

23th of January

MCCS Session 10

10H10-11H10

“SACT will give an update on Cyber in NDPP targets, in Education Training Exercise and Education, in Smart Defence projects, in NATO-UE coordination”

As we know, Cyber Defence is first and foremost a national responsibility, however NATO has an important role to play, primarily in protecting its own systems, but as well to facilitate and co-ordinate activities with Allies and I would stress, as well, the need for a close coordination with the EU Cyber Strategy.

Through the NATO Cyber Defence Action Plan, ACT's main focus is on ensuring that Education, Training and Exercises help to prepare Allies to face this threat and in promoting related multinational Smart Defence projects. We must also ensure that the Lessons Learned process is fully exploited and the good news is that we are making progress....

If I turn first to Education, Training and Exercises. The 2 Strategic Commanders have drafted the NATO Cyber Defence Training and Education Plan (also known as the Cyber Defence Strategic Training Plan) now with the MC for approval. We have already started integrating Cyber elements into our training and exercises, as was recently achieved in Steadfast Jazz 13.

We also intend to continue incorporating cyber serials into future exercises such as Trident Jaguar and Trident Juncture in 2014 and 15, among others. This year, this also includes taking on responsibility for the Cyber Coalition Exercise.

In this regard, I also welcome the approval by the NAC of the integration of cyber defence considerations into the next annual Crisis Management Exercise (CMX 2014) as part of the CFI Implementation Plan.

I see this work in Education, Training and Exercises aspect of Cyber Defence being really instrumental in our efforts to enhance our Cyber Defence Capability. Last Summer, all the Allies accepted their NDPP Cyber targets, and we are already starting to see some interesting multinational Smart Defence projects gaining some momentum.

For instance, Canada is working with 4 Nations¹ on a Multi-National Cyber Defense Capability Development Project to develop a collaborative framework through which to exchange information and improve their national situational awareness.

Belgium is leading on a renewed Malware Information Sharing Platform (MSIP) with 9 other participants² in order to maintain and extend the current MSIP technical capabilities in order to enhance information sharing as well.

Portugal is leading participants from 9 other countries³ on a CIS-E-Learning project and has also proposed a SD project on Cyber Training.

Thirdly, and focusing back on the Cyber Defence Action Plan, the **NATO Cyber Defence Lessons Learned process** is now in place. In addition, our technical ability to **assess the implementation and effectiveness** of NATO's Cyber Defence measures deployed on NATO CIS is now framed in **ACT's Conceptual Framework for Measuring NATO Cyber Defence** and currently under review by the relevant committees.

Finalemment, je voudrais insister sur le rôle grandissant du Centre d'Excellence sur la Coopération dans la Cyber Défense de Tallinn dans nos efforts collaboratifs et tout particulièrement le travail fournit en soutien des exercices et sur les didacticiels de formation en ligne.

Nul ne peut contester le défi que représente le domaine Cyber pour les Allies et pour l'OTAN. C'est aussi une occasion qui se présente à nous de poursuivre la Transformation de l'Alliance. La réponse dépendra de notre aptitude à évaluer la nature de la menace, à partager l'information et à assurer une coordination efficace de toutes les actions individuelles et collectives.

Merci

¹ DEN, ROU, NLD, NOR

² CZE, DEU, LTU, LUX, NLD, NOR, POL, ROU, TUR

³ ALB, GRC, ITA, LVA, NLD, ROU, GBR, TUR, HRV