Organization for Security and Co-operation in Europe

Statement by OSCE Secretariat at the 6th 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 Capacity-building

In line with the second Annual Progress Report stating "States in a position to do so are invited to continue to support capacity-building programmes, including in collaboration, where appropriate, with regional and sub-regional organizations […]" I would like to share some capacity-building activities carried out recently within the OSCE and also relevant for the implementation of the Framework on responsible State behaviour in cyberspace.

OSCE CBM No. 15 deals with critical infrastructure protection, which includes the promotion of the use of national cyber incident classification system. The objective of the relevant OSCE project funded by France and Germany is to increase State's capacities to deal with significant cyber/ICT incidents in an effective way. As part of these efforts the OSCE Secretariat conducted a workshop this September in Tashkent Uzbekistan. The event was attended by representatives of Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyzstan, Mongolia, Tajikistan and Uzbekistan. The workshop built on the good practice report titled "CYBER INCIDENT CLASSIFICATION: A Report on Emerging Practices within the OSCE region"[1] and was facilitated by experts from Czechia, France, Kazakhstan and Switzerland. The participants together with the contribution by the experts exchanged good practices and discussed the recommendations and challenges on implementing these systems especially in their specific regional context. The workshop was another good example how open and transparent engagement between cyber experts can build capacities, trust and partnership.

The sharing of information on vulnerabilities has been mentioned by many delegations this week. CBM No. 16 covers this issue within the OSCE. 4 OSCE participating States – namely Czechia, Hungary, the Netherlands and Romania – engage under the "Adopt-a-CBM" initiative by developing implementation modalities for that specific CBM. This September a workshop was organized in Istanbul, Türkiye for participating States of the OSCE sub-regions of Eastern and South-Eastern Europe, Central Asia, South Caucasus as well as Mongolia with the aim to discuss Coordinated Vulnerability Disclosure as a keystone of a comprehensive approach to national and regional cybersecurity. The event provided a platform for the exchange of good practices and examples of national Coordinated Vulnerability Disclosure policies. Most notably, it was organized in co-operation with the Dutch National Cyber Security Centre and the Public Prosecutor's office, who held a practical exercise on the second day of the event, which further created understanding about the nuances of vulnerability disclosure. Based on the feedback received from the participants the workshop contributed to their increased understanding of the CVD process, as well as the importance of defining national ICT vulnerability sharing processes.

[1] https://www.osce.org/files/f/documents/6/5/530293_1.pdf

Besides implementing CBMs the OSCE Secretariat also aims to raise awareness on the UN Framework of responsible state behaviour in cyberspace and cyberdiplomacy in general with the aim to create better understanding of the global processes on international cyberpolicy issues and enable participating States to engage in international cyber policy deliberations both at the OSCE Informal Working Group as well as the UN Open-ended Working Group. The training held in Vienna this November gathered 21 delegates from Eastern and South-Eastern Europe, Central Asia, South Caucasus and Mongolia and provided them with opportunities to exchange views with renowned cyber practitioners and diplomats closely involved in these processes. During the event, notable cyber diplomacy practitioners shared their experiences with cyber diplomacy, covered past and present UN cybersecurity policy processes, with a specific focus on the framework of responsible State behavior in cyberspace. I would like to agaom express my gratitude to Katherine Prizeman who accepted our invitation to speak at the training and shared the most recent developments on the work of the OEWG. Further, the training event also engaged participants in a practical exercise on coordinating national cybersecurity positions and prompted participants to share information on their national organization pertaining to cyber/ICT security. Participants also elaborated on some of the obstacles they face in engaging in international cyber deliberations, which provided valuable insight into future capacity-building needs, which the OSCE Secretariat will aim to address in upcoming training events.