the need for reasonable redundancy and the need to consider degraded modes in all operational plans and therefore in the training of forces. Connection to the combat Cloud should not become a sine qua non condition to participation in operations. The open question is: should the tactical combat Cloud become a means to accelerate and optimise multi-domain operations or should it become an end in itself?

Technology, however powerful, cannot be the sole driver of the operational digital transformation. Only close cooperation, driven by operational requirements, nurtured by realistic experimentation and failure, can confidently develop the combat Cloud at both the command & control and execution levels.

The digital fog should not replace, or worse, feed the fog of war.

Général (rtd.)
Jean-Paul PALOMÉROS
Former Supreme Allied Commander
NATO Transformation (SACT)
and Senior Advisor at Avisa Partners

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

CONTRIBUTORS

Axel DYÈVRE
Partner
AVISA PARTNERS

Martin DE MAUPEOU
Director
AVISA PARTNERS

Marin MESSY
Analyst
AVISA PARTNERS

"We have always practiced collaborative combat. The information transmission system is what's changed." Lieutenant-Colonel Ludovic, Second-in-Command of the French 1st Marine Infantry Regiment.

The private sector has recently seen a rapid adoption of centralised cloud services. This has proved to be economically and operationally attractive to many organisations. Cloud operation allows for a cost-variable IT infrastructure which can be flexibly scaled almost immediately to the needs of the organisation, whether in terms of storage space, processing capacity, or the number of users. In addition, cloud technologies have helped accelerate the networking of connected physical objects and the development of new services and uses for sharing and accessing increasing amounts of data and information.

To enable the networking of actors and resources in a theatre of operations, the "tactical Cloud" reflects the interest of the armed forces in applying this logic to military operations. While this is today still at the prototype and test stage, the main challenge is to enable forces to carry out their missions, even in "degraded mode", i.e. when communication with a centralised Cloud is not be possible, be it because of geography or enemy action. Unlike the private sector, which has developed and popularised cloud concepts and service offers, armed forces engaged in operations - i.e. requiring "tactical" resources - must be able to fulfil their missions at all times, whatever the state of the networks. At the crossroads between a centralised and decentralised logic, hybridising several resources, the tactical Cloud therefore aims to distribute data and its processing, and therefore computing power, between the different levels engaged (HQ, armoured vehicles, soldiers, etc.) to enable autonomous operations if necessary.

The requirements of a theatre of operations may at first sight seem difficult to reconcile with the use of resources operating in the Cloud. On the one hand, this is due to the outsourced and centralised nature of the Cloud and, on the other, to the challenge of its deployment in scenarios characterised by temporary and mobile infrastructure as well as in a constrained and degraded environment. For these reasons, and despite advances in connectivity, cloud computing is currently deployed within military forces primarily in an unconstrained, non-operational environment. The US Army has worked on the subject for over a decade, and only in 2022 announced the deployment of a first Cloud in a foreign theatre, with experiments thus far conducted on US territory[1].

Following this example and in view of the growing need for rapid access to large quantities of information, the question is no longer whether armed forces should consider setting up tactical Clouds hybridising localised and remote resources. It is above all a question of determining how they can be deployed given the specific operational constraints which will govern their implementation in a military context.

Stocking, transmitting and exploiting the mass of data "in real time"

With the digitalisation of the armed forces, the individual soldier, the combat platform and the weapon system are now all agents in the collection and transmission of data to the higher echelon. Equipped with sensors, they are integral parts of the network and provide access to environmental and instruction data. The ability to process and share this data, then to circulate stored and archived information, contributes to the enhancement of knowledge and experience and allows different actors access at any time and any place. While current tactical data links such as "Liaison 16" showing limits in terms of throughput, the tactical Cloud reflects the desire to enable platforms and combat units to access the massive volume of stored data and enhance it through the application of advanced algorithms.

