VAUBAN PAPERS

avisa partners

vmware

WWW.VAUBAN-SESSIONS.ORG

THE VAUBAN PAPERS
COLLECTION

This collection of papers on the impact of digital transformation on Armed Forces and on the conduct of operations summarises the first series of "Vauban Papers", the result of a partnership between Avisa Partners and VMware.

The Papers are both the result and follow-up to the discussions held during the Vauban Sessions 2021 and 2022, an annual conference organised by Avisa Partners and the Rapid Reaction Corps - France (RRC-Fr), in Lille. The 2022 edition brought together over 150 representatives from 19 NATO Nations' Armed Forces, as well as from NATO, EU institutions, and defence industry.

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

ABOUT AVISA PARTNERS

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

For more information, please visit:
www.avisa-partners.com/?lang=en

avisa partners

ABOUT VMWARE

VMware is a leading provider of **multi-cloud** services for all apps, enabling **digital innovation** with enterprise control. As a trusted foundation to **accelerate innovation**, VMware software gives businesses the **flexibility and choice** they need to build the future. Headquartered in Palo Alto, California, VMware is committed to building a better future through the company's 2030 Agenda.

For more information, please visit:
www.vmware.com/company

vmware

COLLECTION

VAUBAN PAPERS

SUMMARY

WWW.VAUBAN-SESSIONS.ORG

VAUBAN SESSIONS

VAUBAN PAPERS

#1 DATA: THE CORE OF COLLABORATIVE COMBAT

avisa partners

vmware

WWW.VAUBAN-SESSIONS.ORG

FOREWORD

Twenty years ago, the revolution in military affairs (RMA) was described as a new approach to warfare, focused on the use of information and automation on the battlefield to make forces "more lethal" and more "agile". During the last decade, the accelerated digital transformation based upon the combination of breakthrough technologies and new concepts has given its true momentum to RMA. It is now possible to generate, share, exploit huge amount of data which opens the way to global information dissemination and better informed, machine assisted, accelerated decision process. The efficiency of this operational digital transformation relies on capacity to build adaptive and secured command and control networks able to answer to operational environments' diversity, ensure the suitable connectivity between all participants, and deliver relevant information to selected participants at the right time. This opens the way to optimizing the contribution of every single battlefield actor, be it land, see, air, space or cyber combatant, remotely controlled systems, autonomous vehicles and a multitude of sensors… This should ultimately allow to select in near real time the most suitable combination of military kinetic or non-kinetic effects to achieve operational aim. This is the essence of the collaborative combat concept, which should enable the building of multinational coalitions based on the combination of genuine digital interoperability and maximum flexibility. Developing collaborative combat requires a deep transformation of development, acquisition, upgrading, modernization, and support processes. It also relies on promoting collaborative innovation involving operational end users and industry to integrate new digital technologies while keeping a constant operational focus.

This first contribution is part of a "Vauban papers" series aiming at sharing best practices on operational digital transformation through a multidomain, multinational, public and private collaboration.

General (Rtd)

Jean-Paul Paloméros

Former NATO Supreme Allied Commander Transformation (SACT) and Senior Advisor at Avisa Partners

DATA: THE CORE OF COLLABORATIVE COMBAT

The past decade has seen a return of power politics and inter-state competition, and the resurgence of the potential for major armed conflicts. In this context, the challenge for armed forces is to secure operational superiority with more efficient use of human and material resources, with reduced numbers and shorter reaction times. In contested physical, cyber and electromagnetic environments, commanders must have accurate, up-to-date, reliable situational assessments, shareable in near-real time with all the players concerned. Only then is it possible for commanders to adapt their means in the shortest possible time with maximum efficiency.

The digital transformation of civil society and armed forces is a key component of this efficiency. It can provide armed forces with the flexibility, reactivity and manoeuvrability necessary to the concentration of efforts and efficient decision-making. Digital technologies (Internet of Things, Augmented Intelligence, Cloud, etc.) make it possible to conceive a "collaborative" mode of combat and gain the upper hand over the adversary.

The digital transformation of Armed Forces: a new deal for collaborative combat

Forces' ability to act collectively and in coordination has always been a foundation of armies' superiority over their adversaries. This efficiency is based on communication between the different levels of command and the combination of different effects. The digitisation of armed forces enables the optimisation of manoeuvres using near-real-time sharing of information and the networking of all players on the battlefield, both horizontally (tactical level) and vertically (strategic level).

This increased connectivity has two direct impacts on the conduct of operations:

- Faster feedback between the tactical and strategic levels
- Increased knowledge and understanding of the battlefield to reduce the "fog of war".

These elements can contribute to operational superiority through:

- Detection and almost instantaneous anticipation of the adversary's manoeuvres, through feedback from technical and human sensors
- More informed and precise decision-making through a shared assessment and a near-real-time update of the situation
- Accelerated concentration and de-concentration of forces through improved sharing of the situation and immediate transmission of orders in the command systems
- Better synchronisation of effects, for instance of firepower (e.g., missile fire, artillery) according to evolution on the battlefield.

Far from departing from the principle of concentration of effort, i.e., striking an opponent's weak points as hard as possible, collaborative combat in its digitised version enables greater speed of manoeuvre and a tenfold impact. Moreover, collaborative combat can be leveraged in joint and multidomain warfare (air, land, sea, space and cyber).

Data and network, vital organs of collaborative combat

While digitisation undeniably contributes to the fluidity of operations, it depends on two essential factors: the existence and availability of data, and the network capacity to deliver it.

> DATA COLLECTION AND PROCESSING

In a military context, data refers to all the factual information which can be collected in the field using human and technical sensors. The 21st century digitisation of platforms and equipment has led to an increase in the number of sensors and, as a result, to an exponential increase in the amount of data generated.

To turn this data into an operational advantage rather than cognitive overload, it must be given meaning and become useful to the different levels of the chain of command. Collaborative combat therefore requires efficient and secure IT infrastructures to process this data and use it to derive elements to contribute to improved situational assessment

> NETWORKS: THE CORNERSTONE OF COLLABORATIVE COMBAT

Data must thus be exchanged among the field and command centres to become valuable and usable. Data sent up from the field allows commanders to better assess the situation, decide on the most appropriate course of action and manoeuvre accordingly. Powerful, secure and resilient networks are therefore an essential precondition to the contribution of digital transformation to armed forces' operational superiority.

The critical nature of operational networks places electronic warfare and cyber defence at the very heart of the collaborative combat challenge: to keep control of one's network while being in a position to neutralise the adversary's to induce paralysis.

Stakes and challenges of collaborative combat

Digital technologies follow rapid innovation cycles. The digital transformation of armed forces thus requires constant (r)evolution. The challenges posed are technical as well as human.

> TECHNICAL CHALLENGES

- Classify and disseminate processed data according to their relevance to each echelon (right and need to know)
- Increase connectivity and interoperability of the different tools and information systems, and make them resistant to operational conditions
- Develop simple and clear digital interfaces to prevent information overload and cognitive paralysis.

> OPERATIONAL CHALLENGES

- Adapt command systems to the faster pace of operations
- Prepare armed forces for combat in degraded mode, i.e. the ability to pursue operations when information systems are damaged or unusable, whether for intentional (e.g., cyberattacks) or unintentional (e.g. loss of network) reasons.

> HUMAN CHALLENGES

- Prevent the paralysis of decision-making due to information overload
- Maintain the principle of subsidiarity in a complex information space
- Understand that digitalisation can support decision-making but must remains subordinate to human command.

AUTHORS

Axel Dyèvre, *Partner, Avisa Partners*

Séverin Schnepp, *then Consultant, Avisa Partners*

DATA: THE CORE OF COLLABORATIVE COMBAT

The issue of command in the digital age was already on the programme at the Ecole de Guerre (military academy) in the 2000s. French land forces are now engaged in its concrete implementation.

Battle are won in the field and through intelligence. They begin with competition, continue in confrontation and are exacerbated in combat. Battles are fought and won in the narrative, initiative, flow, integration and insertion, legality and legitimacy. Information and data are at the heart of these tactical, operational and strategic dilemmas.

Adversaries focus their intelligence on locating command posts (CP). The CP can be technically neutralised as early as the competition phase, psychologically inhibited by hybrid actions during the confrontation phase and physically destroyed in less than 72 hours in combat. The main purpose of a command post is to enable operational commanders to make the right decision at the right time. It is structured in a way to reduce its footprint on the ground and to psychologically dominate the opponent. New forms of conflict require us to reduce the CP's vulnerabilities and to optimise the benefits and potential of new technologies to create the conditions for physical victory.

The Rapid Reaction Corps - France (RRC-FR) is conducting research into a new concept for a level 1 CP to meet these challenges. The objective is to make the decision-making process more agile and organise the CP cells accordingly. The challenge is to maintain command continuity while reducing the operational functions of the area of action. CPs must allow Armed Forces to conduct field operations both in the front and rear depths of a contested environment in all domains.

Communication and Information System (CIS) capabilities have a direct impact on the organisation and functioning of the CP. Mastering digital technologies and artificial intelligence enables timely decisions by capturing the right information. It is key to leverage existing CIS resources while taking technological progress into account, to be realistic while remaining cautious with required resources. In addition, the electronic, electromagnetic and cyber environment is both constrained and contested.

