



NORTH ATLANTIC TREATY ORGANIZATION

**SUPREME ALLIED COMMANDER
TRANSFORMATION**

SACT's

State of the NIF

Brussels, 09 Nov 2016, 12.40 – 12.55 Hr

Final (as delivered)

Général d'armée aérienne Denis MERCIER

Ambassadors,

Excellencies,

Admirals,

Generals,

Ladies and Gentlemen,

Distinguished guests,

Thank you *Mr Huygelen, for your opening remarks on behalf of Minister Reynders*, we are very honoured by your presence among us today, and thank you for the outstanding support of the Belgian authorities and their staffs to help organize the NATO Industry Forum in such exceptional conditions.

The Egmont Palace is today's home of the Belgian Ministry of Foreign Affairs, it also has a rich history and witnessed many historical and other important events. It is certainly an inspiring location for this year's NATO Industry Forum.

At the Industry Forum this year we are honoured by the presence of so many distinguished guests. And I would like to add, in light of the US presidential elections results, and since my Command is the only NATO command located in the US, in Norfolk, VA, that I strongly believe in the strength of the transatlantic link. And this transatlantic link is, and I believe will remain, the foundation of our shared security, prosperity, and values.

The Forum takes place 4 months after the historical Warsaw Summit where adaptation and resilience were at the top of the agenda.

As we progress with NATO's adaptation, we scrutinize the future and make sure that **today's** political and military decisions, take into account the requirements of **tomorrow**. The capabilities we discuss today, have to meet the challenges posed by the future security environment.

But first let me invite you for a short journey in a not too distant future.

**** Illustrative Scenario****

In 2031, the Northwest Trade passage through the Arctic has opened, but one nation seeks to deny access to this route. This nation deploys naval vessels and a complex web of air and missile defence systems in international waters and the adjacent littorals. To complicate matters, the aggressor nation employs civilian fishing vessels, believed to be proxies, to harass shipping vessels. Then tragedy strikes, a NATO flagged frigate, collides with a civilian fishing vessel. The adversary launches limited conventional attacks using autonomous swarming drones. Supported by a large part of the international community, NATO formally invokes Article V (Collective Defence) and mobilizes, ***but an A2AD (Anti Access and Area Denial) network stands in the way.***

Due to the heavy cyber-attacks against NATO's land-based operational headquarters, airborne and maritime command and control assets assume decentralized, operational control of forces in a network that can be re-configured in

real time if necessary. NATO conducts multiple strikes against targets on the ground, in the air, in the sea, and cyber space as *integrated cross-domain operations*. Through a networked system of systems, the operation begins. Dynamically, forces share awareness, from the strategic to the tactical level, to create a common understanding and enable distribution of command and control. NATO operations are heavily supported by stand-off stratospheric drones and satellite communications.

Although many current systems – special forces, maritime forces, manned or unmanned air-assets - are on this battlefield, the difference is that they are networked into an integrated whole. By being able to decide and act faster than the adversary, manned and machined formations overwhelm it. Once the adversary's network of systems is disrupted and degraded, they are unable to achieve their strategic goals. *This entire battle from crisis to resolution has been faster than NATO has ever seen before.*

In light of such a fictitious scenario, I am sure that you all possess unchallenged expertise in one or more of the above mentioned domains. However, to achieve this level of ambition, it is clear to me that we must change our way of thinking.

You have probably noticed that I have purposely not mentioned specific platforms (aircraft , ships, missiles, tanks or others) – because we must no

longer think in terms of platforms dedicated to one specific and sometimes narrow oriented purpose. No single platform can counter on its own integrated systems.

What we have in mind and want to develop is a different approach aiming at thinking in terms of mobile ad-hoc networks (systems of systems), in which each element is able to sense, connect, process, make-sense and, eventually assist the commanders to decide and deliver the required effect.

You all have parts of that puzzle for this vision to materialize.

Today we can link very different platforms, in the civilian World, Apple Smartphones, android tablets or Windows computers – whether they are brand new or outdated – not directly to each other, but indirectly through the Internet to exchange huge amounts of data.

But we're still in the age of connected platforms in Defence – let's move to the 21st century!

The question is how to build a network of connected objects, able to collect and share data and to allow distribution of operational control, a network that will enable our forces to keep the edge now and in the future against any adversary in a complex environment, as was fictively presented in the scenario?

But first, we need to look at where we stand now, and what we need to do to prepare for this new and future operating-environment?

