VAUBAN SESSIONS

VAUBAN PAPERS

#3 DATA AT THE SERVICE OF C2

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)

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

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 , 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 deployed force. With digital transformation, the multiplication

1. 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.

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 , 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 »*[3].

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*

Séverin Schnepp, *Consultant*

CEIS-Avisa Partners

2. (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.

3. « 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[4] 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.

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

Digitalisation is key to NATO's proficiency across emerging technologies. Embracing digitalisation enables NATO to maintain its core competencies 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, 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. Much like our immune system, it will react autonomously (according to the rules of the organisation) to deal with viral attacks

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

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

VMWare

VAUBAN
SESSIONS

MORE INFORMATIONS ON:

WWW.VAUBAN-SESSIONS.ORG