Concept paper for the Side Event at the UN Headquarters in New York

"Cyber/ICT security: confidence building measures"

On 8 April 2015, Lithuania will convene a side event on cyber/information and communications technologies (ICTs) security, focusing on confidence building measures (CBMs).

Background

The advent of the digital age and development of the Internet in the past 20 years have changed the world we live in and revolutionized everyday life of peoples and societies on an unprecedented scale. ICT infrastructures and networks have become the very fiber that connects the modern world and measures to enhance their security are among the most pressing security concerns of many states.

The importance of cyber/ICT security is now being recognized globally as is the commitment to proactively address and handle threats to and in the use of ICTs. Considering that these threats are virtually untraceable, eminently deniable, with perpetrators that can be both states and non-state actors – many or few – the need for stronger international co-operation is widely acknowledged. A crucial part of such efforts aims at reducing the risks of misperception and possible emergence of political or military tensions among states from the use of ICTs, as such tensions could escalate into conflicts involving the use of cyber/ICT-related or conventional means and therefore constitute a threat to international peace and security. The use of ICT and cyberspace for terrorist purposes is also a fast growing threat, requiring a proactive and coordinated response.

Response by the UN and regional actors

Regional organizations

The Organization of Security and Cooperation in Europe (OSCE) has been focusing on cyber/ICT security and made tangible progress in particular by developing a set of specific CBMs to reduce the risks of conflict stemming from the use of ICTs. On 3 December 2013, the OSCE Participating States adopted an initial set of CBMs (PC.DEC/1106) that enables voluntary exchanges of information and communication among states. The Informal Working Group of the OSCE Security Committee was established in 2012 and meets regularly to discuss information exchanged and to explore appropriate development of CBMs. The participating States are now pursuing the implementation of the agreed CBMs and consider adopting additional measures.

The Organization of American States (OAS) has also been cooperating in the field of cyber-security through the Inter-American Committee against Terrorism (CICTE) and the Cyber Security Program. In 2004, OAS General Assembly approved the resolution "The Inter-American Integral Strategy to Combat Threats to Cyber Security" (AG/RES.2004 (XXXIV-O/04)), which mandated the CICTE Secretariat to begin working on cyber security issues. The OAS aims to build and strengthen cyber-security capacity in the member states by providing technical assistance and training, holding roundtables and exercises, and the exchange of best practices. The CICTE Secretariat is engaged in a number of initiatives, including creating a hemispheric watch and warning network made up of national Computer Security Incident Response Teams that provides guidance and support to regional cyber security technicians.

The Member States of the Association of Southeast Asian Nations (ASEAN) are likewise actively engaged in dialogue and consultation on issues related to cyber-security. In the Statement of the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security adopted by ASEAN Regional Forum (ARF) on 12 July 2012, the participating states, *inter alia*, committed to promote dialogue on confidence-building, stability, and risk reduction measures to address the implications of ARF participants' use of ICTs, including exchange of views on the potential use of ICTs in conflict.

Work is underway to complete the draft ARF work plan on security in the use of ICTs. In 2014, ARF workshop on cyber confidence building measures was held in Kuala Lumpur, Malaysia.

United Nations

The issue of cyber/ICTs security appeared on the UN agenda in 1998, when the resolution "Developments in the field of information and telecommunications in the context of international security" (A/RES/53/70) was first adopted by consensus. The Secretary-General has since been presenting annual reports containing the views of Member States to the General Assembly. Four successive Groups of Governmental Experts (GGE) were established in 2005, 2010, 2012 and 2014 and mandated to examine the existing and potential threats from the cyber-sphere and possible cooperative measures to address them. The GGEs presented their reports to the General Assembly in 2010 and 2013 (A/65/201 and A/68/98). The current GGE comprised of 20 experts has already met on 21-25 July 2014 and 12-16 January 2015 and plans two more meetings on 13-17 April and 22-26 June 2015.

Threats related to cyber/ICT security were also discussed by the Security Council Counter-Terrorism Committee (CTC). On 24 May 2013, the CTC held a special event with Member States "Countering terrorism through the use of new communications and information technologies" that focused on terrorist abuse of mobile-telephone-based communications and financial transactions, border controls and the internet.

Objective of the meeting

The side-event on cyber/ICT security will focus on confidence building measures to reduce the risks of conflict stemming from the use of ICTs. The meeting will build on exchanges that have taken place in other fora, with a particular emphasis on the work by regional organizations. The discussions would showcase the ever-growing importance and global relevance of cyber/ICT security, in particular when it comes to the question of enhancing mutual trust and confidence between states to effectively deal with cyber-attacks. They would also highlight the need of closer international co-operation in the field as well as sharing of experience and best practises among different regions. Furthermore, the event will provide a platform for regional actors to identify synergies and provide an opportunity to explore possibilities for enhanced and wider co-ordination. The event will not duplicate the efforts currently undertaken by various UN and regional bodies, but rather feed-in into ongoing work. It is also expected to reaffirm a principled position that while fighting against cyber/ICT threats, we must ensure that values of human rights, fundamental freedoms, rule of law and democracy remain firmly safeguarded.

The meeting will be open to all UN Member States, UN agencies, regional organisations and members of civil society and industry.

Speakers

- Representative of a think-tank/academia to set the scene by providing a general overview of the issue;
- OSCE (Chair of the Informal Working Group on cyber CBMs);
- ASEAN;
- OAS.

Questions for discussion

During the session, the Participants will be encouraged to actively engage in discussions and may wish to address the following in their statements:

- What threats related to cyber/ICT security present the most significant risk to international peace and security? Which of them could be alleviated by using CBMs?
- Are cyber/ICT security CBMs sufficiently utilised as part of the UN conflict prevention / pacific settlement of disputes toolbox?
- How could regional initiatives on cyber/ICT security be used to develop UN capacities in this field?
- How could we ensure that all relevant UN and regional actors (General Assembly, Security Council, Group of Governmental Experts, Secretariat and regional actors) provide a coherent response to cyber/ICT threats?