Last July, our heads of State and government met in Warsaw, at a defining moment for the Alliance, a moment when our security and our values face significant challenges.

Considering the recent evolution of the security environment in and around the Euro-Atlantic area, our political leaders took decisions to maintain our ability to tackle challenges and threats from a 360 degrees dimension, not only geographically speaking but also in terms of the wide range of actors and threats involved in potential crises.

These measures have two main objectives: strengthening our defence and deterrence posture and projecting stability across NATO's borders.

In this context, it is essential for the Alliance to keep its military edge through innovation with the aim to identify operational game changers and implement advanced and emerging new technologies applicable to the military domains.

This is why the relationship with Industries is essential to inform and to shape capability design. A more dynamic and open engagement with industries, including non-defence industries, will give us the prospective of the art-of-the-possible.

We must describe to the industries the problem we're trying to solve, for them to provide us with the potential solutions. I did not say solution! It is of course a two way street. We will inform industries of our analysis of the ever evolving future security environment in which we will conduct operations, and industries will inform us of the potential long term technological solutions they foresee to mitigate the shortfalls we have identified in terms of capability requirements.

We will need to weigh the options between “off the shelf capabilities” and “new capabilities development”. We need to switch from a “platform approach” to an “operational function approach”. All platforms, air assets, ships, missiles, and ground forces are to be considered as connected objects. The added value will not be in the platforms themselves, but in their built-in capacity to be connected – to fulfil an operational function.

This requires a change of mind set.

Systems engineering will be key in the development of any future capability.

A perfect example is the Alliance Future Surveillance and Control (AFSC) capability, aimed to replace AWACs in the +2035 timeframe. I won't develop now but we will be able to come back on this topic during the discussions.

Now that we have set the scene of what we need, and must do together, what have we already done to prepare for this?

This year was an unprecedented year for industry engagement, thanks to the strong impulse received at last year's industry forum. Allow me to mention 4 key initiatives on which we will keep building.

First, our common effort with the NATO industrial advisory group (NIAG) under the Conference of National Armaments Directors (CNAD). ACT and the NIAG are working on key areas, such as: Command and Control, Logistics and Sustainment, Capability shortfalls, Concept Development & Experimentation & Exercises.

We expect concrete recommendations on “global ubiquitous communications”, “federated resilience and cyber defence”, “artificial

intelligence” or “federation of clouds”. I want to take advantage of the participating industries present today to thank their leadership for their support to NATO through the NATO Industrial Advisory Group.

Another example is our annual Industry Involvement Initiative in Exercises (I3X) which was just completed last week. It involved 21 members of industry having a close look at NATO’s current challenges in Command and Control during the Trident Juncture Exercise (in Naples and Stavanger). We received very positive feedback from both industry and NATO participants and we will continue to work to improve I3X.

Another line of effort this year has been to better develop our outreach with industries across the Euro-Atlantic area, including new, non-traditional, and small or medium sized industries (SME).

That is why I extended the activity of ACT’s Office for Collaboration with Academia and Industry (OCAI) in Norfolk, with a permanent point of contact in Europe for greater reachability. Yet, together with my co-organizer Camille Grand, NATO Assistant Secretary General for Defence Investment, we decided to go even further and connect our Office for Collaboration with ACT in Norfolk, with a new footprint I want to set up in Brussels, together with the Defence Investment Division in the NATO Headquarters, and involving others such as the Science and Technology Organization, and the NATO agencies. We hope that structure will allow us to work better and communicate more coherently with industry.

At this year’s Chiefs of Transformation Conference (COTC) in Norfolk in December we will test the potential of new technologies (such as cognitive

computing) that will impact and in fact are already impacting defence capabilities.

The COTC allows us to engage more with small and medium businesses, and even beyond the traditional defence industry. ACT has set up an Innovation Hub in Norfolk – to enable free and unclassified exchanges on social networks and build strong communities of interest using online workshops.

In today's and tomorrow's efforts, NATO's relationship with industry will continue to play a key role on the road to transformation. A more dynamic and open engagement with industry, including non-defence related companies, will remain essential to encourage technical and procedural innovation. We need to continue on this path, reinforce and consolidate our cooperation – and making the tools necessary to offer quick practical solutions to new capability requirements.

I would like to stress again that **Industry** is **an essential partner to ensure the credibility of a posture today and tomorrow!**

Thank you for your attention.