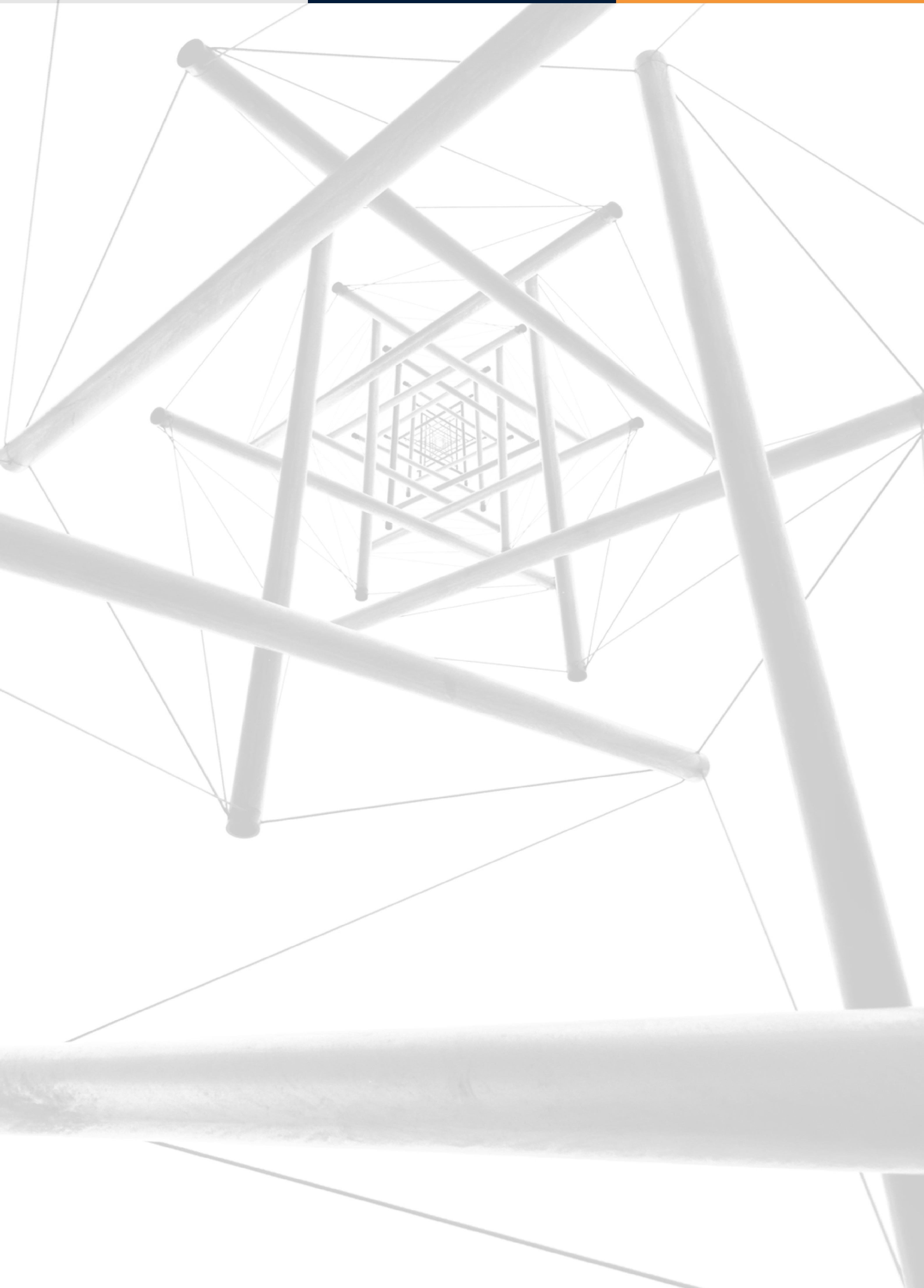
ceis

THE DIGITAL TRANSFORMATION OF ARMED FORCES

A constant (r)evolution

By Axel Dyèvre, Florence Ferrando,
Séverin Schnepp.

Preface by General (ret.)
Jean-Paul Paloméros, Senior Advisor at
CEIS-AVISA Partners, former NATO Supreme
Allied Commander Transformation,
Former Chief of Staff of the French Air Force



CEIS, member of the Avisa Partners group, is a consulting firm specialized in sectors of national sovereignty and their digital transformation. CEIS helps its clients expand both in France and internationally and works to support their interests. Its consultants systematically combine a forward-looking vision with a functional approach, operational knowledge and support to decision-making.

The ideas and opinions expressed in this document are those of the authors and do not necessarily reflect the position of CEIS or the Avisa Partners group.

This White Paper is the result of a partnership between CEIS and VMware. CEIS is solely responsible for the content of this publication, which was developed independently.

