VAUBAN
SESSIONS

#5 CLOUD SERVICE MODELS FOR DEFENCE

MARCH 2023

Forward

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 Forward Global 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 Forward Global 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 Forward Global or VMware. Forward Global retains editorial independence at all times in its work.

ABOUT FORWARD GLOBAL

Forward Global is a global economic intelligence, international affairs and cybersecurity group. **Forward Global's 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:
forwardglobal.com

Forward

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

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 Forward Global

CLOUD SERVICE MODELS FOR DEFENCE

CONTRIBUTORS

Axel DYÈVRE
Partner
FORWARD GLOBAL

Marie KETTERLIN
Analyst
FORWARD GLOBAL

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.

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.

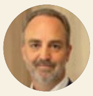
Cloud security requires a high level of expertise from external and internal cloud operators. They must be able to master areas such as identity and access management, connected object security, data security, or the implementation of resilience plans. Otherwise, the risk of losing control of the information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

MORE INFORMATION ON:
VAUBAN-SESSIONS.ORG

Forward

vmware®