1. Jaspreet Gill "*Army "well on its way" to first OCONUS Cloud in Indo-Pacific* ", Breaking Defense, 14/01/2022, URL: https://breakingdefense.com/2022/01/army-well-on-its-way-to-first-oconus-cloud-in-indo-pacific/

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

One of the most perceptible potential contributions of the Cloud at tactical level concerns real-time situation awareness. With the Cloud, the major difference is the accelerated transmission, promotion and sharing of geo-referenced data within a "tactical bubble". The position of each unit, whether friend or foe is automatically transmitted in real-time on a common operational map. The deployment of connected vehicles during French operation Barkhane thus confirmed the relevance of instantaneous and simultaneous transmission of orders to various units, for example for the transmission of bypass routes following the identification of IEDs.

Real-time situation sharing offers many operational advantages for manœuvres, such as:

- Better area coverage, allowing control of a wider perimeter.
- A reduced risk of friendly fire, by making targeting more precise and decisive.
- Better coordination of the various units, allowing to re-articulate the plan more easily.

Generally speaking, reinforced knowledge and sharing of situations make manœuvres, back-up and support more fluid. One can imagine, for example, maintenance units having direct access to the status of the various vehicles on the battlefield, and therefore optimising the distribution of stocks, minimising downtime. Theatre logistics would also be greatly simplified, with a constantly updated view of the level of ammunition, fuel and food, again optimising logistics flows.

Meeting the challenge of the connected battlefield

The use of the Cloud is simple on the national territory where it relies on a controlled technical infrastructure and environment. This is not the case in an operations theatre where the communication infrastructure may be non-existent, insufficient or unsecured. The challenge here is to guarantee on the one hand, the availability of the network and, on the other, sufficient bandwidth to transmit large volumes of data (taking into account that encryption increases data volumes).

Thus, the use of the Cloud in theatre requires a network which manages mobility and ensures the tactical communications necessary for the deployed forces using radio-based technologies. Military communication networks were initially built to carry voice, using a hierarchical structure. They were also designed to connect geographical entities which were not very mobile. These networks were then adapted to carry data, but without revising their overall architecture. The challenge remains to meet today's demand for connectivity and all types of data (images, video, instant messaging, etc.).

In addition to the capabilities offered by satellites to guarantee the confidentiality of communications and to cover isolated areas, a combination of other means can be envisaged to reduce latency (delay in transmitting data) and increase in amounts of data exchanged: the deployment of projectable tactical networks based on portable servers and relays, the reuse of existing communication infrastructures (in urban theatres) or the use of stationary high-altitude balloons.

For over twenty years, innovation in communications has largely originated in the civilian sector: mobile networks, and in particular cellular networks, have in just a few decades become a major component of the development of information technologies and data exchange. These advances, up to the recent arrival of 5G, are improving connectivity and reliability, increasing speed and reducing latency. Increasingly digitised military information and weapon systems are impacted by these developments, which armed forces can take advantage of by matching their specific needs with technological advances. For example, the architecture of communication networks, completely revised with the arrival of IP (Internet Protocol) networks, provides distributed, decentralised and virtualised architectures, making it possible to manage resilience, greater centralisation of applications, and to bring infrastructures closer to the users. The implementation of this all-IP architecture, by allowing the exchange of information between all points of the network, is one of the essential requirements of the connected battlefield.

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

Controlling the security of an interconnected environment

The interconnection of systems, the centralisation and transfer of data are all inherent to the operation of cloud computing, yet represent possible security flaws which require controlled and shared measures and doctrines of use. Requiring more open systems, the Cloud mechanically creates windows of vulnerability and increases the attack surface. Furthermore, the virtualisation of resources and the transfer of part of the computing capacity to connected terminals (edge computing) increase the size of the software considerably, which also contributes to the increase of the attack surface and makes it necessary to integrate cybersecurity as a structuring dimension right from the design of systems.