Content Summary

Summary

"The ongoing digital revolution has already transformed our daily lives and our access to information at breathtaking speed. It is also a powerful driver of transformation for the working world, for administration and more broadly for decision-making systems." [1]

The technologies on which digital transformation is based are constantly evolving, setting them at odds with the traditional development cycles of weapons programs. In this age of connected and collaborative combat, Armed Forces must be able to adopt the best technologies and innovations as quickly as possible to stay at the top of the game in terms of operations and IT systems. NATO, in its "Framework for Future Alliance Operations", therefore emphasizes the importance of collaboration with the research and private sectors—which draw on innovation in the digital domain—so that Armed Forces can maintain a decisive technological advantage.

To increase the agility and flexibility required to integrate the constant evolution of digital technologies, one innovative solution separates software (which evolve very quickly) from hardware (which naturally evolves more slowly) in information systems. The use of these so-called "virtualization" technologies can deliver significant operational gains:

- Reduced weight, bulk and energy consumption
- Less support needed
- Facilitation of deployment and build-up
- Increased application flexibility and agility
- Stronger cybersecurity for information systems

As beneficial as it may be, the use of virtualization by armed forces must form part of an overall strategic approach which takes into account all technical, organizational and financial variables.

[1] Source: *"Digital ambition of the French Ministry of the Armed Forces"*

Preface: Digital transformation at the core of future military operations

The instability of the geostrategic environment, characterized by sudden, simultaneous and enduring crises, confronts Armed Forces with multiple, demanding requirements.

They must be able to both react instantly and sustain long-term operational commitments. They must also adapt to adversaries' new asymmetric and hybrid strategies supported by a large spectrum of modus operandi ranging from rustic to the most advanced and sophisticated. On today's battlefields, Armed Forces have to cope with long standing proven combat techniques (i.e., IEDs), as well as high-end technologies (in particular in the digital space).

Last but not least, they must also prepare for the resurgence of major conflicts involving great powers able to employ numerous, diverse and modern weapon systems, including the most disruptive military technologies (i.e., hypersonic missiles). This new complex, unstable and highly risky environment creates great expectations from both political leaders and citizens from their Armed Forces, made even greater by their perception that large amounts of money are spent on defense modernization.

As far as Western Armed Forces are concerned, while they cannot increase significantly in number to answer increasing and pressing calls, they dramatically need to improve their operational efficiency, from realistic training to high-tempo operational engagement. As such, succeeding in operationalizing digital transformation represents both a great opportunity and a crucial challenge. The digitalization of weapons systems is nothing new, neither are digital Command and Control networks addressing strategic, operational or tactical levels, and able to disseminate multi-source intelligence throughout the operational chain. Today, however, there is an increasing gap between the pace of digital transformation in the private sector and the traditional, incremental procurement process in the military domain. As a matter of fact, the civilian world can make the best of exponential digital technology breakthroughs brought about mainly by US digital superpowers. Not to be ignored either are the titanic efforts made by China to develop its own digital ecosystem supported by a large, dynamic and protected internal market. Last but not least, the "private" digital transformation is fueled by designers and users' limitless imagination and creativity. Armed Forces, for their part, face a kind of digital dilemma. On the one hand, they operate weapon systems which must be certified, secured, and ultimately combat proven, which limits their potential for evolution. On the other hand, they need to keep up with the pace of digital technology and leverage the benefit of private-sector digital dynamism if they want to improve their own efficiency and match the rapid evolution of threats. This is the crucial digital challenge which modern Armed Forces must face. This is the digital battle they must win to improve their readiness, their reactivity, their flexibility, to master information and intelligence warfare, to dynamically tailor their command and control systems and enable adaptable and multiple actors' networks. In addition, bringing digital transformation to the core of military operations will dramatically improve logistics management and reduce operating costs. Last but not least, building, protecting and defending cyberspace 24/7 lies at the heart of the digital battle. Cybersecurity must be considered and embedded at all stages of an effective digital operational transformation.

Cooperation between Armed forces and the digital industry represents a precious key to take on the military digital challenge. It must be built on sound principles.

Operational needs remain the first and most important priority, risk management should become a shared responsibility, rapid and incremental operational experimentation should be the tool of choice. Among many key objectives, collaboration between the military and the private sector should aim to develop digital systems both resilient and easy to reconfigure, fostering leaner logistics and adaptive maintenance, ensuring seamless cybersecurity.

For Allied Nations, and those partners who intend to take part in coalition operations, interoperability is a clear goal, almost a prerequisite. So far, in particular within NATO, interoperability has been established through common agreed standards (STANAGs). But, as far as digital transformation is concerned, defining those common norms in a fast evolutive cyberspace represents a major challenge in itself. One traditional way to achieve this goal consists in accepting major digital companies' own standards, but following this road presents a great risk of irreversible dependency.