The CP must thus have a reliable and ergonomic Operational Communication and Information Systems to guarantee the necessary flows of data for planning and conduct, for its networks to be resilient to attacks, to be interoperable, in particular with Allies, and to increase its reactivity by using technical tools for decision support and data exploitation.

These are the necessary conditions to allow command to maintain superiority of execution by imposing its own rhythm and manoeuvre without allowing adversaries any respite.

AUTHOR

Lieutenant General

Pierre Gillet

Commander of the Rapid Reaction Corps - France (RRC-FR)

DATA: THE CORE OF COLLABORATIVE COMBAT

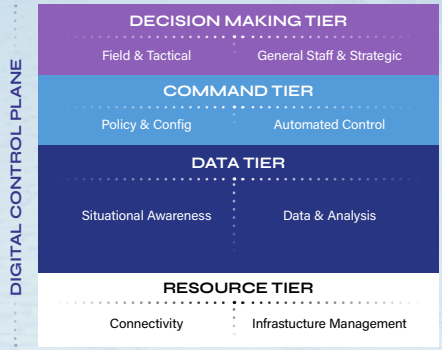
VMware Research envisions an organization fully able to reflect and realize its intent in collaborative combat. We contemplate a structured-control architecture, which we will refer to as the Military Digital Control Plane (MDCP), which consists of a hierarchial series of tiers that enable scale, capacity and performance within their particular discipline, whilst allowing a more intuitive and informative interface with users. Organizations will be better able to realize mission outcomes through controlled creation, consumption and exploitation of data that flows, much like the central nervous system of our bodies.

For reference, consider global-scale telecommunications networks that are increasingly deployed with software, rather than hardware. Within software-defined networking, there is the concept of the data plane and the control plane. Across the data plane, business and mission data courses through the "pipes" of the organization. The control plane itself configures those "pipes," their capabilities, the policies that govern where and how they flow. By separating the control plane from the data plane, network architects have been able to achieve high scale and throughput, while also having better methods to rationalize, secure and adapt the network.

Inspired by the utility of this concept, we propose the further separation of concerns through the MDCP construct. We envision a series of four domain tiers: Resource; Data; Command; and Decision Making. We extend the concept of the network control plane to be data smart and aware, enabling and managing the flow of data and intelligence through the organization and across the tiers. In turn, there are controllable mission verticals within each tier which support the functions and concerns of various stakeholders. There is massive innovation in the data space, and indeed all of the tiers. The MDCP concept calls for the separation of concerns, allowing the tiers to evolve separately and rapidly, whilst maintaining an ability for connection and collaboration across and through them.

While this is a series of abstractions, we remain grounded in reality because of the interrelation and hierarchical nature of the tiers, where the necessary and appropriate context is surfaced by the Digital Control Plane from each tier to the tier above, and across mission verticals in order to promote contextual insight, management and control.

The detailed purpose and operations of each tier will be described in future papers. Let us initially define the Resource Tier as a rough approximation of today's hybrid cloud environment with connectivity to and through the edge, orchestrating across diverse infrastructure pools of compute and sensors. With this in place, the organization can develop the Data Tier, drawing on massive commercial innovations that continue to revolutionize the way organizations exploit data to differentiate from their competitors. Too often today, even agile multi-cloud operations are hampered by the inertial gravity of data. With a true Data Tier, the data would also be virtualized, and able to flow in controlled form with smart AI-enabled orchestration on the underlying tiers based on predicted use, mission requirements, and technical considerations such as communications limitations of endpoints. The Command Tier consists of increasingly virtualized orchestration of enterprise digital activity, ranging from abstracted business operations to policy-driven security and data access controls, all enabled by increasingly ML-automated updates from the Data Tier.



Ultimately, the Resource, Data and Command Tiers all support optimal decision making for the fundamental C2 mission of any military organization. As C2 has evolved, bolting on scope and hardwired functions, it has bloated to C4ISR and beyond, frustrating the core desire for Command and Control. The MDCP approach instead provides a powerfully virtualized Decision Making Tier to consume the output of the Data Tier's dynamic analytics and situational awareness, presenting it to tactical commanders and strategic decision makers through modern user-focused/role-focused applications. With rich data flowing through the MDCP, they can receive timely and actionable intelligence and also drive their intent and response back down through the complex system, which reacts accordingly. We believe that this separation of concerns with intelligent coupling will speed innovation and empower the commanders of the future with greater insight and utility, even as the digital environment gets more complex.

The ultimate goal of the Digital Control Plane is to maximize scale and performance at each tier through specialization and rapid innovation, while allowing massive-scale configuration and management through more declarative means. We consider the concept of coordinated, increasingly abstracted Tiers introduced here to be an important next wave in the industrialization of Information Technology. VMware Research is actively working on declarative computing interfaces, inspired by Kubernetes and related virtualization techniques that should allow us in coming years to prototype higher-utility systems with better human/machine-teaming interfaces with the ultimate goal of making data the vibrant core of any enterprise.

AUTHORS

David Tennenhouse

Then Chief Research Officer, VMware

Robert Ames

Senior Director, Emerging Technology, VMware

Lewis Shepherd

Senior Director, Research & Emerging Technologies Strategy, VMware

VAUBAN SESSIONS

VAUBAN PAPERS

#2 DATA FOR TACTICAL COMBAT: OPPORTUNITIES AND CHALLENGES

avisa partners vmware

WWW.VAUBAN-SESSIONS.ORG

FOREWORD

The digital transformation of Armed forces has impacted key roles in the operational command and control chain and increasingly at the tactical level, down to the combatant across fighting spaces, land, sea, air, space, cyberspace or information domain.

The digitalising of weapons systems has long been a tool for innovation and modernisation of military operational capabilities. It has brought about outstanding progress by dramatically increasing armed forces' connectivity, real time tactical situational awareness, target identification, extreme precision of smart weapons, or miniaturisation of operational sub-systems. Integration efforts have leveraged the benefit of state of art digitalisation technologies and increased operational efficiency across the entire operational spectrum. And yet, lessons learned from a broad range of military operations and exercises have shone a light on key limits and constraints of operational digital transformation. For any military operation, communication networks' capacity, ensured continuity, or reliability are paramount. They often demonstrate disturbing limits however, while the need for increasing information exchange has never been so pressing. While the civilian world is seeing a constant modernisation of communication tools and networks supported by an ongoing revolution of information technologies, in the military, keeping the pace represents a major challenge. Military operational digital transformation must take into account some key military requirements such as rusticity, cybersecurity, as well as the crucial national and interallied interoperability factor.

Operational digital transformation is reaching a major step with the emergence of data as an essential ingredient of knowledge, of power, as the engine for innovation, as a precious good to be capitalised upon, to be fully exploited and shared.

This second "Vauban Paper" aims to share thoughts and best practices on how best to operationalise a fully data-centric transformation at the tactical level of operations. It identifies the benefits of being able to access and exploit gigantic data flows generated by combatants, and by a multitude of sensors and weapons systems. Among the many breakthrough technologies which underpin this tactical digital transformation, attention must focus on the growing potential of edge computing which should enable, among others, the full exploitation of a new generation of smart sensors at the combatant level.

Operationalising a new data-centric approach at the tactical level is certainly is both a major challenge and opportunity, and could well prove to be a game changer. It will require addressing and overcoming potential shortcomings such as data dependency, reliability, or cybersecurity to name but a few. This is the price to pay to ensure that digital transformation brings about a crucial contribution to collaborative combat.

General (Rtd)

Jean-Paul Paloméros

Former NATO Supreme Allied Commander Transformation (SACT) and Senior Advisor at Avisa Partners

DATA FOR TACTICAL COMBAT: OPPORTUNITIES AND CHALLENGES

Collaborative combat relies on the continuous, near real-time sharing of data collected on the battlefield. Once processed, the chain of command can use the data to benefit from a complete view of the operational situation, enabling the various command levels to take decisions with the best possible level of information. In this "digital bubble", the sensors carried by deployed forces play a decisive role in feeding Communication and Informations Systems (CIS). In return, deployed forces[1] can rely on regular updates of the operational situation to facilitate and optimise the conduct of their missions.

The upsides of new technologies in operation are obvious (e.g. detection of adversaries and/or neutralisation of their capabilities). But forces deployed on the ground must still respect the fundamental operational requirements of adaptability, agility and resilience. The geophysical environment as well as adversaries' actions can indeed prevent or limit the use of these technologies. Forces must therefore be prepared to maintain their operational capabilities in degraded conditions or in a contested environment.

Data at the service of tactical units

The continuous update of the Local Operational Picture (LOP) and Common Operational Picture (COP) facilitates the planning and collaborative conduct of operations. The aim is to generate the most accurate and complete view of the operational situation, by identifying both friendly (*Blue Force Tracking*) and enemy (*Red Force Tracking*)[2] troop positions. Sharing LOPs and COPs in near-real time presents a double advantage at the tactical level:

- Greater efficiency - speed and impact - in the planning and conduct of operations based on a more rapidly and accurately updated situation.
- Greater safety in the conduct of operations with improved understanding of threats and risks.

