osce

Organization for Security and Co-operation in Europe
Permanent Council

PC.DEC/1202
10 March 2016

Original: ENGLISH

1092nd Plenary Meeting
PC Journal No. 1092, Agenda item 1

DECISION No. 1202
OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in co-operation with relevant international organizations, hereinafter referred to as “security of and in the use of ICTs.” They further decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

The OSCE participating States, recalling the OSCE role as a regional arrangement under Chapter VIII of the UN Charter, confirm that the CBMs being elaborated in the OSCE complement UN efforts to promote CBMs in the field of security of and in the use of ICTs. The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be consistent with: international law, including, *inter alia*, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms.

The following CBMs were first adopted through Permanent Council Decision No. 1106 on 3 December 2013:

1. Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties.

2. Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs.

3. Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of

political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity.

4. Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.

5. The participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard.

6. Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.

7. Participating States will voluntarily share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.

8. Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.

9. In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary.

10. Participating States will voluntarily exchange views using OSCE platforms and mechanisms *inter alia*, the OSCE Communications Network, maintained by the OSCE Secretariat’s Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs.

11. Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include *inter alia* proposals from the Consolidated List

circulated by the Chairmanship of the IWG under PC.DEL/682/12 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.

The following CBMs were first adopted through Permanent Council Decision No. 1202 on 10 March 2016:

12. Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or subregional level; this is to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating States to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs.

With respect to such activities participating States are encouraged, *inter alia*, to:

– Conduct such activities in the spirit of enhancing inter-State co-operation, transparency, predictability and stability;

– Complement, through such activities, UN efforts and avoid duplicating work done by other fora; and

– Take into account the needs and requirements of participating States taking part in such activities.

Participating States are encouraged to invite and engage representatives of the private sector, academia, centres of excellence and civil society in such activities.

13. Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision No. 1106.

14. Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs.

15. Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies.

Collaboration may, *inter alia*, include:

– Sharing information on ICT threats;

– Exchanging best practices;

– Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;

– Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident;

– Sharing national views of categories of ICT-enabled infrastructure States consider critical;

– Improving the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and subregional levels; and

– Raising awareness about the importance of protecting industrial control systems and about issues related to their ICT-related security, and the necessity of developing processes and mechanisms to respond to those issues.

16. Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region. OSCE participating States agree that such information exchange, when occurring between States, should use appropriately authorized and protected communication channels, including the contact points designated in line with CBM 8 of Permanent Council Decision No. 1106, with a view to avoiding duplication.

Practical Considerations[1]

The provisions of these Practical Considerations do not affect the voluntary basis for the activities related to the aforementioned CBMs.

Participating States intend to conduct the first exchange by October 31, 2014, and thereafter the exchange of information described in the aforementioned CBMs shall occur annually. In order to create synergies, the date of the annual exchanges may be synchronized with related initiatives participating States are pursuing in the UN and other fora.

The information exchanged by participating States should be compiled by each of them into one consolidated input before submission. Submissions should be prepared in a manner that maximizes transparency and utility.

Information may be submitted by the participating States in any of the official OSCE languages, accompanied by a translation in English, or only in the English language.

Information will be circulated to participating States using the OSCE Documents Distribution system.

Should a participating State wish to inquire about individual submissions, they are invited to do so during meetings of the Security Committee and its Informal Working Group

[1] First adopted as part of Permanent Council Decision No. 1106 on 3 December 2013.

established by Permanent Council Decision No. 1039 or by direct dialogue with the submitting State making use of established contact mechanisms, including the email contact list and the POLIS discussion forum.

The participating States will pursue the activities in points 9 and 10 above through existing OSCE bodies and mechanisms.

The Transnational Threats Department will, upon request and within available resources, assist participating States in implementing the CBMs set out above.

In implementing the CBMs, participating States may wish to avail themselves of discussions and expertise in other relevant international organizations working on issues related to ICTs.

Considerations[2]

Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039, to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include *inter alia* proposals for CBMs aimed at increasing transparency, co-operation, and stability among States in the use of ICTs. Such efforts should, to the extent that they relate to the mandate of the IWG, take into account and seek to complement the expert-level consensus reports of the 2013 and 2015 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, including their recommendations on voluntary CBMs, and the Group’s work in support of voluntary non-binding norms, rules and principles of responsible State behaviour in the use of ICTs.

The Transnational Threats Department of the OSCE Secretariat, through its Cyber Security Officer will, upon request and within available resources, assist participating States in implementing the CBMs set out above, and in developing potential future CBMs.

[2] First adopted as part of Permanent Council Decision No. 1202 on 10 March 2016.