As a matter of fact, operationalizing digital transformation is not only a technological challenge. It is above all a strategic and conceptual one which leads to reconsidering some fundamental principles, particularly in terms of operation command, control and execution. The underlying question is how best to harness huge flows of data and resulting information. In the end, operational digital transformation has already proved itself to be a pre-requisite to gaining and maintaining a required level of strategic autonomy. To succeed and take the most advantage of this outstanding opportunity, traditional procurement processes have reached their limit. It is no longer possible to conceive large and somewhat cumbersome information systems, and to afford their expensive operating and maintenance costs. Therefore, in their quest for flexibility, reliability, and efficiency, Armed Forces must be able to leverage the full benefit of the most recent technologies and leverage the dynamism of the digital market while keeping the overall control of their information systems. Relying on a single powerful digital provider, whoever that may be, to achieve those goals may seem an easy solution, yet would entail a high risk of overreliance and would lead to unacceptable dependency. Therefore, new ideas should be considered both in terms of partnership and technology. Among the most promising, the virtualization of information management has already showed its great potential, with many Armed Forces having experimented and deployed it to support major digital projects. To keep it simple, virtualizing information systems aims to allow different operating systems and applications to be run simultaneously and independently on a single host server. To allow this IT breakthrough, virtualization takes the most benefit of new miniaturized chips, which enable the development of small autonomous virtual machines (VM) directly implanted on the host server. Key to virtualization is the interfacing between the host server and VMs. This is done with a thin "hypervisor" software layer which allows a dynamic task allocating to each single VM according to requirements. Therefore, it is easy to figure the potential of virtualization in optimizing each server's efficiency, then limit the associate quantitative requirement, improve information systems resilience, provide greater agility and reconfigurability. This is paramount to assure the highest interoperability between different command and control networks and operational systems, which remains more than ever a crucial goal within NATO or any ad hoc coalition. Today, virtualization is no longer a concept or a future technology, as it has already been operationalized in major Armed Forces such as the US Navy, US Airforce or UK Royal Navy, which integrated virtualized systems in its new generation ASTUTE Class nuclear-powered attack submarines. This example and others are presented in this paper, which aims to be both an introduction to operational digital transformation and a sound analysis of the potential benefits of virtualization for Armed Forces.

As a breakthrough concept and technology, virtualization paves the way to a new era, allowing the development of agile and interoperable command, control and, more broadly, operational information systems, able to respond to the most demanding operational requirements of modern Armed Forces. In a nutshell, virtualization is a great tool to anchor digital transformation at the core of today and tomorrow's military commitments.

General (ret.) Jean-Paul Paloméros
Senior advisor, CEIS-Avisa Partners
Former NATO Supreme Allied Commander Transformation
(NATO SACT)
Former Chief of Staff of the Air Force

Digital transformation: a constant evolution

Since the 1990s, “digital transformation” has led to an explosion in communications devices and data volumes: the volume created has increased from 2 zettabytes (i.e., two billion terabytes) in 2010 to 47 zettabytes in 2020. The trend is expected to continue, with the volume of data created set to reach 2,142 zettabytes (ZB)[2] in 2035.

IT infrastructure—networks, hardware and software—has therefore become a determining factor in civilian or military organizations’ capacity, be they public or private, to benefit from the performance and operational efficiency gains generated by this digital transformation.

Harnessing civilian, market-driven innovation, particularly in digital technology, has therefore been a challenge for the Armed Forces for several years now. The increasing pace of digital innovation is particularly reflected in the arrival on the market of new software solutions and applications at a rate that is difficult to sustain for traditional procurement cycles of weapon systems, the lifespan of which can extend over several decades.

Virtualization technologies and their digital foundation allow software and applications to evolve flexibly, independently of the physical infrastructure on which they are deployed. They also offer the possibility of incremental evolution in information systems’ capabilities, including remotely, in the field, in operation, overseas, thus contributing to mission delivery.

Principle of virtualization

“IT infrastructure” refers to all the hardware and software resources, namely:

- Servers and IT terminals (work stations, tablets, cellphones)
- Networks
- Connected objects (cameras, various sensors, etc.)
- Software and applications

With digital transformation, a key consideration is ensuring the ongoing functionality of the infrastructure, which has become essential to organizations.

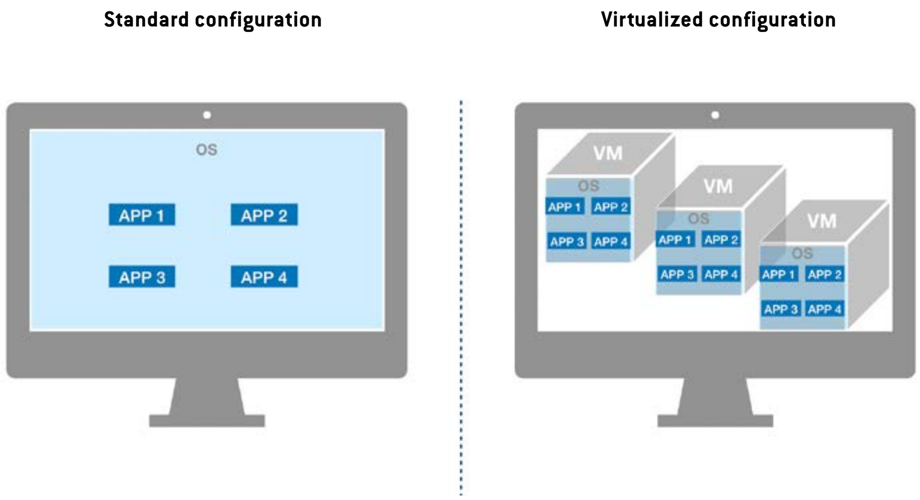
[2] “The volume of data will multiply by 45 between 2020 and 2035” (), Journal du Net, Marjolaine Tasset, URL
As a guide, 1 zettabyte (1021) equals 1 billion terabyte. In comparison, the latest iPhone model (XR) has a maximum capacity of 128 GB. One terabytes equals 1 024 gigabytes.

