VAUBAN SESSIONS

VAUBAN PAPERS

#1 DATA: THE CORE OF COLLABORATIVE COMBAT

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)

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

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*

Séverin Schnepp, *Consultant*

CEIS-Avisa Partners

VAUBAN PAPERS #1

CONTRIBUTION OF LIEUTENANT GENERAL PIERRE GILLET
COMMANDER OF THE RAPID REACTION CORPS - FRANCE (RRC-FR)

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)

VAUBAN PAPERS #1

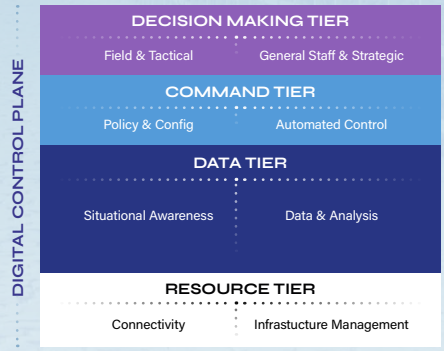
CONTRIBUTION OF DAVID TENNENHOUSE
CHIEF RESEARCH OFFICER, VMWARE

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

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