A direct consequence of the faster update of the friend or foe situation is the significant acceleration of the pace of operations.

Supporting and protecting deployed forces: a dual requirement of connectivity & cybersecurity

Digital transformation yields undeniable operational benefits to armed forces. The multiplication of communications and the increase of exchanged data flows nevertheless introduce risks which, while not new, are considerably strengthened:

- Increased dependence on the electromagnetic spectrum to ensure the connectivity of assets, while natural conditions may block or limit the use of these waves.
- Increased surface exposure to enemy electronic warfare action domain and cyber attacks which can damage, corrupt or expose data and information systems.

Thus, while armed forces must have the capabilities for collaborative combat to gain the upper hand, they must also be able to fight in a degraded and/or contested environment without putting their operational effectiveness at risk. The terrain, electronic warfare actions[3], or the destruction of critical network components by enemy fire, may all deprive units of communications. Enemy actions in the cyber field can also affect protocols, system layers or the data itself. In all cases, the availability, completeness and integrity of the data exchanged may be compromised. Capabilities must therefore be sized according to these new challenges, and doctrines of use and training adapted to prepare troops on the ground to face said challenges.

Although the civilian sector faces very different challenges, some of its solutions can be adapted and hardened for military use. Armed forces can in particular leverage the progress made in the field of edge computing, which consists in collecting and processing data locally, as

1. On deployed troops, vehicles and drones.

2. To locate for instance command posts, logistic infrastructure, forces concentration and main crossing points.

3. Such as jamming radio waves through which communications and data are carried.

close as possible to the user, by integrating processing capabilities (embedded intelligence)[4] into edge devices. In this decentralised approach to data management, edge computing must be developed along with a genuine military "Internet of Things" (IoT). In practice, this would mean that individual and collective equipment have their own storage and computing capacities to function autonomously, no matter the circumstances. The benefits of edge computing for military organisations are threefold[5]:

- **Reduced volume of exchanges and reduced exposure to latency:** as not all data is sent back to a central server. Moreover, local processing speeds up the availability of results.

- **Strengthening data cybersecurity:** the decentralised nature of edge computing makes it more difficult to neutralise all the edge devices simultaneously (unlike a server[6]). But for hackers, edge computing means increasing the number of available entry points, requiring a high level of cybersecurity on all devices[7]. In the event that a virus infects part of the network, it is possible to introduce security protocols to isolate the compromised parts (segmentation) and prevent the virus from spreading to other devices. The risk of capture by the enemy of the connected means also reinforces the need for authentication and maximum local encryption of data.

- **Flexibility and modularity in data management:** by combining edge & cloud computing, armed forces can allocate available resources according to their needs, extending collection and computation capabilities. In order to make the most of this "tactical cloud" combining the advantages of the cloud and the flexibility of edge computing, armed forces must develop efficient data management. This means defining which data should always be available locally, which should be exchanged and at what pace, bearing in mind that requirements may change according to the phase of engagement and the conditions.

From an operational perspective, the use of edge computing for tactical units allows for:

- Greater mobility, as troops are less dependent on the network.

- Increased stealth of movement combined with a reduced level of communication and data exchange.

- Greater speed in mission execution, with local data processing.

- Greater flexibility with faster reconfiguration of devices, and less reliance on centralised instances.

PROJECT LELANTOS[8]
DEVELOPMENT OF A MOBILE TACTICAL HEADQUARTER

The digitalisation of the battlefield requires a more mobile tactical headquarter (HQ) to reduce the risk of being detected. Against this background, project Lelantos[9] led by NATO's Allied Rapid Reaction Corps (ARRC) has proven being particularly innovative regarding the agility brought to the ARRC's tactical HQ (ARRC TAC). The ARRC TAC consists of a Mobile Expandable Container Configuration (MECC) that is transported on a truck so that it can be moved quickly as operations and posture change. This flexible and modular command centre can be deployed very quickly and with little personnel, and contribute to the safety of operations as well as the survivability of the equipped HQ.

4. Edge computing can be seen as the opposite of cloud computing, where data is transferred and processed on a remote server - requiring a reliable and uninterrupted network to enable the flow of data.

5. *" The benefits, potential and future of edge computing"*, VxChange, 29/04/2021, URL

6. In particular, DDoS or "distributed denial of service" attacks, which aim to make a server, a service or an infrastructure unavailable by saturating the server's bandwidth or exhausting the machine's system resources . See *"Qu'est-ce que l'anti-DDoS"*, OVH, URL

7. In this case, the weakest link in the cyber chain determines the resilience of the whole architecture.

8. *"Corps innovation: exponentially increasing survivability, command and control"*, NATO, 14/12/2020, URL

9. *"Innovating, Ready for the Future"*, Allied Rapid Reaction Corps, 01/12/2021, URL

Preparing troops for the digital battlefield

To ensure the benefits of digital transformation outweigh the risks and challenges it poses, it is crucial for the armed forces to provide appropriate responses to several issues.

> TECHNICAL CHALLENGES

- Developing devices with on-board intelligence to optimise data flows, while taking into account the technical constraints of size and weight, energy consumption, thermal signature, and heat dissipation.
- Strengthening the security and cybersecurity of equipment to ensure that it remains safe for troops in the event of loss or capture by the enemy. Security protocols can, for example, cause logical or physical destruction of the compromised device or system, or alter accessible data for the purpose of intoxicating the enemy.
- Ensuring the continuity of the infrastructure: if a network brick is no longer functional, the network architecture must minimise dependence on critical nodes and provide the best guarantee of high service availability at all times.
- Controlling the traceability of supply chains to monitor the cyber security of sensitive equipment and technological components (cybersecurity by design).

> OPERATIONAL CHALLENGES

- Maintaining a high level of stealth: the electronic equipment of tactical units must minimise their acoustic, electromagnetic and thermal signatures to prevent detection by the adversary.
- Possessing the means to neutralise, compromise and intercept enemy CIS: tactical units must be supported by offensive electronic and cyber warfare capabilities to reduce or eliminate adversary operational capabilities.
- Preparing to fight in degraded mode or in a contested electromagnetic and cyber environment: armed forces must be able to pursue their operations and carry out their mission. It implies that they train both in degraded conditions, and for the optimal use of collaborative combat systems.

> HUMAN CHALLENGES

- Developing ergonomic and easy-to-read interfaces: irrespectively of their level in the chain of command, troops must use equipment which reduce their cognitive load. Equipment must deliver the information transmitted instinctively, requiring neither reflection nor analysis, as the soldier's attention must remain focused on the environment and the conduct of the mission.
- Develop software components within CIS to faster identify anomalies resulting from human or technical errors in the data collected (e.g. incorrect GPS readings or erroneous reports) and propose solutions to reduce the risks associated with erroneous data.

AUTHORS

Axel Dyèvre, *Partner, Avisa Partners*

Séverin Schnepp, *then Consultant, Avisa Partners*

DATA WARS

THOUGHTS ON THE IMPACT OF DIGITAL TRANSFORMATION ON ARMED FORCES AND THE CONDUCT OF OPERATIONS

In September 1915 the British Army suffered more than 50,000 combat deaths at the Battle of Loos. In the same month the world's first tank rolled off the production line in England. Few at the time would have anticipated the transformational impact of Armour on the conduct of warfare, although it was demonstrable by 1918 and the Battle of Cambrai and has been a predominating feature of conventional war ever since. Armour was a paradigm shift in Industrial Age warfare.

Self-evidently the world has changed in over a hundred years, but that rate of change is now on an exponential curve, as we move out of the foothills and onto the massif of the data-age. It is axiomatic that defence must now undergo a new paradigm shift of a magnitude as great-as if not greater than that made by "Little Willy" and its armoured successors from 1915 onwards. Four key areas worthy of thought: the impact of digitization on the conduct of war; on our people; on our structures; and on "peace".

Digital Warfare

The advent of a 'new' domain in Cyber is one facet of a digital transformation but it is not the whole. Artificial Intelligence divides opinion ~ some fear it, whereas others are very willing to divest authority from human to machine. Either way, AI will become a central factor in warfare and those forces that embrace this change most readily are likely to have an advantage in the future. Artificial Intelligence is a means by which we may accelerate the tempo of warfare; applying action at scale or by means that outstrip the adversary's ability to respond (on preferential terms). Warfare will remain a fundamentally simple concept —in which the importance of holding the initiative remains a central tenet of victory— but the interactions between opposing states and their militaries will become increasingly complex and, beyond the whit of man alone. The ability to acquire, process, understand and act upon data —observable factors across physical and virtual environments— will be stretched by the complexity of contemporary warfare, unless we embrace the processing power of modern computers. Speaking as an armoured officer, this is not about abandoning the reassuring authority of hardware, but about understanding the interplay between "sensors and shooters" — in which digitization serves as a new form of delegated authority designed to expedite effective decision making and bring capability to bear at a speed that outstrip the opponent. There is software, pioneered by an increasingly technical military industrial base that can acquire, track, and interdict tactical threats without human in-put. However, one senses that the aiming mark must be a world in which commanders can employ data in order to seize the advantage —in which strategic calculations and variables, such as where the schwerpunkt may lie in the enemy's defence— emanate from split-second computer calculations. Commander's art —Lawrence's "Kingfisher moment"— being the guts to take risks or decisive actions where human judgements trump computer algorithms: to deceive, feint, exploit, consolidate, etc.