Within IT infrastructure, computers consist of several elements, which can be structured into different "layers":

- Hardware[3]
- Operating System[4]
- Softwares

The principle of virtualization consists in optimizing hardware use by running several segregated environments on it, each with its own OS, applications and therefore network access. The "instances" created are called a "virtual machines" (VMs). This process makes the best use of a computer's physical resources (computing power and memory, for example).

Comparison of standard and virtualized configurations



Standard configuration

Virtualized configuration

[3] "Definition: hardware", Le Mag IT, URL

[4] "Definition: OS", Culture Informatique, URL

What can be virtualized?

Depending on user needs, the following can currently be virtualized[5] :

- **Operating systems:** virtualization makes it possible to place several virtual machines on the same physical machine, all of which operate in parallel as if there were several machines. This means that the capacities of the physical machine are maximized, while limiting its size, power consumption, weight, and heat dissipation.
- **Workstations:** Users can simulate their work environment from any connected device to access them from anywhere. This also makes maintaining and upgrading workstations easier because the applications on virtual workstations reside on a central server, allowing all updates and backups to take place simultaneously and in a harmonized manner (thereby respecting compliance standards). Another advantage is the option of running several partitioned environments on the same workstation and even several operating systems to use specific applications, for example.
- **Applications:** With virtualization, applications are executed in an "encapsulated form " (also called a "container")[6], which allows users to ignore the operating system. As an example, a Windows software can be used on Linux or Mac OS. Regardless of the OS, users can run applications, bypassing this limitation without virtualizing the entire system.
- **Storage:** Virtualization software identifies the storage space available on physical machines connected in a network and creates a "virtual disk" which can be controlled from a central interface. This storage space is seen as a single disk by the computers that use it, and it is the virtualization software that distributes the data over the physical spaces available.
- **Data:** Virtualizing data means an application can access said data and "use it without needing the details of the physical location or format of the data."[7] This access is made possible by a specific virtualization software, which retrieves the "scattered" data within an IT environment and groups it into a single form by virtualizing it.[8] Thus, by relying on a dashboard integrated into the virtualization software, the user can aggregate data from several sources at different physical locations without having to copy, move or format it beforehand.
- **Network:** A traditional network relies on hardware resources (switches, routers, servers, cables and hubs. [9] Virtualizing a network makes it possible to disregard its hardware components because a virtual network can "combine several physical networks [...] or even divide a physical network into several independent and distinct virtual networks." Here, virtualization makes it possible to optimize network functions and offers several advantageous use cases: preparation of updates or new network configurations, testing before installation on the network and even simplification of network management based on the needs of different users and available bandwidth.

[5] *"What is virtualization?"*, Citrix, URL

[6] *"Virtualization: What is it and what does it do?"*, Le Big Data, URL

[7] *"What is virtualization?"*, Citrix, URL

[8] *"What is virtualization?"*, Red Hat, URL

[9] *"What is virtualization?"*, Red Hat, URL

Operational gains for Armed Forces

For both Armed Forces and the civilian sector, investing in virtualization solutions offers financial gains because fewer physical computers (hardware) are required to perform the same tasks. Studies estimate that IT infrastructure using virtualization reduces the number of physical workstations and servers by 50%.[10] The cost of software licenses remains the same because they are used “virtually”.

Armed Forces have very specific constraints. As a result, operational advantages must be considered in addition to more general advantages.

- **Reduced weight and bulk**. The platforms concerned (land command vehicles, shelters, planes and ships) are, by nature, small spaces. Digital transformation requires the Armed Forces to have increasingly embedded computing capabilities. Being able to reduce bulk and weight while increasing available power is a real advantage in the battle for operational information superiority.
- **Energy Reduction.** Electricity consumption and heat dissipation are specific challenges for military platforms. The more electronic equipment consumes, the more the dedicated engine power is and the greater the fuel consumption, with all the autonomy and logistics limitations that this entails. Heat dissipation caused by their operation also generates ventilation and cooling requirements, which increases energy consumption. By virtualizing IT infrastructure, estimates show that energy requirements can be reduced by up to 80%. [11]
- **Less support needed.** The reduction in physical resources logically leads to a reduction in material maintenance operations and therefore fewer dedicated staff members. Some studies say that the gain of virtual machines can reach up to 50% in terms of investment and maintenance compared to physical machines.[12] For Armed Forces who constantly seek to reduce their logistical footprint to decrease exposure and improve maneuverability, this advantage provides real added value in operational terms.

