NORTH ATLANTIC TREATY ORGANIZATION

SUPREME ALLIED COMMANDER
TRANSFORMATION

NATO Science and Technology Organisation conference Bordeaux:

“How will artificial intelligence and disruptive technologies transform military operations and organizations?”

31 May 2018

Général d’armée aérienne Denis MERCIER

Introduction:

- Very happy to be with you today.
- This conference organized by STO is an **excellent occasion to carry on the conversation** initiated last year, when ACT expressed its needs to STO in terms of big data and artificial intelligence to enhance military decision-making.
- This conference is exactly what STO and ACT had in mind when we signed our structured partnership in March, this year. This type of event is an encouraging first step in our ability to work closely together and connect ACT's work on warfare development with the latest technological evolutions studied by STO.
- **Before I get to our topic, I want to express my gratitude to several people and organizations, without which such an event would not have been possible:**
- First, the **Aquitaine Region and its president, Mr. Alain Rousse**t, who are welcoming us today.
- Second, my dear friends of the **Ecole Nationale Supérieure de Cognitique, Bernanrd Claverie and Hervé Le Guyader**, who initiated this conference.
- And of course, the **Information System Technology Panel and the STO executives, with the helping hand of Al Shaffer**, for their support in the preparation of this beautiful event.
- Thank you all. As I said, I am very happy to be with you today. And this being said, let us get back to our topic of interest.

- Today, I want to address the nature of the connections between disruptive technologies and the way militaries operate and prepare the future.
- But in order to frame the problem correctly, we must start from the strategic environment.

- Today’s strategic environment has gone from “**complicated**” to “**complex**”. It is the first element to analyse if we want to frame the problem correctly.
- **In a complicated world**, systems and situations can be processed and analysed, and upcoming events anticipated with a reasonable degree of certainty.
- **In a complex world**, there are so many interrelated variables that the evolution and consequences of any single event are impossible to predict. From a military point of view, this means a world in which surprise is now certain, failure always an option, and resilience a necessity.
- This complexity **applies to civilian and military organizations alike**.
- It will profoundly **transform both the organizations and their processes**, the way they operate.
- **One of the aspects of complexity is the increasing pace of technological disruptions** – presenting us with threats, but also with opportunities.
- **And the two key elements of technological disruptions are data and human capital.** They are also two of the most important strategic resources in our current environment.
- **We will focus today on data-centric and digital technologies, but there are much more disruptive technologies currently emerging** (hypersonic missiles, for example).

1) <u>The influence of a data-centric approach on military concepts</u>

- **Data is a strategic resource.**
- We need to reassess the way we integrate data in our processes, and evaluate how data – and AI, consequently – will transform the way we approach challenges.

- To illustrate this, I will use **some examples of a data-centric approach** to actual military issues. You will see that these issues apply to the civilian world as well.

a. *Strategic awareness and assessment of the information environment*

- The first topic I will cover is **strategic awareness and assessment of the information environment.**
- A global strategic awareness is essential for NATO – for every organization with a global reach, indeed. And it relies increasingly on massive amount of data, because in today's world, open source information is even more important than intelligence for decision-making.
- Today, algorithms are used in the civilian sector to predict and identify patterns of behaviour. Framed properly, they can also serve in the development of predictive tools as early warning signals.
- Google tried to do this in 2008 with their predictive model on flu outbreaks. While ultimately unsuccessful, this experience has provided researchers with useful lessons learned on the design of such algorithms – and their potential hubris.
- More recently, **one large aircraft manufacturing company had recurring problems with the engine of one of their aircraft**, and they could not figure out what the problem was, because they were focusing on the engine itself. They contracted a company to conduct a data analysis on the entire plane – which ultimately found that the issue came from a sensor in the tail of the aircraft. It was unnoticed because that sensor's variations were in the acceptable margins of error. But the connection was there.
- This example teaches us two things: first, **the importance of weak signals and of enlarging the frame of study** – hence the importance of global strategic awareness.
- Second, the use of big data to identify the problem. **The data was submitted by the companies operating the aircraft to a third-**

party contractor. If you imagine this example in a military setting at the scale of NATO, with data owned by the nations, it raises the questions of **data ownership and rules for sharing**. We'll get back to these topics of digital sovereignty in just a moment.