Empowering people and driving efficiencies

Don't fear obsolescence. Warfare will remain a fundamentally human endeavour. However, as commanders it is important to note the often-quoted statistic about the civilian job market: ninety percent of the vocations that today's school children will do, have not yet been invented. Setting aside some of the hubris in this statement, we must anticipate and be agile to the fact that technology will change the face of defence. Machines will do jobs that humans presently do; but is that not an opportunity to re-employ our people in new ways? It would be presumptive to say exactly how, but one could envisage that in Krulaks "Three Block Warfare" analogy that we might see more machines at the harder edge of warfighting with AI driven sensors and shooters engaged in a Deep stand-off battle; and more of the force focused on critical peace-enforcement and stabilization efforts short of combat. Victory being harder to maintain than win.

Structural shifts

Together with the impact on people is the impact on structures. We shall need to be equally agile in how we allow our structures to flex to the opportunities of digitization, rather than bending digitization into the current ORBAT. It being a folly to have software that is restricted by the conventions of an anachronistic force laydown. We shall need to identify the common denominators that straddle the old and the new, and then identify how those denominators come together to form future structures. Our understanding of "componency", "jointery", and the echelons of war will be as much about programming as it will be about C2 organograms. One school of thought being that the aiming mark for a genuinely effective sensor-to-shooter kill chain is an agnostic system of systems: where hierarchy is less about a linear process and more about pre-defined conditionality — think freedom to fire in the rural as opposed to constraints in the urban and how programming might define the "rules" and criteria for deployed forces.

"Peace"

In an economic sense, data is now one of our most traded "commodities". Meta-data providing banks, insurance companies, businesses and governments with an edge for their core decision making. Such is the value of data, that it is now the subject of competition between States: who can acquire it, and who can influence it — as we have seen in the debate that has taken place over the accesses of Chinese telecommunications companies around the provision of 5G technology. One suspects that "peace", between competitors, will take on a new facet with an indefinite 'shaping' period prior to an undefined crisis. A period in which one must collect and store data against an adversary in order to pre-load information advantage for the opening phases of a heightened crisis or conflict. As the saying goes, you get out of AI what you put in, and so we will see an increasing focus on building data-banks prior to conflict, as part of a broader endeavour to assure or deny a first-mover advantage. This will ultimately have a profound shift on what constitutes competition, crisis and deterrence; an impact that will straddle the levels of war and provoke some introspection on the theories that have defined our western approach to warfare since the Treaty of Westphalia.

These are interesting and exciting times. We would be wise to remember that those who doubted the value of "iron horses" ultimately came to rely upon them!

AUTHOR

Lieutenant General

Sir Edward Smyth-Osbourne KCVO CBE

Then Commander of the Allied Rapid Reaction Corps (ARRC)

DATA FOR TACTICAL COMBAT: OPPORTUNITIES AND CHALLENGES

In the inaugural paper in this series[10], we introduced the concept of the Military Digital Control Plane. As a a structured-control architecture, it consists of a hierarchical series of tiers that enable scale, capacity and performance within their particular discipline, whilst allowing a more intuitive and informative interface with users. This paper concentrates on the most important Data Tier, as well as some elements from the Command Tier, and the Digital Control Plane, all concepts that address challenges and opportunities of data at the tactical level.

We will assume that the organisation has a fully functional Resource Tier, with ubiquitous connectivity, and dynamic resource allocation that is effectively managed globally. Those elements are fundamental elements along the journey to well-managed Digital Transformation. With these in place, a powerful Data Tier that flexes and adapts to the needs of the organisation is now conceivable. This Data Tier will be unencumbered by physical boundaries and will enable the smart flow of data around the organisation, from sensors, through analytics, to databases to application and users – and back. Much as our blood flows through our bodies, the organisation of the future's data will flow as needed to the right place at the right time, guided by the brain – in this case, the Command Tier, informing and informed by the Decision-Making Tier. This flow will carefully reflect the intent and policies of the organisation as expressed through the Command Tier, in close coordination with the Digital Control Plane, which interfaces with each tier to manage and assess its configuration, activities, and status.

We have stated that today, Data has deep inertial forces, often requiring the organisation to optimise applications around its immovability. Applying the concept of a Data Tier to the issue at hand, Data at The Tactical Edge, we can envision sensors deployed at the edge, collecting anything from RF data to full motion video and beyond. The Resource Tier will support the sensor itself, configuring its connectivity and security, and allocating the appropriate resources to support the ingest of data, and the in-line analytics that it will perform. In the event that it is to receive a pre-built model, that will be deployed to the sensor as needed. The data generated by the sensor can be analysed in real-time, tagged and packaged as necessary for the needs of the organisation.

What are the advantages of this approach compared to today? With the powerful Data Tier, the environment can be aware of and adapt to real-world limitations dynamically. If that sensor is deployed on a marine vessel with limited connectivity, the model can make use of local cache, be more selective, or have a deeper understanding of the bandwidth patterns that are observed on the vessel and carefully sync communications with any optimal scenarios that arise. With a fully functional Data Tier, the users need not bother interfacing directly at this level. Instead, in concert with the Resource Tier, the Data Tier uses Machine Learning and Artificial Intelligence to benefit from comprehensive awareness of available resources, and of the demands and intent of the modern organisation.

The collected data now simply flows throughout the organisation as necessary. Indeed the system, benefitting from the separation of concerns across the tiers, is able to scale dynamically well beyond today's limits, because of the benefits of rapid innovation and industrialisation at each Tier. The system also has a better understanding of itself than any human could, but it is still subject to human

10. Vauban Paper #1, Data at the core of collaborative combat

intent and will as expressed through the Command Tier and Digital Control Plane. The tiers work in concert and coordination to realise the goals and requirements of Tasking, Collection, Processing, Exploitation and Dissemination and thereby to realise the desired outcomes, adjusting to abnormalities or perturbations and the changing realities of every day.

The digital revolution is continuing apace, and with it continuing apprehension that capacities, performance and requirements grow exponentially without any sign of limitation. Amid the noise, there hasn't been enough focus on the groundbreaking concept of data becoming less inertial and more kinetic. VMware Research believes that through the separation of concerns at the tiers, with appropriate command and control constructs to unite them, a transformational Data Tier will can be realised, changing the paradigms of data that we struggle with today.

AUTHORS

David Tennenhouse

Then Chief Research Officer, VMware

Robert Ames

Senior Director, Emerging Technology, VMware

Lewis Shepherd

Senior Director, Research & Emerging Technologies Strategy, VMware

VAUBAN SESSIONS

VAUBAN PAPERS

#3 DATA AT THE SERVICE OF C2

avisa partners

vmware

WWW.VAUBAN-SESSIONS.ORG

FOREWORD

DATA INTEGRATION:

A POWERFUL LEVERAGE FOR TRANSFORMING OPERATIONAL COMMAND AND CONTROL, A KEY TECHNICAL-OPERATIONAL CHALLENGE, A NEW APPROACH TO MEETING OPERATIONAL NEEDS.

The question of how to integrate a multitude of diverse data collected by multiple human and technical sensors is not new. Until recently, a typical answer has been to create numerous specific chains dedicated to sorting, assessing, deciphering, and merging operational data in operational Command and Control (C2) organisations to advise military authorities.

In the process, commanders have been confronted with a clear dilemma: on the one hand, they can push for the systematic exploitation of the huge intelligence potential of an exponentially growing mass of data. One the other, they may prefer to rely on their own operational experience, on their own assessment and on their own selection of information, at the risk of ignoring weak but essential signals. The outcome of the information battle depends on this choice. This major operational challenge for national armed forces and multinational organisations (NATO, EU, coalitions…) calls for a structured, concerted yet urgent answer, combining end-users' expertise with the adoption of the most advanced digital technology.

To be clear, this does not mean superposing the former and the latter, but rather the integration of both. The ability to achieve this synergy is at the core of a true digital transformation for modern armed forces, starting with their C2 structures and systems. Since the end of the Cold War, C2 capabilities have dramatically evolved to cope with very dynamic operational environments and face a wide spectrum of threats, both in the traditional domains (Land, Sea, Air) and in space, cyberspace and, increasingly, in the informational sphere. At the command level, integrating these different domains, assessing related threats, and synergising the most appropriate actions represent the new operational paradigm.

In the face of this profound transformation, the traditional approach to "Command and Control" and ways of expressing and meeting operational needs are no longer relevant. As a matter of fact, today and even more so tomorrow, the modern C2 should allow the centralisation, organisation, and smart employment of vast amounts of diverse data for a better control of operations in real time, and the conduct of fruitful ex-post analysis. Here, the exploitation of Big Data should improve commanders' situational awareness and assessment of the best course of action, and their ability to learn from potential mistakes. It should in turn lead to swift and effective planning adaptations through improved prioritisation of efforts and more accurate identification of adversaries' centres of gravity. Achieving this level of reactivity, agility and efficiency, while guaranteeing security and resilience, requires that new C2 systems be designed to provide a high level of flexibility to adapt to the evolutions of operational needs (and not the opposite!) and conceiving their security and resilience by design.