[10] *“The virtualization of data, an economical solution”*, CapInfo, November 2019, URL

[11] *“How VMware Virtualization Right-sizes IT Infrastructure to Reduce Power Consumption”* VMware, URL

[12] *“4 major benefits of virtualisation,”* ACCU, URL

Virtualization on board Astute-class submarines

The latest generation of British Navy nuclear attack submarines (Astute class) incorporates a virtualization solution for their integrated combat system, which is highly sensitive and considered to be the "eyes, ears and nervous system" of the warship. Tested in 2016 for a torpedo firing, the solution provided by VMware, Dell and Aish supports crew members' decision-making by processing the data collected by the submarine's sensors. The use of this technology has made it possible to reduce the volume of physical equipment with a «miniaturized» data center, providing the operational center of the submarine with more flexibility. In addition to reducing the size of embedded computer equipment, the solution also improves performance, as close as possible to real time, and improves the availability of vessels by decreasing the time needed to configure systems and their updates.

Source
https://www.baesystems.com/en/article/artful-submarine-fires-first-torpedo-using-new-common-combat-system

- **Facilitation of deployment and build-up.** The application flexibility of virtual machines, coupled with the digitization of this configuration, makes it possible to configure a virtualized environment based on the mission and operational requirements faster and more easily than with traditional solutions. "Out of the box" VMs can be transferred using network transfer or physical media. For example, configuring the information systems required for a vessel takes several weeks, even months, for a standard configuration because the preparation phase involves testing and updating the vessel's IT infrastructure. The virtualization of these information systems makes it possible to reduce the time spent on their deployment by configuring them upstream, downloading the upgrades through the network, logically freeing up more time for operations while increasing the availability of the vessel. While the concept of digital twins—a sort of carbon copy of a system's configuration—is not new, virtualization can greatly simplify implementation. In the United States, a virtual digital twin of the nuclear-powered aircraft carrier Abraham Lincoln (CVN-72, in service since 1989) was used in late 2019 to test and assess embedded systems to be installed. The analysis of the operation of these systems in the "virtual lab"[13] identified overlaps in processes performing the same tasks. By correcting the problems identified in this way—a process currently in progress—a significant gain in bandwidth is expected, which is a constant challenge for Armed Forces.

[13] "*NAVWAR completes first digital model of systems on USS Abraham Lincoln*," Naval Information Warfare Systems Command, 10/23/2019, URL

Virtualization of a C2

The **United States Central Command (USCENTCOM)** has developed a control, command and communication (C3) system to make operations easier in coalition mode. Deployed via a network of satellites and fully virtualized, it allows each of the United States' Allied Nations to connect to a common digital environment bringing together information collected by different sources (ground units, reconnaissance drones, armored vehicles, forward headquarters). This has many advantages:

- Rapid deployment of the system (10–15 minutes)
- Improved coordination and interoperability of allied forces, each receiving the same information at the same time (continuous and near real-time flow)
- High level of security (micro-segmentation of the network with VMware NSX) preventing attack propagation on the whole network and providing more time to counter such attacks
- Quick disconnection once the mission is complete (2–5 minutes).

The system was tested during the Bold Quest exercise (Savannah, Georgia, United States), which brought together 1,800 troops from 16 allied countries

- **Increased application flexibility and agility**. Increased application flexibility and agility. For Command & Control (C2) systems, for example, virtualization makes it possible to easily deploy, backup and restore virtual machines. It is the principle of encapsulation[14] that technically makes it possible to simplify actions on virtual machines (copies, backups or creation) and, in particular, completely move computer systems from one physical server to another without causing any interruption in services. This means that the fleet of virtual machines in a C2 can be adjusted quickly, or even reconfigured, based on operational requirements using the options offered by a tactical Cloud deployed as close as possible to the theater of operations. By way of illustration, during Exercise Trident Jupiter (late 2019), NATO assessed the performance of its IT systems, including its RemoteApp Provisioning Service, a system that enables users to use NATO computer applications that are not installed on their workstations. Another key element of the exercise was the 18-hour deployment of the Communication and Information Network (CIS) by a NATO battalion based in Bulgaria. Through the use of the virtualized tactical C3 system "DragonFly HQ08", adapted to a dynamic network and using micro-segmentation to guarantee its cybersecurity, the Bulgarian battalion was able to provide a communication network to users located in Stavanger, Norway.[15]

- **Virtualization of legacy systems.** Armed Forces have a variety of existing systems and equipment (legacy systems[16]); integrating them into a modern digital environment is challenging. Moreover, not having been designed to operate in environments which are as connected as today's, they can be vulnerable to cyberattacks. The ability to "carry" these old systems[17] on virtual machines running on modern environments means their operational life can be extended, avoiding complete overhauls.

