NORTH ATLANTIC TREATY ORGANIZATION

SUPREME ALLIED COMMANDER
TRANSFORMATION

French-American Foundation Conference on cyber issues

Opening remarks

25 October 2017

Général d’armée aérienne Denis MERCIER

Ladies and gentlemen,

It is a great honour and a personal pleasure for me to be among you today, and I thank the French-American foundation for its kind invitation. I will try, over the next fifteen minutes, to present the current cyber picture from the perspective of Allied Command Transformation, after which I will gladly open the floor to your questions.

In terms of cyber, as for almost everything else, a good place to start to understand the problem is our security environment. Today, this environment is characterized by **complexity** and **unpredictability.** Nations and international organizations like NATO are confronted with the **interrelation of crises and threats**, with hybrid challenges intermingling state and non-state actors, at a time when **technological evolutions happen at an increasing pace**.

The 2016 NATO **Warsaw Summit,** in the continuity of the 2014 Wales Summit, aimed at providing the Alliance with answers to these challenges. Among the outcomes was the **decision to recognise cyber as an operational domain.**

Cyberspace is now regarded as a potential area of confrontation – like land, sea, air and space – but moreover, it is a **cross-functional** domain. This decision will foster progress, as a honest self-assessment leads to the conclusion that cyber activities today are less understood, less mature and less resourced than other military tasks. We are late in the game. Our cyber adversaries have motivations, expectations and ambitions that are very different than those of our traditional adversaries. Old-style military thinking alone does not work well here.

Our cyber adversaries have little entry barriers and need little investment to engage in cyber hostilities against NATO and the nations. Usually, a small laptop and an internet connection is all they need to disrupt our activities. With just that, they can deny services, corrupt and exfiltrate information, defeat our intelligence and create adverse opinions against our forces and our actions.

To address this issue, our aim is not to create “cyber armies” to operate in this domain, but rather to **integrate cyber aspects into all the other domains in a multi-domain approach**. No operational domain is self-sufficient in today’s complex environment.

At the core of cyber is the **emergence of data** as one of the two main **strategic resources** of the 21st century, the other being human capital. As we are increasingly dependent on data, **one aim of cyberspace operations is to assess vulnerabilities, detect attacks, and protect the validity of data.** To illustrate this point, I will elaborate on cyber considerations at different levels.

At the **political and strategic level**, it is essential to **detect and assess cyber-attacks**, focusing on the **nature of the target,** the **potential effects** of the attack on the target, and, as much as we can, on **the attribution**, which comes from a permanent awareness and understanding of the environment.

We must approach cyber defence in terms of target vulnerabilities and effects on key infrastructure. I would like to stress that at the highest end of the spectrum, a cyber-attack could threaten our vital interests. This underlines the necessity to strengthen the resilience of our civilian and military networks, organizations and structures, and it clearly requires a whole-of-government approach.

At the operational and tactical level, cyberspace operations aim primarily at **ensuring the reliability of data**, because this **data informs our decision making process** and the **integrity and resilience of our C2 architectures**. This implies the ability to detect network intrusions or information alteration in a timely manner, and to assess the effects and vulnerabilities of operational networks.

As we develop offensive capabilities, we must also **improve our understanding** of the consequences of offensive cyber actions, especially in **defining the threshold of vital interests** that might be crossed by a cyber-attack. **Cyber-attacks**, when targeting critical military or civilian infrastructure, have the **potential to trigger escalation** in any crisis. And finally, we must **assess the vulnerability of our capabilities** in a broad sense, as was illustrated by the recent targeting of NATO soldiers' smartphones attributed to Russia.

To achieve these objectives, it is critical to **integrate cyber defence at the very first step of our capability development process**, in every operational domain, because **upcoming capabilities will be increasingly reliant on data.**

These are but a few aspects that we must consider in the development of our cyber strategy. I will now expand briefly on **four current areas that we identified as priorities**.

The first is plans and policy.