- In terms of military usage, a data-centric approach could be used for the **development of predictive tools to identify the early signs of a crisis**. More precisely, it can be used to detect trends and signals that may have no obvious link to our areas of interests, but when connected together, can inform us on a developing crisis. as well as detecting disinformation manoeuvres, to speed-up and enhance decision-making
- And consequently, the use of data can also **inform our strategic foresight documents** (future SFA) in a more comprehensive way. And we are already working on this approach in NATO.

b. ***Data-centric approach to operational concepts***

- **Data will also change the way our forces operate.** Let us take an example to see what these evolutions might look like with a simple case study.
- **Imagine a soldier, under enemy fire, calling his headquarters for support.**
- **Here is the sequence of events today:** the request is transmitted to a tactical operations centre which orders an artillery fire or a close air support mission, depending on availability. If the close air support option is chosen, a tactical air controller or a drone will guide the aircraft to strike the target in accordance with the rules of engagement, while integrating the risk for potential collateral damage, and also considering that all the actors involved can come from different nations.
- A first conclusion is that **data** (the call for support, the fire order) and **human capital** (all the actors involved) **are essential throughout**

the process. And most of the time there is a lawyer behind the screen (no one has all capacities…) It is a battle-proven system, but **conceptually outdated**.

- Updating the data transmission system is a first evolution, but the process remains centralized, in a point-to-point approach to decision-making.
- **What would an entirely digital approach look like?**
    - Here the same soldier sends his request for support and the system locates the request and automatically updates the operational environment. It processes the problem and analyses the soldier's ecosystem (other soldiers with their vehicles and weapons, intelligence sensors, aircraft, drones and even potential ships in the vicinity, etc.).
    - All these elements are interconnected within a common operational architecture. These assets then exchange data in order to process and validate the target, and offer engagement options associated with different levels of risk, taking into account the environment and the rules of engagement.
    - Once the target is approved, one of the assets assumes control over the others and proposes the best engagement option.
    - A human still decides (if this is our choice), but he or she is not necessarily located within the operations centre: depending on the operational architecture in place, this responsibility can be decentralized.
    - Any of these steps can be automated or not, depending on the rules of engagement, until the required effect is delivered: the support requested by the soldier.
    - It is not any longer a question of soldier, aircraft or command and control system, but **the service that must be delivered to the user drives the concept.**
- This **cloud approach** is not new in itself – but it would be revolutionary in a military environment where we are used to a very

vertical decision-making process, and where we centralize decisions and the control of forces.

- This approach, using new technologies, is based on data, managed with artificial intelligence but it entails a new concept that gives subordinate echelons decentralized control of capabilities.
- This is the biggest evolution: entrusting subordinates to take control of capacities that are not necessarily assigned to them, where **what is central is not the materiel but the service to be delivered, on time, and on target**
- It requires a significant change in the way we think of delivering effects, and **consequently in how we conceive our command and control architectures**.

c. ***<u>Capability development</u>***

- **Capability development has broad implications that go way beyond the sole development of a platform**, and in the digital age, data is a central part of it.
- To illustrate this fact, look at the **development of the driverless car in the civilian world:**
- The car itself is not the objective: it is a means to an end. The real goal is to bring a customer from a point to another, which requires to think about what new services and consumption models it might allow, such as the transition from an individual-property-based model to a shared, collaborative or on-demand use.
- **The performance of the vehicle itself is secondary to the notion of service.**
- It will require the **creation of an ecosystem** that associates traditional motor companies – the ones that actually build the car – with a broad network of start-ups and digital companies capable of developing the associated tools and services – geolocation, applications, personal services, environment management, e-trade, communication systems, etc. – as well as looking at human factors and legal aspects.