[14] *VMware vSphere 4. Installation of a virtual infrastructure*, URL

[15] "*NCIA puts IT systems to the test in exercise Trident Jupiter*", NCIA, , URL

[16] The term legacy system refers to one used by an organization that is in some way outdated compared to the state of the art or the current market.

[17] *VMware vSphere 4. Installation of a virtual infrastructure*, URL

Kessel Run[18], a radically different U.S. Air Force approach to innovation

A sort of "software factory", the USAF Kessel Run project offers a radically different approach to innovation, using an agile methodology. Kessel Run solved many of the challenges previously encountered in the development of software used by the U.S. Air Force.

The project stands out with:

- A project based on an agile development platform for business applications by end users (VMware Pivotal Lab)
- Development thus led by military personnel, closely aligned to operational requirements
- Operational application design in short iterative cycles and rapid deployment through virtualization and containers
- Automated deployments of updates for developed applications.

The Kessel Run teams thus managed to deliver an approved development platform for a Secret Internet Protocol Router in less than 130 days to a base in Qatar—where the previous program lasted 10 years and cost close to $340 million without *"having provided significant capacity".*

Sources:
https://mwi.usma.edu/software-wins-modern-wars-air-force-learned-kessel-run/ & https://media.defense.gov/2019/Mar/07/2002097482/-1/-1/0/SWAP_STUDY_VIGNETTES.PDF

[18] "Why Kessel Run is such a big deal", The Business of Federal Technology, URL

Strengthening the cybersecurity of military systems

The need for connectivity, even hyperconnectivity, is the core of IT systems and equipment's cybersecurity issues. Connecting and communicating across dispersed forces and coalition members is essential to gather, analyze, and process information and deliver actionable information across deployed and back end systems. However, by its very nature, connectivity creates cyber vulnerabilities. It makes sense that a totally isolated server, dedicated to a single application, will be better protected because it has only one entry point. This vision however is increasingly one of the past.

In this age of collaborative and therefore connected combat, virtualization makes it possible to strengthen the cybersecurity of information systems:

- ***"Silo"* Operations**: Virtualization makes it possible to create as many virtual machines as there are needs and to run operating systems and applications in an isolated and independent manner, without having to increase the number of machines. Each virtual machine has its own configuration, applications and adapted network configurations, thereby limiting cyber risks.
- **Security provided by isolation** : The isolation of virtual machines keeps them and others secure because potential vulnerabilities on one VM do not affect others, even though they operate with the same hardware components. VMs can also serve as a secure space to test software updates before rolling them out to all workstations. By the same principle, Network Virtualization allows the network segmentation with corresponding user right. This logical segmentation, called micro segmentation, is the most effective cyber barrier. Hence, any cyber breach is limited to a segregated environment, providing time to detect, isolate and neutralize the threat before propagation.
- **Segregation of work environments**: Virtualization allows different working environments to coexist on the same computer hardware in complete segregation. This possibility has advantages for coalition operations because it allows, for example, a French operator deployed as part of a NATO mission to use its usual system and the Alliance system on the same computer. Each system is hosted by a different and isolated virtual machine.
- **Creation of secure environments for friendly forces.** In a coalition context, virtualization makes it possible to include friendly forces in an information system, more simply and securely, by providing them with secure and ready-to-use VMs, which they can easily place on their infrastructure.
- **Simplified creation of *"honeypots"***. Virtualizing an information system also eases the transition to a more aggressive stance in terms of cybersecurity. The *honeypot technique*[19] creates a false network to deceive the adversary and observe its methods and targets without compromising the rest of the network and equipment. As a result, the adversary's resources are mobilized on a fictitious target which can also "brainwash" the adversary by giving it access to false information. Virtualization helps the implementation of these honeypots by minimizing requirements while maximizing how realistic they appear.

[19] *"Why use virtualization?,"* Françoise Berthoud & Maurice Libes, URL

Challenges of digital transformation

While virtualization can provide answers to the problems which Armed Forces face in their digital transformation, certain points must be taken under careful consideration to succeed in deploying the software solution securely and effectively.

Scalability and maintenance

The availability of IT and cybersecurity skills is a major challenge for Armed Forces, as is the choice of architectures and solutions implemented; license and integration costs are therefore key points to factor in. Indeed, like any software, virtualization solutions must be deployed, maintained and updated regularly to adjust to changing environments, correct operating anomalies and security breaches and ultimately develop new functions.

Of course, open-source virtualization solutions exist, such as Oracle VM VirtualBox and OpenVZ.[20] These solutions are often free of charge and allow easy access to the source code. However, as with all open-source software, maintenance is not contractual and is therefore not always performed with the same diligence as for proprietary solutions, because it often takes place in the form of "volunteer work" from the community, which provides support. Poor support of ten forces user organizations to take responsibility for software integration issues themselves or call on contractors, thereby increasing costs. The lack of technical roadmaps can also be a drawback in terms of organizational planning. For example, in the field of virtualization, only VMware—the world leader in virtualization solutions— invests some $2 billion annually in its R&D activities.[21]

The use of a virtualization solution, whether proprietary or open source, is inherently attractive because the infrastructure develops around specific solutions. This aspect should be taken into consideration to avoid problems with architecture durability if development of the solution is stopped—a risk that is often more unpredictable for open-source solutions—if there is a change in pricing policy or even if there is a new technological breakthrough.

