VAUBAN SESSIONS

VAUBAN PAPERS

#2 DATA FOR TACTICAL COMBAT: OPPORTUNITIES AND CHALLENGES

avisa partners ceis vmware

WWW.VAUBAN-SESSIONS.ORG

THE VAUBAN PAPERS

COLLECTION

The Vauban Papers are a series of publications dedicated to the impact of digital transformation on the Armed Forces and the conduct of operations, published by CEIS in partnership with VMware.

The Papers are both the result and follow-up to the discussions held during the Vauban Sessions, an annual conference organised by CEIS and the Rapid Reaction Corps - France (CRR-FR) in Lille. The 2021 edition brought together some 120 participants and featured speakers from NATO, European Union institutions, national Armed Forces and defence industry from 23 Allied nations.

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

ABOUT CEIS

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

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

avisa partners ceis

ABOUT VMWARE

VMware software powers the world's complex digital infrastructure. The company's cloud, **app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device**. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact.

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

vmware

FOREWORD

GENERAL (RTD) JEAN-PAUL PALOMÉROS, SENIOR ADVISOR AT CEIS-AVISA PARTNERS

FRENCH AIRFORCE CHIEF OF STAFF (2009-2012)

NATO SUPREME ALLIED COMMANDER TRANSFORMATION (2012-2015)

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

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*

Séverin Schnepp, *Consultant*

CEIS-Avisa Partners

VAUBAN PAPERS #2

CONTRIBUTION OF LIEUTENANT GENERAL SIR EDWARD SMYTH-OSBOURNE KCVO CBE
COMMANDER OF THE ALLIED RAPID REACTIONS CORPS (ARRC)

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

Sir Edward Smyth-Osbourne KCVO CBE

Commander of the Allied Rapid Reactions Corps (ARRC)

VAUBAN PAPERS #2

CONTRIBUTION BY ROBERT AMES, LEWIS SHEPHERD,
DAVID TENNENHOUSE, VMWARE

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 intent

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

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

Chief Research Officer, VMware

Robert Ames

Senior Director, Emerging Technology, VMware

Lewis Shepherd

Senior Director, Research & Emerging Technologies Strategy, VMware

VMWare

VAUBAN
SESSIONS

MORE INFORMATIONS ON:

WWW.VAUBAN-SESSIONS.ORG