CIO.GAL/87/11
11 May 2011

ENGLISH only

OSCE Conference on a

Comprehensive Approach to Cyber Security:

Exploring the Future OSCE Role

Closing Remarks by H.E. Ambassador Norkus

Chairperson of the OSCE Permanent Council

Excellencies, Ladies and Gentlemen,
Dear Friends and colleagues,

On behalf of the Lithuanian Chairmanship-in-Office, I have the honour to begin this final session of the *OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role.*

Over the last two days we have heard many interesting discussions and have covered a lot of ground. I am particularly pleased by a number of concrete recommendations for OSCE follow up activities raised by conference participants.

It was reiterated that the OSCE offers a unique platform to discuss threats to cyber security due to its comprehensive approach to security and broad membership. We began our conference with this important departure point. I am certain that this approach has been enhanced and strengthened as we get closer to our conclusions.

I think it is safe to say that a solid agreement exists that the OSCE has a role to play in comprehensively enhancing cyber security and can draw on the work of several OSCE entities working on related issues.

In preparation of this meeting the Chairmanship circulated a Non-Paper under CIO.GAL/80/11 outlining a possible way forward and additional follow-up activities. We are pleased to see that a good number of ideas contained therein have been discussed and supported.

That said, let me highlight some concrete recommendations that were proposed during the working sessions:

- Several participating States suggested the OSCE to focus on measures related to the politico-military dimension.
- In particular the OSCE's expertise regarding CBMs and CSBMs was highlighted. Moreover, the usefulness of applying this expertise in cyberspace to enhance transparency, predictability, stability and reduce the risks of misperception, escalation and conflict was emphasised. Such CBM's could also permit an exchange of national views on norms of behaviour within politico-military context building on existing international law.
- Participants highlighted the OSCE as being a unique platform for sharing expertise, good practices and raising awareness of cyber threats and potential responses.
- It was stressed that the OSCE should continue and expand on its capacity building efforts in this thematic area mindful that cyber security starts at the individual level.
- The issue of mainstreaming cyber related issues across all three OSCE dimensions was raised ("cyber mainstreaming").
- It was reiterated that OSCE should complement existing efforts and actively co-operate with other regional and international entities active in this thematic area.
- It was underscored that while countering cyber threats we need to ensure our shared values of human rights and fundamental freedoms.
- It was suggested that the OSCE could discuss pertinent terminology as agreement on terms/definitions is crucial.
- Support was expressed to potentially elaborate on a strategic framework in the area of comprehensively enhancing cyber security at the Vilnius OSCE Ministerial Council.

Ladies and Gentlemen,

Our objective has been to explore the future OSCE role in this thematic area. We believe we have succeeded in this endeavour. The conference report which will be prepared by the conference focal points as stipulated in PC.DEC 992 and will sum up all of the recommendations, and we hope that it will ultimately inform our next steps as we continue our path towards Vilnius.