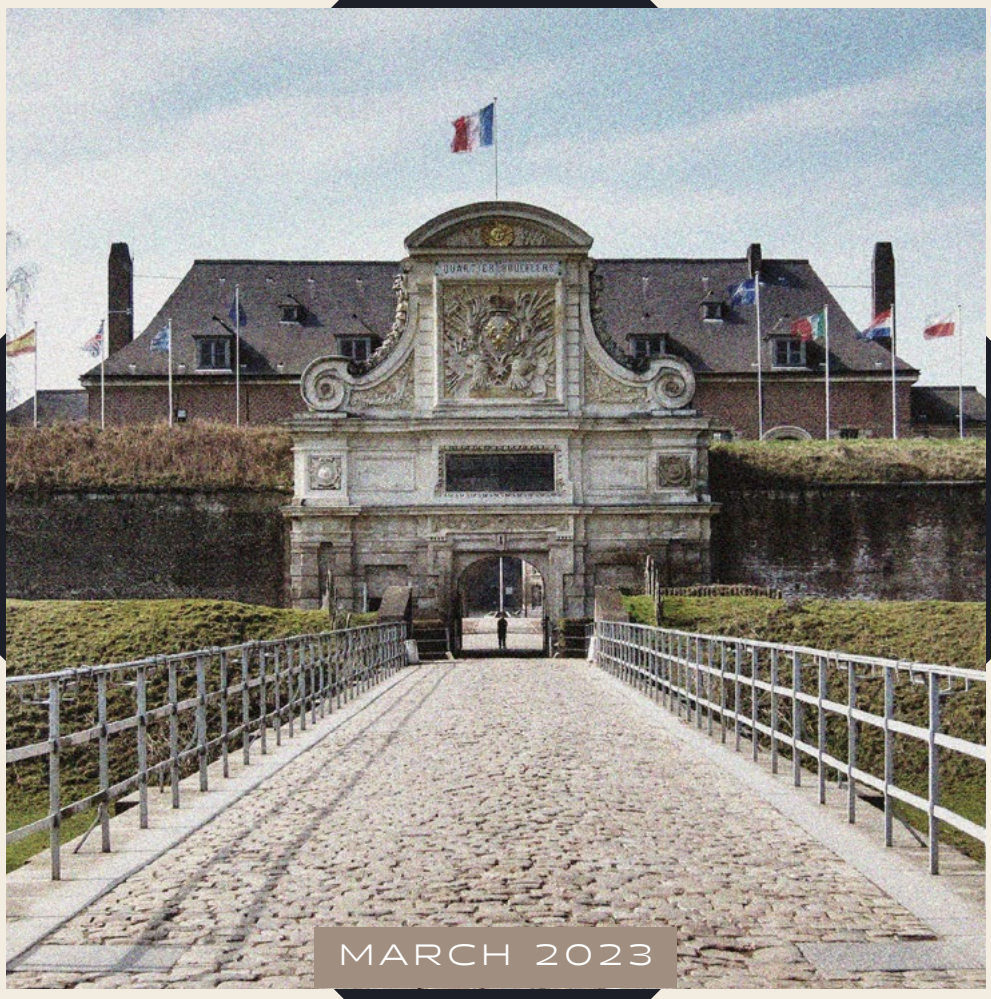
VAUBAN
SESSIONS

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



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 Group 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 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 Forward Global

1. Cf. Vauban Paper n°5.

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

CONTRIBUTORS

Axel DYÈVRE
Partner
FORWARD GLOBAL

Martin DE MAUPEOU
Director
FORWARD GLOBAL

Marin MESSY
Analyst
FORWARD GLOBAL

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.

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.

Forward

vmware