osce

Organization for Security and Co-operation in Europe
Permanent Council

PC.DEC/991
31 March 2011

Original: ENGLISH

856th Plenary Meeting
PC Journal No. 856, Agenda item 3

DECISION No. 991
OSCE CONFERENCE ON A COMPREHENSIVE APPROACH TO CYBER SECURITY: EXPLORING THE FUTURE OSCE ROLE

The Permanent Council,

Recalling Ministerial Council Decision No. 3/04 on combating the use of the Internet for terrorist purposes, which calls on the participating States to exchange information on the use of the Internet for terrorist purposes and to identify possible strategies to combat this threat,

Recalling Ministerial Council Decision No. 7/06 on countering the use of the Internet for terrorist purposes, which voices the participating States’ concern over continued hacker attacks and calls on them to take appropriate measures to protect vital and critical information infrastructures and networks against the threat of cyber attacks,

Recalling Ministerial Council Decision No. 9/07 which further broadened the OSCE mandate to also include combating sexual exploitation of children on the Internet,

Recalling Ministerial Council Decision No. 9/09 on combating hate crimes, which calls on the participating States among others to address the increasing use of the Internet to advocate views constituting an incitement to bias-motivated violence including hate crimes, while ensuring that any relevant measures taken are in line with OSCE commitments, in particular with regard to freedom of expression,

Recalling Forum for Security Co-operation Decision No. 10/08 on an OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security and acknowledging the outcomes of this event including recommendations and suggestions circulated under FSC.DEL/92/09,

Recalling discussions on the issue of cyber security in the framework of the Corfu Process,

Recalling Ministerial Council Decision No. 2/09 which underscored the willingness of participating States to address cyber security as a transnational threat and challenge to security and stability and taking note of 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) which showcased options for a more active role of the Organization in comprehensively enhancing cyber security,

Recalling presentations and discussions at the 45th joint FSC-PC session on 2 June 2010, which considered, *inter alia*, the potential role of the OSCE as a platform for exchanging national views on norms pertaining to the behaviour of States in cyberspace,

Taking account of efforts, initiatives and instruments by other regional and international entities active in areas related to cyber security – in particular at the United Nations level – and wishing to complement, promote and enhance existing efforts, as appropriate, while avoiding unnecessary duplication,

Having regard to continuing interest by the United Nations, notably in a report in 2010 on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201) by a Group of Government Experts established pursuant to paragraph 4 of General Assembly resolution 60/45,

Recognizing that threats emanating from cyberspace and measures to enhance cyber security are among the pressing security concerns of participating States,

Noting with concern that threats emanating from cyberspace are constantly evolving and rapidly increasing,

Recognizing that in order to remain relevant to the needs and interests of the participating States, OSCE activities that tackle threats emanating from cyberspace need to evolve in line with the threat and noting pertinent OSCE-wide, regional and national awareness raising and capacity-building activities organized by a number of OSCE structures,

Recognizing that interrelationships among the various aspects of contemporary threats emanating from cyberspace require a comprehensive approach to cyber security,

Reaffirming that respect for human rights and fundamental freedoms, democracy and the rule of law is at the core of the OSCE’s comprehensive concept of security, and that efforts to enhance cyber security shall fully respect fundamental freedoms such as freedom of opinion and freedom of expression, including the freedom to seek, receive and impart information, which are vital to democracy and in fact are strengthened by the Internet and the rule of law,

Reaffirming that the OSCE can act as a platform for co-operative security dialogue among participating States as well as regional and international entities active in the thematic area, including exchange of views on norms and behaviour of States,

Tasks the Secretary General to organize an OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role, to be held on 9 and 10 May 2011, in Vienna, with the participation of relevant international entities and private sector representatives, and in line with the outline description annexed to this decision;

Invites the participating States to consider providing extrabudgetary contributions for the above-mentioned event.

PC.DEC/991
31 March 2011
Annex

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

Vienna, 9 and 10 May 2011

The OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role, will study the potential way forward in this thematic area.

The event will be conducted in two parts:

Part 1 of the conference will showcase and raise awareness of various threats to cyber security related to (a) the politico-military domain, including critical infrastructures and the nature and possible extent of norms of behaviour in cyberspace; and (b) cybercrime and terrorist use of the Internet, highlighting potential countermeasures, lessons learned and national best practices, also with regard to investigation and prosecution, the development of public-private partnerships and effective involvement of civil society.

Part 2 of the event will then focus on potential responses to cyber threats and consideration for developing norms of State behaviour that can contribute to cyber security as well as measures that can reduce misperception and risk, including confidence-building, relevant human rights considerations, stability and risk-reduction measures, information exchanges, for example on pertinent legal frameworks, and will, in particular, highlight developments and initiatives at the global and regional level, especially the roles of other regional organizations in this area.

The closing session will look forward to 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, including through capacity-building measures, and which potential gaps OSCE initiatives might fill, also in light of recommendations made by the pertinent United Nations Group of Governmental Experts[1].

Overall, the conference will be conducted with a view to:

– Highlighting the impact on security in the OSCE region of various forms and techniques of misusing cyberspace, the different perpetrators and targets, and relevant countermeasures and responses in particular from international and regional organizations;

[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).

– Exploring the potential for the OSCE to add value to existing efforts through a comprehensive approach to cyber security including the exchange of views at national level and potentially developing norms relevant to the behaviour of States in cyberspace;

– Providing a basis for determining the future role of the Organization in this thematic area and how, in general, the OSCE profile could potentially be sharpened building on the discussions, recommendations and outcomes of previous OSCE meetings;

– Examining the steps that may need to be taken both on an organizational level and with regard to the political framework, and if initiatives at the global and regional level could be further enhanced by building on the OSCE’s strengths related to confidence-building, sharing lessons learned, capacity-building and promoting best practices – possibly through the development of a strategic OSCE document.

The OSCE Secretariat will prepare a follow-up report, outlining concrete suggestions and recommendations made at the event regarding a future role for the OSCE in the area of comprehensively enhancing cyber security and for potential follow-up activities by the relevant OSCE structures as a complement to international efforts in this area.