Organization for Security and Co-operation in Europe

Statement by OSCE Secretariat at the 4th Substantive session of the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025

Under Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240

- *How international law applies to the use of information and communications technologies by States [from para 1, GA resolution 75/240]*

Related to increasing capacities of states on how international law applies to the use of ICTs I would like to share with you information about some activities the OSCE Secretariat has facilitated in the past months.

In February 2023, the OSCE organized the Executive Course on the International Law of Cyber Operations in Skopje, North Macedonia for 27 participants from the sub-region of South-East Europe. I am also happy to share that 55% of participants were women. The course was organized with the support of the Netherlands and delivered by Cyber Law International, an international legal firm specializing in such trainings. The training was designed for legal experts dealing with cyber/ICT issues and policy advisors responsible for cyber matters, to enable them to better navigate through the complex legal issues involving cyberspace. In particular, the course examined key legal principles, such as sovereignty and jurisdiction, and regimes of international law that govern cyber operations conducted by, or directed against, states and was complemented by practical exercises aiming at applying the legal principles to fictional scenarios. In their feedback participants indicated that the course proved very useful and improved their level of understanding of the applicability of international law in cyberspace.

Furthermore, with the support of the United Kingdom and the Netherlands the OSCE conducted an advance training on international cyberdiplomacy last November for diplomats from 16 OSCE participating States. The training aimed at familiarizing the participants with the UN framework of responsible state behaviour in cyberspace and the work of the OSCE in the field of cyber confidence-building measures. During interactive sessions, the participants shared their experiences on engaging in international cyber negotiations and delivering national statements in relevant forums. I would like to use this opportunity to thank UNODA, Ms. Katherine Prizeman, for her valuable contribution to the training.

- *Confidence-building measures [from para 1, GA resolution 75/240]*

Reflections on the OEWG Chair's non-paper on the Global PoC Directory

We would like to thank the Chair for distributing the non-paper on the Global PoC Directory. From the point of the OSCE, which has an operational regional Points of Contact network on policy and technical level, we welcome the proposed elements, which correspond to a high degree with the OSCE's database.

Related to the interaction with other directories, we welcome the changes introduced in the second version of the non-paper as we had concerns related to the possibility of automatic addition of information from the regional to global level, in particular related to interoperability with databases already in place.

Related to the interaction between PoCs, we have made the experience that confirming the receipt of the communication – without any prejudice to the substance of the response to be given – helps further build confidence, as the outreaching PoC is assured that the request has been received and work on the reply as started. For example, during OSCE exercises for the PoCs, we always request a confirmation of the receipt of the e-mail (ideally within 24 hours), while the timeline for a substantive answer might take longer (the recommended response time is usually 72 hours).

Regarding capacity-building for PoCs, the OSCE Secretariat stands ready to continue collaboration with OSCE participating States on delivering capacity-building activities. I would like to use this opportunity to share with you some examples of capacity-building activities specifically carried out for the OSCE CBM8 Points of Contact.

- On one hand we organize the Annual Meeting of Points of Contact, which aims to bring together the technical and policy Points of Contact to exchange views on various topics on the agenda, for example small group discussions on CBM 15 on Critical infrastructure protection and CBM16 on Coordinated Vulnerability Disclosure.
- Furthermore, we organize study visits between PoCs of a few states, which expressed interest to exchange information and engage in dialogue. For example in 2019, PoCs from Kazakhstan, Kyrgyzstan and Mongolia visited their counterparts in the Czech Republic and Slovakia to meet with various national authorities to have in depth discussions and further build confidence and trust.
- During the pandemic, we organized online expert sessions on various topics like cyberdiplomacy, education, public-private partnerships, table-top exercises, to just name a few which helped participants to gain knowledge on the specific topics and through its interactive character allowed participants to pose their questions related to the specific issue. Topics were selected based on the feedback received from CBM8 PoCs.

We welcome the OEWG Chair’s intention for holding a table-top exercise on the practical aspects of participating in a PoC Directory. As the OSCE Secretariat has years of experience in maintaining the PoC Network and has worked with OSCE participating States on implementing and strengthening the network, including through various exercises, we stand ready to support the Chair and UNIDIR in conducting this exercise, if this is of interest.

In conclusion, I would like to reiterate the OSCE Secretariat’s readiness and availability to share its experiences related to the development and implementation of cyber confidence-building measures and ensuing capacity-building activities with other regional organizations and interested states, which are not members of a regional organization.