



OSCE CONFERENCE ON A COMPREHENSIVE APPROACH TO CYBER SECURITY: EXPLORING THE FUTURE OSCE ROLE

Vienna, Hofburg

09-10 May 2011

Draft Annotated Agenda

Monday, 09 May 2011

08.45–10.00 **Registration**

10.00–10.30 **Opening Session:**

- Opening remarks by the OSCE Chairmanship;
- Opening address by the OSCE Secretary General;

10.30–10.45 **Coffee break**

10.45–13.00 **Working Session 1: The Politico-Military dimension**

The session will showcase and raise awareness of various threats emanating from cyberspace related to the politico-military domain, including to critical infrastructure. OSCE participating States recognise that national security is intrinsically linked with cyber security, and the topic has become part of foreign policy considerations. Consequently, one important aspect will be to elaborate on the desirability, nature and possible extent of politically binding norms of State behaviour in cyberspace. In the past norms related to other thematic areas including confidence-building measures, political guidelines or codes of conduct, have been adopted to supplement legally binding instruments. At other times norms have served as precursors or a “bridge” for subsequent legal instruments. Questions that could be addressed:

1. Is there a need for State norms of behaviour in cyberspace?
2. What could such norms look like?
3. What comparative advantages does the OSCE have for developing such norms based on its comprehensive approach to cyber security?

- **Timothy Dowse**, Director, Intelligence and National Security, Foreign and Commonwealth Office, UK

- **Michele Markoff**, Director, Office of Cyber Affairs, Department of State, US
- **Nicolay Klimashin**, Assistant to the Secretary, Security Council of the Russian Federation, Russian Federation
- **Dr. Detlev Wolter**, Head of Section, Federal Foreign Office, Germany

Discussion

- Moderator's closing remarks

Moderator: (tbc)

13.00–15.00

Lunch break

15.00–16.00

Working Session 2: Cybercrime and terrorist use of the Internet

This session will focus on cybercrime and terrorist use of the Internet. It will highlight potential countermeasures, lessons learned and national best practices, also with regard to investigation and prosecution. Central to discussions will be the development of public-private partnerships and effective involvement of civil society as part of enhancing cyber security, in recognition that a secure cyberspace is as much in the interest of states and the individual user as it is for businesses. The session will also focus on relevant fundamental human rights and civil liberty considerations, such as freedom of expression and free information as well as privacy aspects, and the responsibility of States and the Private Sector to upholding them in efforts to enhance cyber security. Questions that could be addressed:

1. Which criminal and terrorist threats emanating from cyberspace are participating States most concerned about?
2. How can the knowledge and expertise of the private sector and civil society in terms of dealing with cyber threats and enhancing cyber security by fully harnessed by countries?
3. What are the biggest challenges for countries in responding to cyber challenges, also in light of fundamental human rights and civil liberty considerations? How can the OSCE assist in this regard?

- **Jürgen Treib**, Assistant Head of Section , Ministry of Internal Affairs, Germany
- **Keith Verralls**, Detective Inspector, New Scotland Yard, UK
- **Mirco Rohr**, Technology Evangelist, Kaspersky Labs

16.00 – 16.15

Coffee Break

16.15 – 17.15

Working Session 2 continued

Discussion

— Moderator's closing remarks

Moderator: **Sanjay Goel**, Professor, NYS Center for Information Forensics and Assurance Associate, School of Business University at Albany, State University of New York

17.15–19.15 Networking reception opened by OSCE CiO

Tuesday, 10 May 2011

10.00–12.00 Working Session 3 – Global responses

This session will review global responses to cyber threats and developments in the area of cyber security. Of particular focus will be initiatives at the UN level, inter alia, related to the international legal framework. In addition, the session will focus on measures that can reduce misperception and risk including confidence-building, stability and risk-reduction measures, and information exchanges e.g. on pertinent legal frameworks. One discussion topic will be whether a set of politically binding norms may represent a practical tool to complement and advance initiatives taking place at the global level, especially at the UN level. Questions that could be addressed:

1. How well are international co-operation mechanisms used for dealing with cyber threats? Could they be further improved and if so, how? How could the OSCE contribute to this process without duplicating efforts?
2. How can co-operation between and among organizations dealing with aspects of cyber security be enhanced or potentially even institutionalized?
3. Could co-ordinated international awareness-raising campaigns enhance current efforts dealing with cyber security, and what could such a campaign entail?

— **Gillian Murray**, Focal Point for Cybercrime, UNODC

— **Jan Neutze**, UN CTITF (tbc)

— **Marco Obiso**, Co-ordinator for Intersectoral Activities, ITU

— **Andrea Cavina**, Office of Nuclear Security, IAEA

— **Milos Mijomanovic**, Criminal Intelligence Officer, INTERPOL

Discussion

— Moderator's closing remarks

Moderator: **Gavin Willis**, Deputy Head International Relations, National Technical Authority for Information Assurance, UK

12.00–14.00 **Lunch break**

14.00–15.00 **Working session 4 – Regional responses**

This session will review the roles and initiatives of regional organizations related to specific aspects of cyber security, and how they contribute to pertinent international developments. Specifically, it will highlight how regional organizations have addressed global disparities in cyber capabilities on a regional level through technical assistance, awareness raising, capacity building as well as developing guidelines and norms. One discussion topic will be whether the OSCE can build on the work of such regional organizations adding to its capacity building repertoire in this thematic area. Questions that could be addressed:

1. What would be areas in which regional organizations should play an even bigger role in terms of combating cyber threats?
2. Are there specific areas the OSCE should consider with regard to capacity building assistance drawing on the work of other regional organizations?
3. How could an “alliance” (formal/informal) of regional organizations dealing with cyber security aspects enhance global efforts?

