NORTH ATLANTIC TREATY ORGANIZATION

SUPREME ALLIED COMMANDER
TRANSFORMATION

Debating Security Plus Conference opening statement

Online chat stream

27 September 2017

Général d'armée aérienne Denis MERCIER

The security environment today 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. In order to respond to these challenges, several decisions have been made during the 2016 NATO Summit in Warsaw. Among them, the definition of cyber as an operational domain stands out.

Cyber is now regarded as a potential area of confrontation – like land, sea, air and space – but it is also a cross-functional domain. Consequently, the aim is not to create “cyber armies” to operate in this domain, but rather to integrate cyber aspects in other areas of confrontation, and to draw the necessary conclusions on the way NATO operates.

We must reason in terms of desired effects – what we want to achieve in the cyber space. For every actor, but even more importantly for the defence community, cyber actions aim primarily at ensuring the reliability of data, because this data informs our decision making process. For example, it implies the ability to detect network intrusions or information alteration in a timely manner, among other aspects.

We must also integrate cyber issues from the very first step of our capability development process, in every operational domain.

NATO has already initiated several work strands to achieve these objectives, and much remains to be done, but I will expand briefly on three current priorities.

First, we are developing expertise, collective understanding of cyber issues, and resilience across the Alliance, across our nations, and with the private sector. Understanding and accepting our interdependency is a necessity, because in cyber, the vulnerability of one affects everybody else. Consequently, broad and resilient networks are more likely to be able to withstand attacks and intrusions. Building resilience and interconnectedness has many practical aspects: the definition of a common terminology, the harmonization of national processes, and the establishment of a common doctrine, to name a few. It is essential in a multinational environment, where nations provide the bulk of capabilities to the Alliance. Interoperability is a major challenge, because our national assets and forces must be able to communicate and understand each other.

Second, we are putting a strong emphasis on training, a domain in which much is yet to be invented. Training has individual aspects – for example, how do we develop our best practices in daily activities to reduce vulnerability – but also collective aspects. In this regard, 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.

Third, the defence community must be able to keep up with the pace of technological change, because cyber is a rapidly-evolving environment. To achieve this, we have to redefine our relationship with the industry as a whole, and to include non-traditional defence companies from the digital sector. 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. Reflexions are being conducted on these questions as well.

To conclude, before opening up to your questions, I will stress that cyber is a domain in which we will have to assume an acceptable risk in order to make progress – quite similarly to the early stages of aviation, a century ago. Across NATO, we need a federated approach in cyber to leverage the capacity of our nations and our partners.

I will now gladly answer your questions.