At the tactical level, communications are further exposed to an extremely constrained magnetic environment due to the threat of jamming or decoying. Equipment and platforms risk coming under increasing attack as a result of this «hyperconnectivity.» They must therefore be designed to withstand and delay the effects of attacks and use a highly secure network. The systematic use of data encryption is a first response. Beyond that, cybersecurity requires the design and implementation of security measures, from the design of military systems (technical specifications) to their use (doctrines and employment concepts), including their deployment and configuration. These cybersecurity requirements apply at different levels:

- **Physical securing** of servers and connected systems physically accessible by the enemy. This could lead to their physical neutralisation or destruction but also their capture, offering a potential entry point to compromise the network.
- **Software security**: embedded components within connected systems offer additional points of vulnerability.
- **Securing communications**: cloud computing involves openness while ensuring the security of data transit infrastructures and protocols; network monitoring is essential in this regard.
- **Application security**: data aggregation platforms and the applications used to exploit them can be the object of cyber-attacks that exploit their flaws.

Putting the "degraded mode" and the human factor at the heart of doctrinal reflection

As with the introduction of any new technology on the battlefield, the issue of doctrinal integration of this new technical environment in a real combat situation arises with cloud computing. As mentioned, the implementation of a cloud-based operating mode comes up against natural obstacles in theatres, such as limited bandwidth, energy supply issues, or even enemy action. Faced with an adversary using advanced electronic warfare capabilities, there is no guarantee that the advanced functions provided by the network will be freely available. As a result, the full range of information sharing capabilities can only be available sporadically and partially. This makes it necessary to consider the degraded mode in the employment concept of the tactical Cloud to ensure the operational continuity of the forces in case of temporary disconnection or loss of the network.

The second key element is that the human factor must be placed at the heart of doctrinal thinking in a context of constant evolving tools and means. While cloud computing can improve combat performance, the human factor remains the primary variable in combat, which by its very nature is an intense stress situation involving reduced cognitive availability. Under fire, soldiers can only process a limited amount of data and therefore tend to practice targeted information selection to avoid cognitive overload. While increasing the capacity to accumulate, exploit and share data, cloud operation - coupled with artificial intelligence - can and should help to obtain the best representations of information to be able - at the time of action - to establish the right priorities, eliminate irrelevant information and guide decision-making. Moreover, the increase in geographical dispersion - made possible by increasingly decentralised tools and technologies - can lead to increased isolation of combatants, and therefore a loss of the tactical link usually maintained by strong physical and psychological proximity. These cognitive and psychological dimensions, as well as the technical and security dimensions, must be taken into account when considering the use of the Cloud at the tactical level.

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

CONTRIBUTOR

Isidoros MONOGIOUDIS
Project Officer for Information Technologies
EUROPEAN DEFENCE AGENCY

A key function of cloud computing in the military is the support of improved situational awareness to enhance decision-making. At the tactical level, specific computing capabilities are needed where standard commercial Cloud solutions are not adapted. The term tactical Cloud was introduced to reflect the special requirements for cloud computing in military operations. Related concepts include:

- C4ISR Systems enabled by tactical Cloud infrastructure: this type of cloud computing reflects the capability to collect and process data closer to the battlefield in order to improve situational awareness at tactical levels and to enable a common real-time operational image available from the tactical (soldier) up to strategic level.
- Information management of heterogeneous sources: the nature of military networks and digital components means that information must be collected from different sources. This requires proper handling and management for efficient aggregation.
- Information process enhancement by using Artificial Intelligence (AI) and Big Data: the use of AI and Big Data tools focuses on the different ways in which available data sources may be processed.
- Support to decision-making by AI and Big Data: the use of AI and Big Data tools to use the outcome of previous processes to support decision-making process.

The use of a conventional Cloud can pose problems for military tactical edge purposes, which requires innovative solutions. A key problem is the unreliability caused by DIL (disconnected, intermittent, low-bandwidth) communications between tactical users and the Cloud, where multiple communication jumps increase the latency on said communications. Information provided by a tactical user can take a long time to become available for other tactical users. The latter evolves in a very dynamic environment and cannot afford to wait for replies to information or service requests (sometimes generated by other users in the tactical edge at a very short network distance).

The tactical Cloud is a combination of a central Cloud, computing capability on sensors and several possible levels of small Clouds located at diverse levels between the centralised Cloud and sensors. In this hierarchical network, the higher a fog node is, the larger its processing/storage capacity, since it is expected to support more devices in the tree downwards to the edge. On the other hand, fog nodes which are higher in the hierarchy are also expected to present longer network delays to the edge. Therefore, the hierarchical composition of micro data centres (or cloudlets) along with the Cloud provides a range of computing capacities at different geographical (and logical) distances to the IoT devices at the edge.

