REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

Statement by Estonia at 4th substantive session of

the 2021-2025 UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security

Discussion under the Thematic Session on Capacity Building,

9 March 2023

Thank you, Mr Chair, for giving me the floor.

Estonia underscores in the fundamental value of capacity building in as a prerequisite for achieving the goals and agreements sets in the OEWG discussions. Estonia supports and continues to substantiate the use of the principles of capacity building adopted in the 2021 final report of the OEWG. We believe that States need to mainstream these principles in all capacity building efforts – including in all national, regional and international formats and platforms.

Estonia regards cyber capacity building as a priority area in order to improve the overall resilience of countries against malicious cyber activities and allow to implement the recommendations reached at the UN level. Capacity building is a key part of our national cyber security policy, which is why we remain committed and open to sharing our knowledge and experiences.

Estonia has supported the development of cyber security systems in developing and partner countries for over ten years and continues to contribute to a number of multilateral cyber capacity building initiatives, such as the Global Forum on Cyber Expertise (GFCE), the World Bank's Cybersecurity Multi-Donor Trust Fund, various European Union initiatives, such as EU CyberNet, Cyber Resilience for Development (Cyber4Dev), as well as national initiatives. In order to carry out effective capacity building we need to make a continuous and conscious effort to coordinate, collaborate and pool our resources. There is a need to improve information exchange on existing activities, including lessons learned and best practises. A very useful platform for this is the GFCE and the Cybil portal. We would like to underline that there are also other capacity-building project mappings, such as the EU CyberNet´s mapping of ongoing projects of the EU member states, which could highlight gaps and potential opportunities for synergy and coordination. We would also like to point out the National Cyber Security Index

developed by the e-Governance Academy in Estonia which is an effective tool for national-level cyber security capacity assessment and development.

In order to accurately identify the exact need of recipient countries and build local ownerships of capacity-building projects it is important to engage countries in the early stages of the projects – this in turn will ensure the sustainability of our capacity-building efforts.

When it comes to capacity building mechanisms, Estonia believes that the Programme of Action (PoA) could become an important mechanism for promoting responsible state behaviour in cyberspace in an action-orientated manner, supported by capacity-building mechanisms. Estonia sees the potential in the PoA to building a pragmatic approach to coordinating capacity-building efforts and mapping as well as meeting capacity building needs of the developing countries.

This is why Estonia is also conducting capacity building projects through organisations such as the Estonian development cooperation agency EstDev in Africa, Asia, Latin-America as well as at home, in Europe. In addition, Estonia remains committed to organising multilateral capacity-building events on cyber diplomacy and international law. Estonia is currently working on organising the next Tallinn Summer School of Cyber Diplomacy – a training that also some of the delegates here today have benefited from.