Organization for Security and Co-operation in Europe

Statement by OSCE Secretariat at the 7th Substantive session of the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025

On the topic of Confidence-building Measures:

The Organization for Security and Co-operation in Europe has a 10 year experience in developing and implementing regional cyber confidence-building measures. OSCE participating States are committed to operationalizing the 16 cyber/ICT security CBMs. The OSCE Secretariat supports states in these efforts and I would like to share some examples of this experience.

Chair, in your guiding questions you mention the possibility of developing additional global CBMs, amongst others related to public-private partnerships, critical infrastructure protection and coordinated vulnerability disclosure.
I would like to inform you that the OSCE participating States have adopted regional CBMs on these three topics. Implementation of the CBMs creates trust and confidence, and at the same time builds capacities and creates national cyber resilience. The work done related to these OSCE Confidence-building Measures might inform the discussions in the OEWG.

I would like to share some tools the OSCE participating States have developed regarding the above mentioned three topics.

A report on Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States[1] - This report is the result of research conducted on concrete examples of public-private partnerships (PPPs) for cyber/ICT security in OSCE participating States. It presents emerging practices in PPPs as baseline recommendations and promote public-private collaboration as an important element in strengthening national cyber resilience and international cyber stability. The report is publicly available on the OSCE website in English and Arabic.

Related to Critical infrastructure protection we have published a report titled - **Cyber Incident Classification: A Report on Emerging Practices within the OSCE region**[2]. The report highlights emerging practices in and provides recommendations on national classification of cyber incidents by underlining commonalities in existing approaches to cyber incident classification among OSCE participating States and identifying limitations in this process.

The OSCE has also developed a publicly available **e-learning course on coordinated vulnerability disclosure**[3]. It provides an overview of CVD as a tool to strengthen national, regional and international cybersecurity. Over six modules, it gives an overview of the CVD process, the main stakeholders and their roles and responsibilities, as well as look as some of the main challenges of CVD.

---

[1] https://www.osce.org/secretariat/539108
[2] https://www.osce.org/secretariat/530293
[3] https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCVD+2022_04/about

The OSCE Secretariat follows the deliberations at the OEWG and encourages all OSCE participating States to engage in and contribute to these discussions. During our training events we give regular updates on the developments in the OEWG. Furthermore, we conduct every year a cyberdiplomacy training for OSCE participating States with the aim to create better understanding on the Framework of Responsible state behaviour in cyberspace and enable them to meaningfully engage in international cyber policy deliberations both at the OSCE and the UN.

In this spirit, we have continuously updated the OSCE cyber Points of Contact about the establishment of the Global Points of Contact Directory. With the aim to raise awareness and encourage nominations, we have forwarded to all the OSCE CBM8 Points of contact UNODA's note verbale on the call for the nominations for the Global Points of Contact Directory. I hope you will receive many nominations from OSCE participating States. At the same time, we will continue to keep OSCE participating States updated on the developments of the Global PoC Directory.

I was delighted to hear Kazakhstan and France share a concrete example how they have used the OSCE Points of Contact network to reach out to another participating State. As the manager of the network, I am usually not informed about exchanges between PoCs, so it is good to receive such feedback.

To conclude, I would like to reconfirm the OSCE Secretariat's continued support for your efforts, Chair, and our readiness to share experiences, as well as our commitment to cooperate with UNODA on these issues.