Emerging digital technologies have the potential to meet this challenge, provided that new C2 systems, including embedded AI engines, are conceived by integrated teams including end-users and industry working in full synergy.

This is one aim of this third chapter of our "Vauban Papers": to promote joint team efforts focused on operational aims, ability to test, experiment and develop adapted, agile, reliable solutions open to interoperability with current and future C2 systems.

General (Rtd)

Jean-Paul Paloméros

Former NATO Supreme Allied Commander Transformation (SACT) and Senior Advisor at Avisa Partners

Command and Control (C2) structures are central to the planning and conduct of military operations. Their effectiveness depends on the continuous exchange of information among the various levels of the chain of command. Digital transformation has over the past 20 years opened new perspectives for C2, based on the collection, valorisation and dissemination of information. The combination of forces' hyper connectivity and computers' increased computing and processing power (such as Cloud Computing) has indeed made it possible to accelerate and enrich the planning and conduct of operations, increase operational situational awareness and improve threat detection. The use of digital technologies should also theoretically discharge the cognitive load of personnel and decision-makers, so they can shift their attention towards essential activities. But while the digital transformation of the command post (CP) generates new possibilities, it brings with it technical, operational and human challenges.

Digitisation of C2 structures : knowing faster and better

CPs must, in order to function, have an updated vision of the operational situation based on information received from the battlefield. From there, the military commander can plan and conduct the action, issue orders to the various levels of the chain of command, and anticipate opponents' possible actions.

Digital transformation can greatly increase PCs' planning and conduct capabilities. On the one hand, the multiplication of onboard sensors deployed on the battlefield of operations - combined with the development of ever more efficient transmission networks (in terms of bandwidth and latency) - provides an ever more accurate vision of the reality on the ground and enables a truly collaborative combat. Near-real-time information allows headquarters to better anticipate threats and monitor the evolution of operations, allowing the commander to count on a greater reactivity of forces.

On the other hand, the computing and processing power of today's information systems (whether embedded in platforms and sensors, or in PCs) can also be used to calculate scenarios in near-real time and thus improve leaders' decision-making capacity by presenting a more exhaustive list of possible options and their consequences. The use of algorithmic computation not only accelerates and facilitates the sorting of collected data, but also reduces the impact of human cognitive bias in this analysis and projection phase.

Technical challenges of the digital CP

To take advantage of digital transformation, C2 structures must cope with challenges inherent to data processing. In short, the issue is not just about having more information, at the risk of rendering decision-making impossible[11], but about having better information. In this regard, data collection and processing are crucial steps within the CP because they can influence the leader's decision making. Armies need efficient IT infrastructure and architecture capable of turning large volumes of data into usable information in a limited amount of time to maintain the operational advantage of near real-time information. These same infrastructure must be equipped with a high-level of cybersecurity to protect them for enemy actions.

Three other technical challenges mut be taken into account:

- **Dependency on networks:** temporary or continuous unavailability of network, resulting from a dysfunction or enemy action, preventing any upward or downward communication with the different levels of the chain of command.
- **Interoperability of systems:** this is crucial in contemporary operations that are often conducted in the framework of a coalition, with Allies being sometimes equipped with very different systems.
- **Technological sovereignty:** C2 structures are critical to the conduct of operations, thus require technical and logistical self-sufficiency and the establishment of relationships of trust with the manufacturers who supply them.

Stealth and survivability of the CP

CPs remain priority targets, considering that their neutralisation reduces the operational efficiency of the

11. The risk of « infobesity » is indeed to paralyze the decision-making process in waiting for the next information to have a perfect situation awareness, thus delaying always more the decision.

deployed force. With digital transformation, the multiplication of data flows leads to an increase in transmissions, with a greater electromagnetic signature. The challenge for the opponent therefore is to identify the source of these exchanges in order to neutralise it as fast as possible.

To reduce the risks of detection, modern CPs must therefore be designed to increase their agility, whether physical (mobility) or technical (electromagnetic stealth). Several options are thus available to decision-makers:

- **Resilience:** for instance by burying PCs underground to make them more resistant to direct hits.
- **Mobility:** it is possible to increase unpredictability by being in continuous motion, whether on land or in the air.
- **Stealth:** which can also take the form of decoys and operations to deceive the enemy (fake CP, generation of false electromagnetic signals).

Tomorrow's C2 structures

While the CP's missions remain unchanged[12], their exposure to attack is increasing in the current geostrategic context: whereas in the past, obstacles to the conduct of operations were natural (distance, terrain), it is now able to create them artificially (e.g. jamming, taking control of information systems). The return of high-intensity conflicts indeed increases the spectrum of threats to C2 structures: air warfare, electronic warfare, ballistic missiles, cruise missiles, etc.

In June 2020 in his *« Vision Stratégique 2030 »* for the French Army, the Chief of Staff of the Land Forces, Lieutenant General Thierry Burkhard, now Chief of Staff of the French Forces (since July 2021), highlighted that *« tomorrow's conflicts will combine combat actions, information warfare, cyber actions and economic retaliation. These actions will be conducted in a synchronized, brutal or insidious manner (…) a high-intensity conflict between States is therefore once again possible in all fields of confrontation »*[13].

These new risks and threats must therefore be taken into account in the design and implementation of C2 structures, while continuing to increase their capacities. The future CP will therefore need to take into account the following characteristics:

- **Modularity:** geographical splitting of the CP (distribution in several places) at different distances from the frontline.
- **Technology:** optimisation of data management to increase the quality of information and orders transmitted to the commander, improvement of interoperability (ability to connect different systems).
- **Mobility:** rapid deployment and disassembly of the PC to facilitate relocation operations, requiring a minimum footprint for the least amount of personnel, and the shortest possible operational implementation time, requiring the use of appropriate technologies.
- **Stealth:** reducing the electromagnetic signature, energy consumption and thermal footprint to reduce the risk of detection and resulting vulnerability to strikes.
- **Resilience:** taking into account the return of threats related to high-intensity combat (electronic and cyber warfare, long-distance combat, air strikes, special forces…) by including several levels of physical and cyber protection.

AUTHORS

Axel Dyèvre, *Partner, Avisa Partners*

Séverin Schnepp, *then Consultant, Avisa Partners*

12. (1) Process and synthesis information from data streams collected on the battlefield ; (2) General a global and systematic view of the operational situation ; (3) Distribute and relay information and orders between the different operations in the command chain.

13. « Supériorité opérationnelle 2030 : vision stratégique du chef d'état-major de l'armée de Terre », 08/07/2020,, URL

CHALLENGES AND OPPORTUNITIES OF DATA AT C2 LEVEL

The digital transformation of Command Posts implies that Command and Control (C2) function is improved through flexible and adaptable systems, the evolution of the doctrine and Emerging Disruptive Technologies[14] such as Artificial Intelligence (AI), Machine Learning (ML) and Quantum Computing. Technological advancements in communications and networks have shifted. The commercial sector is developing the most advanced capabilities at an increasingly faster rate. Governments and their military forces are struggling to adapt their acquisition policies to take advantage of technological changes.

Digitalisation can bolster NATO's ability to gather and process information, take decisions and automate routinised processes. Maintaining the tempo of digital transformation of C2 systems is crucial, as it allows to gain and maintain a technological edge over adversaries. It also presents a number of challenges and opportunities:

- The networks essential to enable communications and real time Situational Awareness will require Artificial Intelligence (AI) remediation algorithms to continue to operate effectively against degradation, failure and hostile actions. In particular, there is a need for a great degree of resiliency and adaptation in the way to deploy. Conventional and innovative (i.e. cyber) weapons lethality implies respectively the need to minimise physical presence on the ground and to enhance the redundancy of C2 systems, by means of modular and scalable C2 systems distributed into multiple Command Element and nodes geographically dispersed.

- Future Multi Domain Operations battlefield will be populated by a myriad of sensors and requiring huge bandwidth to allow the timely exploitation of the information gathered. Data compression software is essential and AI is critical to face information overflow. Information Retrieval (IR) and Big Data methods can be used to analyse huge quantities of data, facilitating a more efficient processing for assessment purposes. The use of IR and big data techniques could be greatly beneficial in delivering the right information to the appropriate level.

- AI and Machine Learning (ML) can help harness the big amount of data that floods into C2 systems while they are processing information to build an exhaustive operational picture. They can improve decision making and support C2 function. ML allows to possibly establishing data models with specific instructions for performing a task. ML algorithms basic risks may include amplification of human bias, accidentally revealing private/secret information, feeding false/malicious data. AI can assist operations assessment process by supporting the staff to analyse trends and predict scenario possibilities and developments.

- Quantum Computing advancements would allow CP C2 systems to improve resiliency via communication encryption methods. Quantum computers use the unique properties of atoms and photons to solve complex mathematical equations faster than traditional computers can. This "quantum supremacy" would enable users of quantum computers to quickly transmit and process secure data between sensors and C2 Systems through the Internet of Military Things (IoMT), offering near impenetrable encryption.