The computing hierarchy in the fog infrastructure can offer a wider range of service levels, supporting applications which cannot be supported by cloud computing alone. A fog infrastructure can handle applications with a variety of QoS requirements, as applications can run at a hierarchy level which provides adequate processing capacity and meets latency requirements. Another consequence of the use of processing closer to the edge is to reduce (aggregate) bandwidth use in the network along the path between edge and cloud.

The connectivity between several tiers in the fog/cloud hierarchy can be possible using several network technologies, including wired and wireless, with 5G potentially significantly improving network performance.

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

Outcomes of related studies have showed some key benefits from the implementation of the tactical Cloud:

→ **Edge users (combatants)**:

- Automatic threat recognition using real-time video processing at the edge.
- Early risk assessment and automatic alerts.
- Information augmented for the combatant, e.g. video is processed and enriched with information obtained through AI applications in near real-time.
- A combatant on the edge with a C2 or similar system to display tactical information will be able to easily view the enhanced Common Operational Picture (COP) with this information.

→ **Strategic/Operational users**:

- The operator will have access to the complete COP, adding information of interest to the analyst, directly from the fog nodes.
- He/she will receive automatic intelligence reports/alerts generated by the tactical platform. These reports can be shared with any intelligence network according to standard procedures.
- This COP is automatically built, in parallel, with the information available at a strategic level (OSINT, and tactical enabled information).

A key concept in tactical Cloud is the Internet of Things or Military Things (IoMT), i.e. is simply the application of IoT technologies and concepts to the military domain.
To date, the deployment of IoT technologies in the military has primarily focused on applications for C4ISR and fire-control systems. IoT technologies have also been adopted in some applications for logistics management and training and simulation.

The Internet of Military Things interconnects sensors, effectors and data. This data can be related to own forces, to opponents, to environmental conditions and to population attitudes, among others. Sensors and effectors can be attended or unattended, wired or wireless. Some devices in the IoT market are designed for harsh industrial environments and could thus be relatively well-suited for adoption in military environments.

Overall, the concept of IoMT is largely driven by the idea that future military battles will be dominated by artificial intelligence and cyber warfare and will likely take place in urban environments. By creating a miniature ecosystem of intelligent technology which can distill sensory information and autonomously manage multiple tasks at once, IoMT is conceptually designed to offload much of the physical and mental burden from fighters in a combat.

Informed decision-making requires comprehensive knowledge of the battlefield and an accurate picture of the current situation. The information a commander needs to make effective decisions has expanded exponentially, meaning that commanders often bring together volumes of diverse data to understand their battlespace.

The importance of data in modern warfare poses two distinct challenges for a commander: handling the sheer volume of data produced, and integrating numerous types of data into one coherent battlespace picture. Military data-fusion applications incorporate not only videos but still imagery, signals intelligence, human intelligence, ground sensors, battlefield reports, map data, and a host of other data sources.

IoT usage in operational communications is constrained by technical limitations in mobile communications networks' bandwidth and robustness. However, with 5G technology, speeds will be more than enough for a true IoT application that would require enhanced bandwidth and close-to-zero latency for accurate and timely data collection and process.

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

The European Defence Agency aims to define the technology requirements for cloud computing for the defence operations analysing the concepts of tactical Clouds, IoMTs, data collection and analysis from multiple sensors with AI, 5G implementation through an ongoing study started in 2019 and to be completed in 2023. Those concepts will be reflected in a pilot prototype platform/demonstrator, which will try to showcase the benefits of edge computing and the significant performance enhancement in the situation awareness process. Further implementation may be addressed under EDA's framework with ad-hoc projects tailored to the identified operational and technical requirements.