— **Eneken Tikk**, Legal Adviser, Co-operative Cyber Defence Centre of Excellence

— **Marta Requena**, Head, Public International Law and Anti-Terrorism Division, Council of Europe

and

— **Alexander Seger**, Head, Economic Crime Division, Council of Europe

— **Andrea Servida**, Deputy Head, Internet, Network and Information Security Unit, Information Society and Media Directorate-General, European Commission

— **Vladislav Shushin**, Counsellor, CSTO

— **Heli Tiirma-Klaar**, Senior Advisor, Cyber Defence Section, NATO

— **Belisario Contreras**, Assistant Project Manager, Inter-American Committee against Terrorism Secretariat for Multidimensional Security, OAS

15.00 – 15.30 **Coffee Break**

15.30 – 16.15 **Working Session 4 continued**

Discussion

— Moderator’s closing remarks

Moderator: Petr Korbelt, Policy and Planning Officer, Office of the Secretary General, OSCE (tbc)

16.15–17.30

Closing session: The potential role of the OSCE

The closing session will look at the potential future role of the OSCE and, specifically, whether and how initiatives on the global and regional level might be further enhanced by the OSCE, also in light of recommendations made by the pertinent United Nations Group of Governmental Experts¹. Central to the discussion will be to explore the possible OSCE role in discussing and potentially developing norms pertaining to the behaviour of States in cyberspace, building on its comprehensive approach to cyber security as well its strengths related to confidence building, sharing lessons learned, capacity building and promoting best practices. In addition, this session will explore what a “different OSCE role” would mean and entail related to: 1.) OSCE structures in all three dimensions; 2.) The political framework and decision making process including a strategic OSCE document, 3.) international efforts. Questions that could be addressed:

1. How could the OSCE mandate be further strengthened so as to enable the Organization to make an even bigger contribution to international efforts aimed at enhancing cyber security?
2. What are participating States’ views on the elaboration of an OSCE strategic document on a comprehensive approach towards cyber security?
3. What could an internal OSCE co-ordination mechanism dealing with cyber security look like?

- Overview of Non-Paper and conference recommendations
- Discussion
- Closing remarks by the OSCE Chairmanship in Office

1 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)

II. Background

The threats to the security of the OSCE participating States are constantly evolving, reflecting the changing security environment and the emergence of new risks and challenges. Over the last several years, cyber security has emerged as an increasing concern to OSCE participating States. In response, they have agreed to address certain cyber threats building on the OSCE's comprehensive approach to security.

Initially, the OSCE's activities were focused mainly on individual aspects of enhancing cyber security such as combating cybercrime and combating the use of the Internet for terrorist purposes, while ensuring that efforts to enhance cyber security do not impinge upon fundamental freedoms such as freedom of expression (and assembly) and the freedom of information on the Internet. Since 2005 several OSCE-wide events have been organized to deal with various aspects of the issue.

At the same time, however, recognizing the close interrelationships among the various aspects of contemporary threats emanating from cyberspace, participating States began deliberations in early 2008 on a more comprehensive approach, culminating in the 2009 OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security, organized under the auspices of the Forum for Security Co-operation (FSC), pursuant to FSC.DEC/10/08 and FSC.DEC/17/08. The objective was to increase awareness of concrete steps that can be taken to comprehensively strengthen cyber security, to explore the potential role for the OSCE in this regard and to identify concrete measures for possible follow-up action by all relevant OSCE bodies. Recommendations and suggestions, based on discussions at the workshop, were circulated under FSC.DEL/92/09.

In addition to these OSCE-wide initiatives, a number of smaller-scale events organized by the OSCE – and in particular those organized/facilitated by the ATU and the SMPU in 2009/2010 – have promoted a more comprehensive approach to cyber security.

Participating States have remained seized with the topic – for instance, the United States circulated a cyber security self-survey designed to identify national gaps and capacities in response to cyber threats (PC.DEL/38/10) and a food for thought paper on possible *OSCE Contributions to International Cybersecurity Efforts* (PC.DEL/143/10) – and in June 2010 a joint PC/FSC session discussed the potential role of the OSCE as a platform for exchanging national views on norms pertaining to the behaviour of States in cyberspace, building on the Organization's comprehensive approach to security and complementing initiatives and developments at the regional and international level.

The issue of cyber security was also discussed in the framework of the Corfu Process and as a necessary component of the broader effort to tackle transnational threats. The Report by the OSCE Secretary General on the Implementation of MC.DEC/2/09 on Further OSCE Efforts to Address Transnational Threats and Challenges to Security (SEC.GAL/107/10) showcased options for a more active role of the Organization in comprehensively enhancing cyber security.

Ensuing discussions have shown that participating States are willing to explore the possibility of such a role for the OSCE. In order to further facilitate the political debate on this issue the OSCE Lithuanian Chairmanship-in-Office (CiO) has put forward this initiative. The conference is organized in line with PC.DEC/991 and PC.DEC/992.

Workshop Points of Contact

Nemanja Malisevic

Associate Programme Officer
OSCE Action against Terrorism Unit

Nemanja.Malisevic@osce.org

Tel. +43 1 514 36 6711

Ben Hiller

Assistant Programme Officer
OSCE Action against Terrorism Unit

Ben.Hiller@osce.org

Tel. +43 1 514 36 6682