Digitalisation is key to NATO's proficiency across emerging technologies. Embracing digitalisation enables NATO to maintain its core competencies

14. Technologies that should reach maturity level in the next twenty years

required for collective defence, cooperative security and crisis management, while enhancing its ability to anticipate non-military threats and opportunities and interaction/cooperation with stakeholders. Digitalisation requires a data factory consisting of robust data pipelines, algorithm development centres, associated workflows and storage facilities that work together seamlessly across the Alliance. Storing, sharing and processing huge quantities of data in real time require an enterprise-wide approach that connects to the Internet on trusted 5G networks. From a technological point of view the operational requirement is to implement an IoMT in combination with a C2 capability managed by AI which can support commanders. The main challenges required for the implementation of this system are represented by the availability of data and interoperability of systems provided by public and military multi-sensors platforms as well as the complexity of cryptographic algorithms to be used.

AUTHOR

Lieutenant General

Guglielmo Luigi Miglietta

Commander of NATO Rapid Deployable Corps - Italy (NRDC-ITA)

DATA AT OPERATIONAL LEVEL

In our previous two papers[15], we introduced the vision of the Military Digital Control Plane (MDCP) and the logical hierarchical tiers of architecture. We expanded on the concept of the modern Data Tier as a concept enabled by this architecture that features a separation of concerns across the tiers, with smart coupling and orchestration that affects the intent and will of the organisation from strategic decision making, through operational action. In this paper, the focus will be on the operational features and considerations of the MDCP.

Recall our analogy where data flows around the organisation as our blood flows throughout our bodies enabled by the Data Tier. If the Data Tier is the blood of the system, the Command Tier and the Digital Control Plane are akin to the brain and the central nervous system respectively. Collectively, these tiers focus on reflecting and enacting the needs, intent, policies and rules of the organisation in partnership with the Data and Resource Tiers.

The principal purpose of the Command Tier is as an interface to the human users and consumers of the system. For decades, there has been a significant gap between the realm of computer science and communication styles and languages of humans who use the systems. In order for the intent of the organisation to be reflected in the system, deep expertise was needed to "translate" these needs into system and security configurations, application designs, policy enforcement regimes and so on. In reality, those translations often missed the mark, witness countless failed projects. With the advent of massive scale architecture, and Kubernetes, there has been important innovation in more declarative means of system configuration. With this, the application developer is not prescribing specific numbers of systems, availability regions, or other details. Rather, they tell the system what features their application needs, such as availability, scale, load balancing and firewalls, and the system, which has a better understanding of its physical realities, provisions the resources appropriately. As the needs flex, the system adjusts accordingly, both scaling up, and scaling down, which has been difficult previously. This concept is also reflected somewhat with Software Defined Networking and Software Defined WANs, which allow the enterprise to configure, connect and secure according to function, rather than the brittle IP source, destination and port rules that often confounded network architects and were frequently woefully behind the actual deployed reality.

If we extend the concept of a declarative systems interface and management, then we can anticipate that the Command Tier will offer allow the organisation and its commanders to clearly outline its priorities, understand and rationalise its resources and maximise their utility to support mission. The information and intelligence required for effective decision making will flow through the organisation and its applications to inform and enlighten commanders. Further, the Command Tier will provide effective and intuitive interfaces to declare, enforce and audit policies, whether they be security, information sharing, or even the lawful and predictable understood use of Artificial Intelligence, and/or weapons systems. With a robust and well instrumented and automated Data Tier, there can also be careful enforcement of the data flows throughout the organisation, and that data can be well understood, compliant to the international standards of the day, and accurately reflect and enforce the current privacy regimes.

Returning to our analogy, the equivalent of our central nervous system in this architecture is the Digital Control Plane. In effect, it logically runs throughout the tiers of the organisation, much as our spinal cord runs from the brain stem down through our vital organs and connecting through nerves to our extremities. In this digital realm, the Digital Control plane enacts the commands throughout the architecture, creating flows, connecting new regions, healing failed, and removing obsolete ones.

15. See Vauban Paper #1 « Data: the core of collaborative combat » and Vauban Paper #2 « Data for tactical combat: opportunities and challenges ».

Much like our immune system, it will react autonomously (according to the rules of the organisation) to deal with viral attacks or other anomalies. With its connectivity throughout the system, it has comprehensive ability to act, to react and to inform the Command Tier for further input and guidance.

VMware Research sees massive utility and promise in the concept of the MDCP. There are often biological inspirations to system design as our bodies are a true system of systems with effective command, control, messaging and response. Through the separation of concerns proposed with the MDCP, true focus and innovation can be applied within that domain, whilst ensuring connection, interoperability and relevance through effective use of standards. The beauty of virtualising and abstracting, which has been the core of VMware's existence, is that the limitations of physicality are overcome, yielding to the power of resource pooling, scale and vastly more effective configuration and management of complex systems. A successful organisation of the future will exploit concepts such as outlined here to operate within the OODA loops of its competitors through pervasive and effective operational management supported by something like the MDCP.

AUTHORS

Robert Ames

Senior Director, Emerging Technology, VMware

Lewis Shepherd

Senior Director, Research & Emerging Technologies Strategy, VMware

VAUBAN SESSIONS

VAUBAN PAPERS

#4 AUGMENTED C2: COMBINING THE ART OF COMMAND WITH NEW TECHNOLOGIES

avisa partners

vmware

WWW.VAUBAN-SESSIONS.ORG

FOREWORD

OPERATIONAL DIGITAL TRANSFORMATION , THE WAY AHEAD

Digital transformation in defence represents both a way to improve the planning, control and execution of military operations and a powerful leverage to prepare armed forces to face new geostrategic challenges, emerging risks and resulting threats.

The three previous "Vauban Papers" have highlighted the current state of play of digital transformation, its benefits and limitations for the combatant and most recently its major impacts on the art of command.

These food for thought papers have been fuelled by "Vauban Sessions" organised under the auspices of the French Rapid Reaction Corps. A clear outcome of these reflections was how the success of operational digital transformation relies on a dynamic combination of factors, namely human skills, new digital technologies and the involvement of industry. For maximum benefits, this joint endeavour must be supported by a sound dual track approach. First, a continuing reflection on new operating concepts (multi domain combat, agile command posts, sharing of responsibilities between operational and tactical command, combat clouds development…). Second, as Artificial Intelligence (AI) capabilities evolve, the benefits and limitations of the automation of command and control functions and processes must constantly be assessed.

A first conclusion is that operationalising digital transformation calls for an innovative, collaborative, cross functional effort. This should yield a new incremental approach, centred on operational users' requirements, moving beyond traditional and lengthy capability development processes.

The aim is the early integration of the latest digital technologies on the market, together with the inception of new systems, supported by a dynamic demonstration and development process. Operational users, supported by industry experts, must be able to test and refine new concepts, imagine innovative solutions, and take back control of the development, uses and evolutions of operational systems. To be clear, this is not about armed forces taking charge of the entire information systems conception, development, exploitation and maintenance cycle. This is not their job, acknowledge even by the US's powerful armed forces, as well as the British. Both have decided to build the success of their digital transformation on co-innovation and cooperation with industry. To achieve that goal, it is paramount to identify the indispensable skills that armed forces must develop and retain in order to understand the added value of new technologies, to develop their operational requirements accordingly, drive needed adaptations and ensure the highest level of cybersecurity. Maintaining interoperability between different information systems, be it for national, NATO or international coalitions, represents a key challenge which must be addressed as early as the conception phase. Most advanced technologies such as virtualisation cast a new light on interoperability, much more dynamically than in the past. It is now possible to create different spheres of information confidentiality and sharing according to national policies (strictly national, open to NATO, open to coalitions partners…) in near real time. In the end, the will and ability of different actors to cooperate is key to the success of an operationally driven digital transformation. To promote such an open approach of digital transformation, this 4th Vauban Paper addresses the potential and limitations of AI systems in supporting operational command.

General (Rtd)

Jean-Paul Paloméros

Former NATO Supreme Allied Commander Transformation (SACT) and Senior Advisor at Avisa Partners

AUGMENTED C2: COMBINING THE ART OF COMMAND WITH NEW TECHNOLOGIES

Previous publications in this series have highlighted the technical, operational and human challenges and opportunities created by Armed Forces' digital transformation. The last chapter of this series intends to continue the line of thought by focusing on a strategic question: how to combine the very human art of command with the use of new technologies in a sustainable and relevant manner?

Digital transformation is having a significant impact on the conduct of military operations. Continuous increases in computing power; increased miniaturisation and energy efficiency; software performance; reduced latency and increasing speed of the networks on which information flows: the amount of data collected in the field is expanding as well as its transmission speed and usability within C2 structures is accelerating. This combination of factors can, among other things, improve the coordination of forces in the field in real time.

From now on, the use of technologies to enhance and process the data collected makes it possible to envisage an interactive and collaborative combat between the various parties and the multiple platforms that now act within a multi-domain operational environment. This broader information control is now a prerequisite for ensuring the necessary reactivity and manoeuvrability to maintain the operational superiority of forces facing both asymmetric threats and the return of high-intensity conflict.

