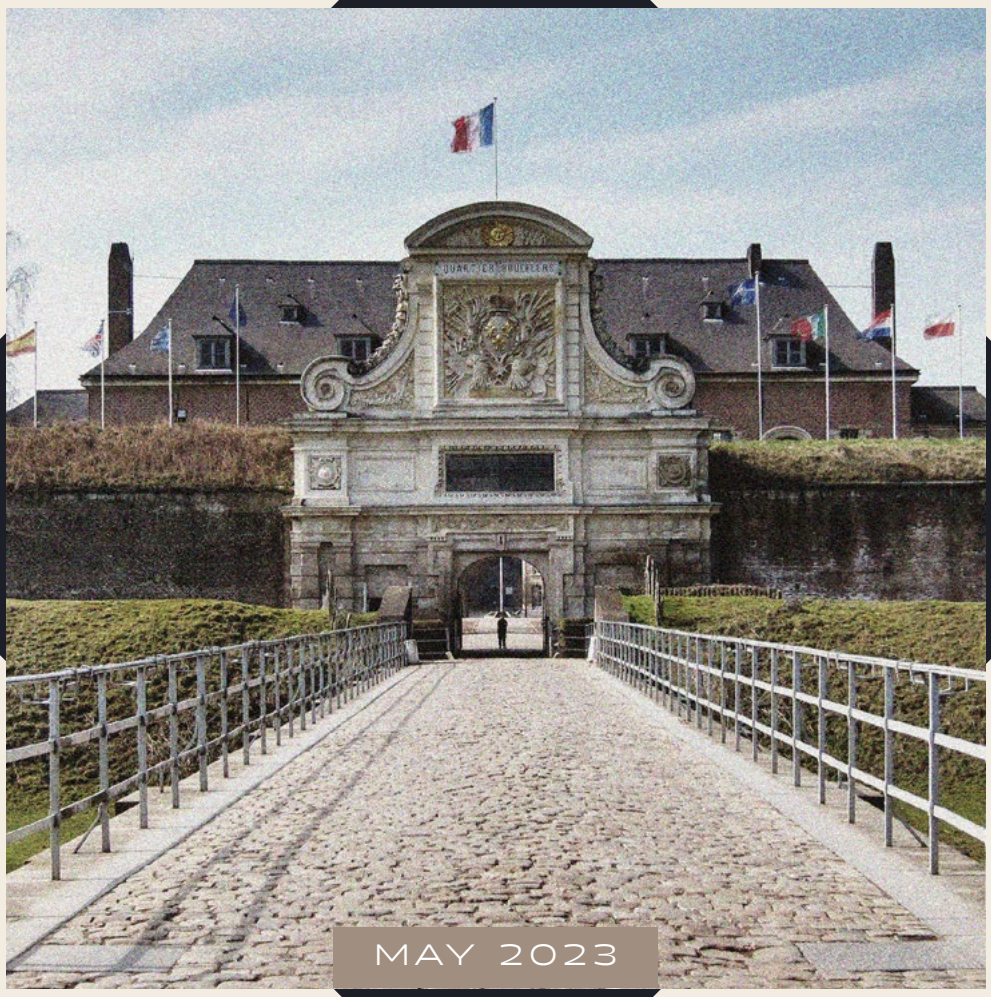
VAUBAN
SESSIONS

#8 CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT



MAY 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

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

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

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

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

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

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

CONTRIBUTORS

Axel DYÈVRE
Partner
FORWARD GLOBAL

Martin DE MAUPEOU
Director
FORWARD GLOBAL

Marin MESSY
Analyst
FORWARD GLOBAL

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

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

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

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

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

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

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

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

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

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

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

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

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

Meeting the challenge of the connected battlefield

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

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

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

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

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

Controlling the security of an interconnected environment

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

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

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

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

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

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

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

CONTRIBUTOR

Isidoros MONOGIOUDIS
Project Officer for Information Technologies
EUROPEAN DEFENCE AGENCY

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

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

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

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

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

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

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

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

→ **Edge users (combatants):**

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

→ **Strategic/Operational users:**

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

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

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

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

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

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

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

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

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

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

CHALLENGES OF DEPLOYING A TACTICAL CLOUD FOR COLLABORATIVE COMBAT

CONTRIBUTOR

Joe BAGULEY
Vice-president & Chief Technology Officer EMEA
VMWARE

Turning to the edge to gain advantage in the field

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

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

Pushing innovation to the front line

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

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

Edge in the military

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

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

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

Augmenting the best of man and machine

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

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

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

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

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

A defining factor between forces

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

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

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

Forward

vmware