- Data in its broadest sense is at the core of the capacity, to allow safe navigation, but also to adapt the vehicle to the needs and habits of the users. The autonomous car will use data, but it will also create data.
- **The question is no longer “which vehicle?” but “what data, and for what use?”**
- **Which brings me back to military aspects of capability development.**
- To develop capabilities that are able to meet the challenges posed by technological evolutions, the **key issue is to raise the problem correctly.**
- In the complexity of our environment, the first obvious solution will most likely not deliver the right answer to our problems.
- **Let me illustrate this by an example, the successor of the AWACS capability for NATO.** The AWACS is this large aircraft with a radar mounted on top of it. The aircraft are set to retire by 2035, and the capability will be replaced by what we call the **Alliance Future Surveillance and Control (AFSC).**
- **The solution will not be another airplane with a new radar.** We have refused to go directly to what could have appeared as the obvious solution.
- We have first studied the problem and examined thoroughly the effects: **the key functions performed by an AWACS today are surveillance and control.**
- **Our starting point was the following question**: what will the future functions of surveillance and control look like in 2035?
- **As in many future capabilities, data is key.**
- In ACT’s view, supporting future functions of surveillance and control, requires the design of digital architectures that will allow to collect, to concentrate, to fuse and to re-distribute data to future users.
- **Data and human capital are the main strategic resources for the AFSC, and we need to define the right “human versus machine**

balance", and identify the level of autonomy that would be necessary and acceptable.

- But there are **other aspects to take into account** in terms of capability development.
- Obviously, when developing capabilities that generate and exchange data, **cyber protection must be integrated to the process from the onset**, and not as an afterthought.
- **Interoperability** – the ability of our forces to operate together and exchange information seamlessly – is also a critical aspect of future capabilities. This is why we are developing a system called **Federated Mission Networking** to allow the exchange of information between these different capabilities – think of it both as a standard of communication and as the federation of different networks to appear as one, allowing capabilities to exchange data.
- **Another aspect is data ownership and protection.** Capabilities in the Alliance are mostly owned by the nations. We are trying to identify solutions acceptable for our allied nations to share their data when it is relevant to the Alliance as a whole.
- **And finally, there are also ethical and legal considerations**, especially when we touch upon the subject of autonomous systems.
- **These legal considerations highlight the need to work with a wide variety of actors for these questions. Which brings me to my last point: the importance of human capital**

2) <u>The importance of human capital</u>

a. <u>Human resources challenges</u>

- It seems paradoxical, but, in the digital age, **human capital will be more essential than ever**.

- In the military, it will be essential to **attract, train, educate and retain** a human capital adapted to the functions we will have to perform.
- We will need **to educate leaders at all levels that are able to function in decentralized architectures**, which is a considerable cultural shift in the military. For example, a pilot in a modern aircraft (Rafale, or F35) can be used as a remote C2 centre. And in order to maximize the use of these systems, we must train our pilots in C2 management.
- We will also need **people that are both able to function in combat – in every domain – but also digitally "fluent"** to process future systems and operate in complex architectures.
- We will need **people capable of understanding and explaining** the recommendations provided by complex algorithms.
- These are daunting challenges, because they will require our military to rethink its understanding of what a soldier should be, in terms of physical and intellectual standards, to recruit people up to the missions.

Conclusion:

- The digital revolution will profoundly impact the way military and civilian organizations operate and organize.
- **This transformation will probably question our deepest-established convictions.**
- To illustrate this, there is an anecdote involving US Secretary of Defense, James Mattis, who also happen to be one of my predecessors as Supreme Allied Commander Transformation.
- He was interviewed during a trip about the nature of warfare a few months ago. And he answered that he had spent forty years in the Marines being absolutely convinced that the essence of war, its principles would never change. And yet, when envisioning the

developments of artificial intelligence, he said that he could not hold this opinion anymore. That we had to be open-minded about what may occur.

- **This open-mindedness to change is the first step to preparedness, and ultimately, to responsiveness.**
- In this regard, in a complex environment, it is important to remember that **no organization or nation holds alone every key to solve every crisis**. We need allies and partners, both inside and outside the defence sector.
- Because innovation is not just about the research and the technological evolutions. **We also need to be able to explain it, to present conclusions and recommendations to our political leadership – and this is where our ACT-STO partnership is especially important.**
- At a larger scale, we must **develop an ecosystem** built around 3 pillars: structures and institutions, human capital, and relationships.
- Finally, given the pace of technological change, we cannot address all the questions and solve every dilemma before launching projects and initiatives – **we must learn by doing**.
- **The technology already exists, let's use it!**
- Thank you for your attention. I will gladly answer your questions.