[20] *"An update on Open Source virtualization,"* Wooster, June 2014, URL

[21] *"NITECH. NATO Innovation and Technology,"* NCI Agency, June 2020, URL

Controlling data

Several types of virtualization solutions exist on the market, whether open source or proprietary. Among these, so-called "on-premises" virtualization solutions seem to be the best suited for military use. This process allows Defense stakeholders to license the software and use it independently, while remaining responsible for the management of the IT infrastructure mobilized—a significant effort in terms of human resources and skills compared to Cloud solutions. On the other hand, on-premises solutions enable Armed Forces to maintain control over their implementation and, above all, keep their data on internal networks.

Standards and certifications

Rapid technological developments pose standardization and certification issues regarding the resilience and security requirements specific to the defense sector. Indeed, these standardization and certification processes are long, with procedures which are out of step with the fast pace of technological innovation. For example, a virtualization solution or service may be halfway through a certification process and then be subject to an update or a version change during that time, making the certification process outdated. However, some virtualization solutions, such as VMware[22] or Red Hat (for Linux OS),[23] for example, comply with international standards, such as the Common Criteria,[24] or national standards, such as the U.S. Federal Information Processing Standards (FIPS). In addition, virtualization solutions typically incorporate security arrangements to ensure their resilience, such as hypervisors that support the management of virtual machines. By assigning them specific tasks, the principle of isolation can be applied between the various virtual machines deployed.

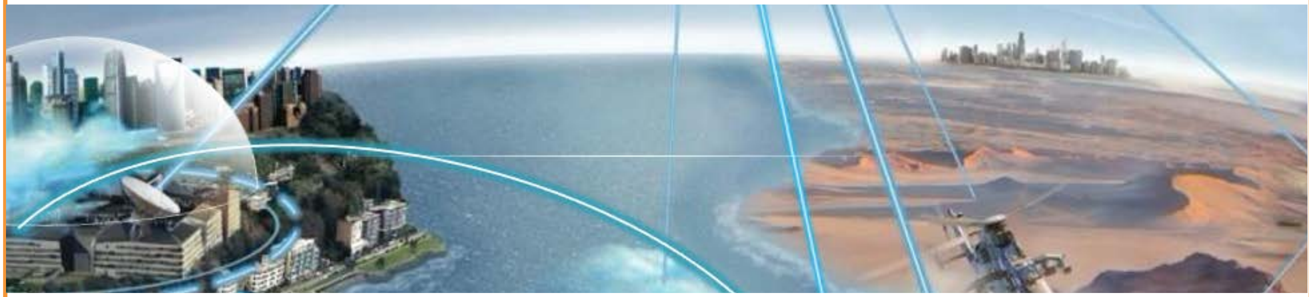
[22] VMware FIPS 140-2 Validated Cryptographic Moduless, URL

[23] Red Hat Completes FIPS 140-2 Re-certification for Red Hat Enterprise Linux 7, URL

[24] The Common Criteria (CC) consist of a set of standards for assessing the security of systems and software, URL

NEXIUM DEFENCE CLOUD

Information is a decisive weapon in today's military actions. NEXIUM Defence Cloud (NDC) is an accredited cloud solution for Armed Forces aimed at ensuring information dominance and system compactness. Its private elastic cloud-native infrastructure is highly secured. It is available from homeland to theatre command posts and mobile units next to the soldier. It supports demanding defence requirements, including military security and ruggedized hardware, and conforms to latest standards like NATO Federated Mission Network (FMN).



The main benefits are:

- Acceleration of the collaborative combat (situation awareness, etc.), OODA and sensor-to-shooter loops, and intelligence consolidation and information sharing across domains,
- Secured information sharing with a Zero Trust architecture, military grade encryption, multilevel classification and need-to-know access,
- Mastered fast and adaptable deployments, agile reconfigurations with a fully orchestrated Communication and Information System (CIS) including heterogeneous networks and ciphering,
- Resiliency to disconnected, intermittent and low bandwidth connectivity, and electronic and cyber warfare,
- Rugged hardware form factors to cope with extreme environmental conditions (size, weight, power, cooling, vibrations, etc.) and reduced logistics with standardized form factors,
- Agility with cloud-native properties (DevSecOps chain, virtualisation, containers, etc.),
- Support of cloud-native applications relying on latest digital technologies (Data Analytics, AI)
- The Nexium Defence Cloud infrastructure maximizes the use of constrained IT and network resources with virtualization in order to provide agile and fluid operational capabilities. The transparent management of all compute, storage and network resources requires less operation expertise on the field. Optimal use of battlefield heterogeneous network capabilities maintains the highest level of digital service availability.
- NEXIUM Defence Cloud smoothens the cloud transition exposing all legacy and new digital services into a single user portal, and reduces the TCO (Total Cost of Ownership). It benefits from the extensive and enduring VMware portfolio of cloud technologies.
- NEXIUM Defence Cloud solution can operate in all domains and in coalitions. Whatever it takes.