The **development of expertise**, collective understanding of cyber issues, and resilience across the Alliance, across our nations, and with the private sector is essential. Understanding and accepting our interdependency is a necessity, **because in cyber, the vulnerability of one can affect everybody else**.

Building **resilience** and **interconnectedness** has many practical aspects: the definition of a common terminology, the harmonization of processes, and the establishment of a common doctrine, to name a few.

Interoperability is a major challenge in a multinational environment, where we have to determine how we can build an organization based on the federation of different national capacities to achieve operational effects.

In addition, as cyber is an emerging domain, it does not possess a strong legal and ethical framework yet, unlike conventional warfare. Maybe we should consider the development of a “code of conduct” – especially in peacetime – drawing certain lines for every actor on what is and what is not tolerable.

The second area is capability development.

The defence community must be able to keep up with the pace of technological change, because cyber is a rapidly-evolving capability. To achieve this, we have to **redefine our relationship with industry** as a whole, and to include non-traditional defence companies from the digital sector, because **among these companies, some have outpaced the defence industry in terms of innovation**.

We also have to **rethink our capability development process**, in order to implement faster experimentation, development, and acquisition of cyber-related capabilities, on pace with technological breakthroughs. The future might include a two-sided process, with a **long cycle for platforms** (aircraft, ships, etc.) and a **shorter cycle for applications and services,** with cyber being an integral part of the **survivability** of our capacities. As such, ACT is working on smaller, more frequent capability packages, which are much faster to develop, approve, and implement. Our last cyber capability package took only six months to develop. This is the performance we are aiming at, even though six months is still too long in this area. We are also encouraging the employment of development contracts, where we share the risk with industry to adapt partially compliant solutions to NATO needs. This has already happened in the area of cryptographic procurement, and we aim to make it the standard for most cyber capabilities.

In relation to those capabilities, cyber operations require flexibility in profiles and skills that NATO Human Resources policies do not have yet. We are not able to hire and retain the right skill sets. Our capability packages take this fact into account, as we move towards outsourcing of expert-critical services.

The third area is education and training.

This is a domain where we do not train fast enough and need to explore new ways to create capacity across our nations.

Individual training aims at increasing our abilities to process cyber aspects in our daily missions, for example how to develop best practices in order to reduce vulnerability, and how to identify and react to the early signs of a potential cyber action. We will also integrate individual training in the tasks of the NATO Communication and Information Agency School that is moving from Italy to Portugal.

For collective training, we have developed virtual cyber training spaces and exercises, which allow us to recreate virtual network architectures and train them to resist and respond to cyber-attacks, without exposing our operational networks. We are developing a concept for distributed, federated cyber training that allows reusing most national resources to enable a dynamic, flexible and quickly reconfigurable training environment. We will also be relying on commercial training for a significant portion of our future needs.

Lastly, the fourth area I would like to mention is partnership and engagement.

Cyber partnership cannot be limited to nations and large-sized defence industry alone. Leading expertise will have to be obtained also from start-ups, small and medium companies, universities and even individuals. Some of those might dislike or cannot afford association with military organizations, but we still need their skills.

ACT is establishing partnerships and engagement with communities of interest to directly and indirectly pursue putting those skills to work with us.

Trust is a key element in cyber partnership. Trust cannot be achieved immediately after a crisis arises. ACT is developing the information sharing requirements and the supporting capabilities to create a persistent network of trust, to keep the Alliance on the forefront of detection, identification and counter-exploitation capabilities.

As part of the above, we believe we need to leave behind the old policy of hiding our vulnerabilities and being afraid to fail, with the aim to find solutions much faster than we currently do.

To conclude, before opening up to your questions, I would like to stress that cyber is a domain in which **we will have to assume an acceptable level of risk** in order to make progress. Across NATO, we need to study what a **federated approach** in cyber implies, in order to **leverage the capacity of our nations and our partners.** We also need to adapt our processes and policies to this new environment. There is much yet to achieve!

I thank you for your attention and will now gladly answer your questions.