VAUBAN SESSIONS

VAUBAN PAPERS

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

avisa partners

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 Avisa Partners 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 Avisa Partners 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 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 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
FORMER NATO SUPREME ALLIED COMMANDER TRANSFORMATION (SACT)
AND SENIOR ADVISOR AT AVISA PARTNERS

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

VAUBAN PAPERS #4

CONTRIBUTION OF AXEL DYÈVRE, PARTNER & SÉVERIN SCHNEPP, CONSULTANT AT AVISA PARTNERS

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 &* **Séverin Schnepp,** *Consultant at Avisa Partners*

VAUBAN PAPERS #4

CONTRIBUTION OF THE NATO C2COE DIRECTOR,
COLONEL MIETTA GROENEVELD

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

VAUBAN PAPERS #4

JOE BAGULEY, VICE PRESIDENT & CHIEF TECHNOLOGY OFFICER EMEA

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

VAUBAN
SESSIONS

MORE INFORMATIONS ON:

WWW.VAUBAN-SESSIONS.ORG