The Nexium Defence Cloud infrastructure maximizes the use of constrained IT and network resources with virtualization in order to provide agile and fluid operational capabilities. The transparent management of all compute, storage and network resources requires less operation expertise on the field. Optimal use of battlefield heterogeneous network capabilities maintains the highest level of digital service availability.
NEXIUM Defence Cloud smoothens the cloud transition exposing all legacy and new digital services into a single user portal, and reduces the TCO (Total Cost of Ownership). It benefits from the extensive and enduring VMware portfolio of cloud technologies.
NEXIUM Defence Cloud solution can operate in all domains and in coalitions. Whatever it takes.

Conclusion: prospects

Virtualizing new equipments. While virtualization technology is considered mature for IT infrastructure components (servers, workstations, networks, data, applications), with use cases in various Armed Forces, other IT systems are yet to be virtualized. This is the case for terminals operating under a so-called Advanced Risk Machine (ARM) architecture. The architecture of a system establishes how it is set up to perform its function.[25] ARM architecture is used for smaller processors[26], integrated into most tablets and smartphones, as well as connected objects, including embedded sensors (vehicles, smartwatches, robotics, weapon systems, etc.). To date, the virtualization of this type of equipment is still at an experimental stage, given the miniaturization of electronic components and their limited power, making it technically difficult to optimize the operation of additional software.

Facilitating the use of the Cloud in Armed Forces. The use of tactical Clouds contributes *"to the networking of all stakeholders and the optimal use of information for conducting operations."* [27] The use of virtualization makes it possible to multiply the potential of the Cloud because it allows computers connected to it to make additional resources available or draw on other servers and terminals (software, data, storage and computing power, for example). Virtualization makes it possible to further streamline the operating capacities of each machine (hardware) making up the IT equipment and offering more flexible management of the entire IT system thanks to the automation of certain processes (software).

Get ready for 5G. One of the main limitations of military Cloud usage today is the generally limited bandwidth of military networks. For several years, Armed Forces have been studying and testing "Tactical LTE bubbles" using private 4G to access very high mobile speed during operations. By doing this, they can obtain higher bandwidth than with conventional radio networks in order to share any type of multimedia information (voice, photos, video, geo-referenced information, etc.). According to the French Ministry of Armed Forces, *"the use of 5G tactical bubbles, succeeding 4G/LTE bubbles, would allow Cloud services and technologies to be used in the field."*[28] 5G[29] technology can provide 10 to 100 times more bandwidth than current 4G[30] networks, which would greatly speed up the interconnection between various elements. Unlike 4G networks, 5G networks will be decentralized. Essential functions, such as routing and communication, will no longer be managed at core network level only; they can be remote, at the periphery or at base station level. Virtualization will be central to 5G deployment with *Network Function Virtualization* and *Software-Defined Network* type architectures, which will be based on the separation of the routing (transmission of information from a source to a target) and control (calculation of routes, implementation of prioritization and rejection policies) functions of the network. This will make software-defined networking more flexible, and, by eliminating the physical bricks (hardware), virtualization will help to reduce investments and operational costs. Central software will manage and coordinate tasks previously run by physical infrastructure, thus limiting operating costs. In addition, by improving reliability, performance and bandwdth and reducing latency, 5G can help ease network virtualization, allowing forces in theaters of operations to deploy, for example, virtualized C2 systems quickly and remotely.

Recent publications

Download at www.avisa-partners.com/publications/

- A2/AD, access denied and zone prohibition: Operational reality and limits of the concept
- Artificial intelligence: Applications and challenges for the Armed Forces
- Blockchain, Challenges, uses and constraints for Defense
- Intelligence: human factor and cognitive bias
- Immersive reality: Uses of virtual and augmented realities for Defense

THE DIGITAL TRANSFORMATION OF ARMED FORCES

A constant (r)evolution

By Axel Dyèvre, Florence Ferrando, Séverin Schnepp.

Preface by **General (ret.) Jean-Paul Paloméros, Senior Advisor** at CEIS-AVISA Partners, former NATO Supreme Allied Commander Transformation, Former Chief of Staff of the French Air Force.

ceis

avisa partners

CEIS, member of the Avisa Partners group, is a strategic consultancy specialised in sectors of national sovereignty and digital transformation.

CEIS Paris
Tour Montparnasse - 33 avenue du Maine
BP 36 - 75 755 Paris Cedex 15
France

CEIS Brussels
Boulevard du Régent, 35
1000 Brussels
Belgium

www.ceis.eu
www.avisa-partners.com