Disclaimer: *This paper is a short version of a presentation on the topic of "Tactical Cloud with IoMT capabilities" held in the framework of Cloud Intelligence for Decision Making Support and Analysis (CLAUDIA) project, implemented during 2022.*

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

CONTRIBUTOR

Joe BAGULEY
Vice-president & Chief Technology Officer EMEA
VMWARE

Turning to the edge to gain advantage in the field

In the modern battlefield, visibility is paramount and the ability to navigate through the fog of war is predicated on commanders at all levels, not just the generals, being able to see the big picture across the battlefield. This means everyone having the ability to know where forces are, what they are doing and how they are performing.

In an effort to make the best decision possible, military commanders are turning to the edge as they strive to gain advantage in the field.

Pushing innovation to the front line

Edge and combat Cloud - a collection of private Clouds connecting various elements of the battlefield - are pushing innovation and digitalisation to the front line, both literally and figuratively. A good example of which would be the Firefly system[2], which supports NATO forces. The combination of these technologies is making a real difference in how operations are conducted. They enable the mission commander to have the right information, at the right tempo and at the right time when it comes to battlefield engagement.

It also allows commanders to respond appropriately with the benefit of modern applications (apps). Today, apps can be downloaded and delivered almost instantly to the front-line (or where they are required). If there is a change of mission, environment or threat, forces can be rapidly equipped with apps from the combat Cloud that enable them to better act in response. The work we do on Kessel Run[3] with the US Army Futures Command is an example of this in action.

Edge in the military

However, realising the benefits is not possible without multi-domain edge. That is, edge technology deployed over land, air and sea. Its impact is the definition of the sum of its parts because, unless all domains are connected and communicating, commanders will have blind spots and will therefore not have full visibility of unfolding events in the field.

Edge technology is not as widespread in the military as it is in other sectors, like telecoms. Not yet, anyway. Understandably there are more stringent security and reliability requirements while many national forces are tied into existing contracts with providers that may not be able to offer edge technology. Other nations are simply not designed or structured to capitalise on this evolution. Russia, which operates a very monolithic military structure, is a prime example.

While edge deployment and use cases in the military are practically unique when compared to all other sectors, there is one trait that remains consistent irrespective of where or how it is used. That is the need for humans to remain central to its involvement.

Augmenting the best of man and machine

There is a misconception that the more digitised the armed forces become, the less human interaction and intervention there will be. This is certainly not the case. Quite the opposite in fact. It is precisely because more advanced technology is being introduced that humans play an increasingly vital role. The challenge all forces and coalitions face is finding the balance between the two in order to get the best of both.

2. NATO Communications and Information agency, "Agency awards Firefly contrat for deployable communications and information systems", 04/02/2021, URL : https://www.ncia.nato.int/about-us/newsroom/agency-awards-firefly-contract-for-deployable-communications-and-information-systems.html

3. Kessel Run Division "About us", URL: https://kesselrun.af.mil/about/

For a start, technology cannot be relied upon as a sole decision making tool. While the art of warfare is speed of action based on accurate information, and technology is required to navigate through the fog of war, humans remain the best and most trusted judge of action. This means adoption of the edge - and other evolving technologies - is enriching and enabling human decision-making, augmenting the best of man and machine.

At a deeper-level, even leaving aside the emotion, pressure and high-stakes of war, humans don't trust automated systems enough. This is playing out today with leading names from major technology companies voicing their views on the speed of AI adoption. A recent study looked at this issue specifically and found[4] that fully-automated decisions were trusted less than those made when a human is involved. Indeed, results suggest that trust in hybrid decision support was similar to trust in human-only support.

A defining factor between forces

Though for all the advancements made in the armed forces when it comes to technology adoption, we remain much closer to the starting line than we do the finishing one. As the saying goes, "you're never at the end of history, only the middle".

There is no doubt that future military operations will have to include edge of some form. So much so that it will become a defining factor between forces and the difference between victory and defeat.

4. Felix Kares, Cornelius J. König, Richard Bergs, Clea Protzel, Markus Langer "Trust in hybrid human-automated decision-support", International Journal of Selection and Assessment, 01/03/2023 URL: https://onlinelibrary.wiley.com/doi/full/10.1111/ijsa.12423

avisa partners

vmware