osce
Organization for Security and Co-operation in Europe

The OSCE Secretariat’s intervention at the OEWG intersessional meeting
6 December 2022

With its vast experience in traditional arms control the OSCE was well-placed to start to work on CBMs related to the field of ICTs. OSCE participating States have adopted the first set of CBMs in 2013 and agreed on the second set of CBMs in 2016, adding up to 16 cyber/ICT security CBMs[1] overall. These are transparency and cooperative measures.

For many years, the implementation of these CBMs has been at the forefront of both the OSCE Informal Working Group on cyber and in capacity-building work of the OSCE Secretariat. Through these efforts, trust and partnership continues to be built between participating States while at the same time increasing national cyber resilience.

Many OSCE participating States have shared their practical experiences on being a member of the OSCE CBM8 Point of Contact (PoC) Network in the past two days. According to CBM8 “*Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs*”. States voluntarily provide this information on a password-protected platform and have committed to regularly update the data.

The OSCE Secretariat maintains the database, ensures that States receive login data and have access to the platform. The nominated contacts are policy and/or technical PoCs, the former usually – but not exclusively – comprising representatives of MFAs while the latter are mainly CERTs/CSIRTs. One of the objectives of the PoC Network is to enable participating States to reach out to each other in a crisis situation. In our experience the closed online platform ensures that PoCs feel confident to share personal contact details at which they can be reached.

In the initial stage, participating States voluntarily provided the information on the respective Points of Contact, bringing the implementation of this specific CBM to 60% in 2015. With proactive outreach and capacity-building activities by the OSCE Secretariat by 2020 56 out of 57 participating States has nominated a Point of Contact.

The OSCE Secretariat conducts – usually twice a year – so-called Communication Check exercises for PoCs which have a two-fold aim: on one hand to ensure that the contact details are still up-to-date and on the other hand to encourage coordination within national structures as well as cooperation between PoCs, depending on the respective tasking. The results of the Communication Checks are presented to the participating States in anonymized reports.

Furthermore, the OSCE Secretariat introduced the Annual meeting of Points of Contact in 2019, to ensure that the representatives can also meet face-to-face, thus further building trust and partnerships among the PoCs.

When it comes to the other 15 OSCE confidence-building measures, I would like to mention a few examples which might also be relevant in the UN context. Transparency measures involve the voluntary sharing of information on national and transnational threats to ICTs (CBM 1), on measures taken to ensure open, interoperable, secure and reliable Internet (CBM 4) and on

[1] The document containing all the 16 CBMs is publicly available in OSCE official languages: https://www.osce.org/pc/227281

national organizations, strategies, policies and programmes (CBM7). Participating States regularly report on these in the OSCE Informal Working Group on cyber issues.

Implementation of the CBMs is currently the main focus of OSCE participating States, including the "Adopt a CBM" initiative, which invites States or a group of States to champion the elaboration of modalities for implementing a specific CBMs. This initiative has produced tangible results in the past years. For example a database of cyber-related terminology[2] and an e-learning on how to set up national policies for coordinated vulnerability disclosure[3]. OSCE participating States are working extensively on the topic of critical infrastructure protection, with a report just published on emerging practices related to cyber incident classification[4].

More details on the OSCE's 16 confidence-building measures are available in an e-learning course, which is publicly available on the OSCE website.[5]

With the role of regional organizations emphasized in the UN GGE and OEWG reports, the OSCE aims to make the experiences gained in CBM implementation not only available to the OSCE region but also beyond through various capacity-building tools and products. We hope that these might prove useful and serve as inspiration for other regions and countries.

[2] https://cbm9.gov.rs/

[3] https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCVD+2022_04/about

[4] https://www.osce.org/secretariat/530293

[5] English: https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCBM_v1+2020_11/about
French: https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCBM_FR+2022_01/about
Russian: https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCBM_RU+2021_06/about