The 'near-real time' dimension: a new paradigm for C2

Digital transformation offers numerous advantages for C2 structures. It allows for the acceleration and automation of certain tasks, such as the gathering of information from the field, the processing of this data, the visualisation of the friend/foe situation, the anticipation of possible scenarios supported by probability calculations. Military commander thus have not only a near-real-time view of the operational situation, but also elements to reflect on possible scenarios and projections at their fingertips.

To understand the impact of digital transformation on C2 structures, a parallel can be drawn with the evolution of the GPS, including in its commercial, civilian use. The idea is not to compare what is not comparable, but to trace the "digital transformation" of the "mapping" and "navigation" functions in the civilian domain, to illustrate the progressive stages of this evolution. Even if we tend to forget it, the civilian GPS - like many digital devices and services - has undergone evolutions that have led to complete changes in hardware and usage over nearly 30 years, punctuated by 4 different generations of terminal types:

- **Early 90s:** First generation of terminals with LCD screens allowing the reception of coordinates and the transfer of the position on a paper map.
- **Late 90s - early 2000s:** Appearance of devices integrating digital cartography on which coordinates were transferred to a «static» digital cartographic terminal.
- **2000s:** Onboard GPS capability to calculate routes on guidance terminals, but with 'cold' or 'fixed' data (e.g. roads, types of transport used). The GPS was then able to calculate a route and provide additional information (e.g. distance, travel time).
- **Afer 2015:** With the widening use of the smartphone, mobile networks and new versions of signals of various positioning systems - GPS terminals can, in addition to the cold data they were already using, receive 'hot', 'evolutionary' data in real time (traffic, traffic jams, roadworks, weather, accidents, diversion). Fed in real time, they can constantly recalculate routes and propose a new route that is optimised or more adapted to drivers' specific needs (finding fuel, shopping, finding a restaurant).

All things being equal, since the early 1990s and the beginnings of onboard computing, C2 systems have followed an evolution comparable to the above-mentioned example. Whereas a few years ago, computerisation consisted of the parallel use of traditional means (paper maps, chain of command transmission frames) and computers, today, command posts simultaneously receive

and analyse cold data (main infrastructures, geographical features, weather forecast) and hot data (real-time meteorology, friend-or-foe position, command posts, relocatable infrastructure, logistic chains, regrouping of forces, crossing points) both in the planning and conduct of operations. The means of communication and transmission of orders as well as the analysis and visualisation tools are digitised. The onboard power of sensors and platforms makes it possible to provide information with increasing added value and therefore requires increasingly powerful means of operation to get the most out of it.

Placing the end user at the heart of transformation

Assuming that this data is properly secured and stored to prevent 'infoxication', it is easy to imagine that employed technologies will in the coming years be increasingly capable of suggesting action (or a series of choices) to the military leader based on the analysis of plausible or real scenarios (e.g.: lessons learned). But while the expression "artificial intelligence" carries approximations and a number of myths in its wake, it is important to know that even the most powerful computers cannot replace the art of command, which is based on training, practice and individual experience. As with any tool, these new possibilities, if used properly, can increase the speed and relevance of decisions taken, just as they can prove to be formidable cognitive traps. Not to mention the fact that for reasons both natural (terrain...) or resulting from attacks (electronic warfare, cyber...), data flows can be interrupted or corrupted. To use the GPS metaphor, just like reading a paper map, using a compass and a sextant will remain indispensable knowledge in the field, digitised C2s - and deployed units - must be able to function in degraded mode. And just as with a GPS, where the user's intuition and sensory knowledge can lead to a decision contrary to the recommendation, no digitised C2 system, no matter how powerful, will replace the leader's intelligence and ability to arbitrate in uncertain circumstances.

The art of command

In operations, command is performed in an evolving, unclear, pressing environment. Leaders cannot hope to base their decision on "perfect knowledge" of the situation. On the contrary, they must face an adversary who seeks to conceal their intentions, means and plans, but also confronted with natural parameters such as the weather, or human parameters such as the behaviour of populations. They must therefore take decision in a state of uncertainty, trying to dispel the so-called 'fog of war.' Military leaders must thus arbitrate between different hypotheses and scenarios and take decisions based on the information at their disposal (hot and cold data, enemy intentions) and on their experience and intelligence. It is within this framework that the various command support systems must be designed.

Human and augmented intelligence

The use of digital technologies aims to facilitate the data collection, processing and exploitation cycle. They are potentially valuable command support tools. Thus, artificial (or augmented) intelligence generated by algorithms can - if correctly configured and be fed with reliable data - reduce uncertainty and improve knowledge of the operational situation. However, AI cannot decide for its user. In order to better understand command in the digital age, it is necessary to distinguish two types of intelligence:

- **Human intelligence:** this refers to an individual's ability to understand, reflect, know, adapt their behaviour to a situation, and choose means of action according to the circumstances. This intelligence is materialised by cognitive capacities that allow the individual to create complex pathways and to include new variables that may guide decision making at any time.

- **Artificial or augmented intelligence:** Artificial or augmented intelligence: this is materialised by the speed of execution of certain tasks (sorting, calculation, identification, detection) and is based on a defined programme. At no point does digital intelligence take a "decision" in the cognitive sense of the term. It applies rules whose complexity and speed may give the illusion of reasoning, but which remain a logical sequence.

In practice, these two forms of intelligence do not compete, but rather complement each other: when relevant data is available, the computer will be faster than a human in

performing a computational task. If data is unavailable or unusable, only a human can decide by evaluating an uncertain situation and arbitrating between several hypotheses built on incomplete or unreliable data.

Command in the digital age

So-called "artificial intelligence" technologies can in no way replace the decision-making capacity of a military leader:

- Their knowledge of the environment and their functioning are limited by the quantity and quality of the data received. Thus, a variation in flows can distort the final result, while poor quality data will alter the level of granularity and relevance of the analysis. Command is based on the ability to take risks on the basis of incomplete or contradictory elements: by design, a computer can never respond to a need alone. Finally, as analysed in previous Vauban Papers, digital technologies suffer from hardware constraints, such as power consumption, heat dissipation and storage capacity. These limits are constantly being pushed back, but without reaching the optimal functioning of the human brain in terms of decision making. This has led a major researcher in the field, Luc Julia - creator of Siri and then VP of R&D at Samsung - to declare: *"The methods of these intelligences require a crazy amount of energy. It is an aberration. Knowing that with our 20 watts, we can talk, eat and do many other things. The machine only plays Go. So we can see that this 'artificial' intelligence has nothing to do with human intelligence".*

- AI technologies are unable to take into account variables exogenous to their code and do not have the five senses, which reduces their ability to accurately transcribe a complex situation. Humans can be non-linear in their reasoning, insofar as the sequence of their thinking is done via biochemical connections infinitely more complex than massive data processing. This enables them to adapt to changing situations, but also to be resilient in the face of adversity and contradictory injunctions. No computer would be able to say, as General Foch did in his message to the Grand Quartier Général (Joint Headquarters), during the first battle of the Marne in September 1914: *"My centre is giving way, my right is retreating, excellent situation, I'll attack."*

- Furthermore, unlike humans, computers do not have extrapolation or correlation capabilities. They do not have the general predisposition (knowledge) to generate complex paths, i.e. to put several actions together.

Command remains a human specificity and prerogative, i.e. an art in which military leaders must retain their autonomy of evaluation and decision. This is all the more true as the conduct of war remains a complex human act which no computer can grasp in its entirety through figures and algorithms.

To use the GPS analogy again, a driver may decide to ignore the information from his GPS, either because the information provided in his environment is not entirely accurate, or because his experience curve makes him think differently. Technologies are therefore not intended to arbitrate: they simply execute the planned programme and are thus neither more nor less than an aid to decision-making.

The challenge of combining the art of leadership with new technologies

Used in the framework of C2, AI can undeniably be an asset to the effectiveness and operational superiority of armed forces.

Continuous digitisation makes it possible to simplify the architecture of the systems used in the various C2 phases (anticipation, planning, conduct, analysis of ex post effects): «real time» data can become valuable input for feedback and the planning cycle. In the same way, the preliminary calculation elements of planning preparation can become elements contributing to the real-time conduct of operations if they are enriched by relevant and reliable data.

To be fully exploited, these technologies must be developed and integrated with operational needs in mind, but also be subject to a process of appropriation and acceptance by users. All too often, these developments are still presented as competitors or even as substitutes for human intelligence and decision-making capacity, whereas in reality they are only a tool to increase the

latter. It is in becoming "augmented intelligence", i.e. "human intelligence augmented by the machine", that so-called artificial intelligence technologies will become real decision support systems. This will also resolve the ethical and moral debates often associated with these issues: by putting the machine back in its rightful place as an automated system, albeit a highly evolved one, and which will always leave the intention and decision to its human user..

AUTHORS

Axel Dyèvre, *Partner, Avisa Partners*

Séverin Schnepp, *then Consultant, Avisa Partners*

Marie Ketterlin, *Analyst, Avisa Partners*

THE COMPLEXITY OF MDO COMMAND AND CONTROL

The increased pace of information sharing and associated sense-making is an ongoing struggle for NATO. This is not only expressed in publications but was confirmed during the 2020 NATO C2COE annual webinar in which the NATO C2COE addressed the complexity of Multi-Domain Operations Command and Control.

Mastering the complexity of information sharing within the decision-making process needs to be on the NATO war-fighting capabilities development agenda for the coming years.

Our key message during the 2022 edition of the Vauban Sessions was shaped by the outcomes of studies, observations, and events over the past years. Marcel Scherrenburg, our lead Subject Matter Expert on MDO, presented our thoughts on the increased pace of information sharing within the military decision-making process as topic-starter for discussion during these sessions.

We experienced that one of the biggest sources of confusion across the development of the multi-domain C2 concept is information management. Technology provides access to information and means to visualise data and will allow communication at decisive moments anywhere, and at any time. Nevertheless, the limited number of successful introductions of technological game-changers within NATO seems to indicate a disconnect.

The questions we presented to the Vauban Sessions' audience were: how can military commanders and staff cope with the increased pace of information sharing? Why is information sharing essential for the decision-making process? And: what is needed at the operational level to achieve cognitive superiority within decision making? Leading to the hardest question of all: how can NATO achieve this?

Observations from NATO exercises show that information management at the operational level headquarters is a recurring challenge. The headquarters were not fully prepared to absorb, filter, and distribute the abundance of data coming from the operational environment. In some cases, this inability to process all data led to undesirable exclusion of information resulting in inaccurate situational understanding and critical data left unused in a repository. This subsequently led to imperfect decisions.

Within the commander's decision-making process, connected events in multiple domains, vast amounts of data and a lack of clear cause-and-effect relationships, have led to a need to reconsider current information management to achieve cognitive superiority. In a future volatile, uncertain, ambiguous, and complex environment, existing skills and insights will not be sufficient to make well-founded decisions.

Achieving cognitive superiority or having a full comprehensive understanding of the operational environment is not about having more sensors or bigger datasets. True cognitive advantages arise during the sense-making stage. In this stage, data is projected into a specific context and mission framework. To achieve cognitive superiority, NATO requires several types of information sharing platforms which are fed by multiple sources, and which can implement and integrate several situational awareness and decision-making tools.

In the future, instead of employing more human resources and trying to accelerate the C2 cycle, Commanders will rely on decision-making support tools enabled by artificial intelligence and other emerging technologies. These tools are already widely available in the commercial sector.

They provide automated, predictive, and prescriptive analysis through real-time integration with streaming datasets. These emerging technologies could replace tiresome tasks for staff officers contributing to an enhanced situational understanding or even cognitive superiority. As a result, the situational understanding would be more comprehensive, thus resulting in better insights for assessing and developing options.

A system is needed for "information-on-demand," or, in the future, "situational understanding-on-demand" as available products to support the sense-making of the operational environment. Since military operations need to be robust by design, it is difficult to make disruptive change in routines. This should not hamper an introduction of innovative technology, but it is a reminder that change will start small and the proposed innovation should fit within the current mindset.

The introduction of new concepts should not fight existing routines but lower any acceptance barriers by proving the concept is robust and trustworthy. The amount of both friendly and adversary data, the speed of communications, the complexity of the operating environment, and the diversity of actors have all increased exponentially. Given the complexity of military operations, the joint Commander must be capable of focusing on reaching operational objectives and not on information that would distract from those goals.

NATO must embrace technology, learn, and adapt quickly to fully use the potential of the latest innovations. The alliance should strive for a common understanding and familiarity with intuitive technology, like the way we use our smartphones, for example. We therefore need a paradigm shift in NATO and its member states, to bridge the gap between developers and the end user in the NATO headquarters, as there is a fine line between repeating an ongoing promise and the successful introduction of technology.

By doing so, we can focus on what is important: using the agile C2 for effective, synchronised and well-informed decision-making processes. That said, it should go together with the human aspect as well: trust between people, understanding cultural differences and never forgetting teamwork. After all, we are part of one team, we are NATO.

To embrace information management as an enabler for military decision-making, NATO needs to evolve in technology, procedures and capabilities. The question that remains is: who is leading this?

We haven't (yet) untangled the complexity "knot" of information management at NATO, as this may be a complex problem which requires a collective endeavour beyond military capabilities. Problems like these require more than one solution and a comprehensive approach to develop multiple lines of effort to reduce complexity without oversimplifying the sense-making phase.

AUTHOR

Colonel

Mietta Groeneveld

NATO C2COE Director

LEVERAGING CIVILIAN TECHNOLOGIES IN THE DIGITAL TRANSFORMATION OF ARMED FORCES

I was privileged to attend the Vauban Sessions edition of 2022 and exchange with military representatives on how the Armed Forces can benefit from civilian technologies in their operational digital transformation. It came as no surprise to me that many of the conversations, challenges and innovations that are happening within the military - and at every level - are much the same as those in both the technology sector and in civilian life. Indeed, there is much we can learn from each other.

Exploit and capitalise on massive data volumes

At its most fundamental level, the nub of the issue is having the right data, in the hands of the right people at the right time. This is something consumers have become accustomed to with apps opening the door to everything from biometrics to banking. But the Armed forces cannot rely on a store where soldiers and divisions can pick and choose apps that suit. They need consistency, uniformity, and the adoption of technologies predicated on best-in-class Command and Control (C2). As a result, the focus for military leaders is the ability to harness the advanced AI and machine learning techniques available today to understand data, who needs it, when, and what decisions that information is going to facilitate.

As introduced in the previous Vauban Papers by both Robert Ames and Lewis Shepherd, senior directors, national IT strategy, VMware, the development of our Military Digital Control Plane (MDCP) is intended to solve this challenge. It is a modern architectural construct to inform and empower decision-makers. Capable of exploiting and capitalising on the massive data volumes that run throughout military organisations, it is also the foundation on which the latest and most cutting-edge developments in civilian technology can be incorporated to deliver enormous benefits to Armed Forces around the world.

Consumer technology for effective warfare

UA trait that embodies military organisations - and has done throughout history - is resiliency. Teams have to be able to adapt to changing situations. It means Armed Forces require fast and reliable delivery on fast and reliable systems capable of adapting to the unexpected or attack from adversaries. Consequently, this is challenging previously accepted norms. Only a few years back, organisational leaders wanted everything in the cloud but that's not how the world has developed. Instead of being in one place, the highly distributed nature of computing is putting data into the hands of users wherever they are. From cabs to cockpits or trains to tanks, data resides in all manner of places at a device level. C2 centres need the ability to capture it in real-time in order to remain one step ahead.

Networks and devices must also be deployed in a secure way. There is increasing talk within the technology industry around the challenges of trust and privacy. Not just about data being sovereign or being within a particular border, but the sovereignty of the platforms themselves and making sure that we're not beholden to other nations for their technology in order to compete, survive and keep running. It's a big focus for Europe at the moment with the Gaia-X project at the apex.

This is critical for military leaders where data compromise or network failure has the potential to be catastrophic. The combination of highly distributed networks, dispersed operational teams, and coordinated activities between nations mean security boundaries are no longer physical, but virtual. As a result, military organisations are often faced with the challenge of building new highly secure systems on top of old, insecure systems. Not only do they require the ability to do that with total trust but it has to be delivered rapidly. The speed of change means the Armed Forces cannot rely on systems that take weeks

or months to build. Instead, they need to very quickly turn consumer-grade equipment into an effective device for warfare.

"If it has been available since 1960, we run it"

Nothing evolves as quickly or as continuously as the technology sector. And for all the adoption of consumer technology in the Armed Forces to date, new trends, tools and techniques are continually emerging, of which the military needs to be aware. This is particularly the case with low and no code technologies - this is where individuals with limited or no coding skills can develop their own applications in ways that need no assistance from anyone else. A movement that has been coined, 'citizen development'.

Such a movement empowers innovation and situational adaptability and is ideally suited to the challenges the Armed forces face but needs to be done with a root of trust from the get-go. The soldiers of tomorrow, both on the ground and at a digital level, are coming from a very different generation from those that we have now. They'll be more hands-on with technology than ever before and will be expecting to be much more involved in situational application development.

Another area of focus for military leaders is how to fight the challenges of legacy - a problem not confined to the Armed Forces. One of my favorite stories is, 20 years ago, taking a young software salesperson to the UK MOD where he asked, 'what computer systems do you run here?'. The answer was, 'if it has been available since 1960, we still run it.' It's a perennial challenge both in civilian life and the military but, the only way you deal with legacy is by looking at things differently.

The genesis of Armed Forces

While there is much happening for military leaders to grapple with and understand, this story boils down to one key theme - change. There is much the military can learn from civilian technologies from; virtualisation, building on secure platforms, the speed of development and deployment, use and storage of data and so much more. But all of these are satellite issues to the main event which is, how well can you deal with and embrace change?

That is the defining trait of advanced operations and organisations today and, driven forward by developments at a civilian level, will be the genesis of digital armed Forces.

AUTHOR

Joe Baguley

Vice President & Chief Technology Officer EMEA, VMware

VAUBAN
SESSIONS

MORE INFORMATIONS ON:

WWW.VAUBAN-SESSIONS.ORG