Statement by Estonia at the first 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

General exchange of views, 13 December 2021

Delivered by Ms Britta Tarvis, Cyber Diplomacy Department, Ministry of Foreign Affairs of Estonia

Mr Chair,

Estonia aligns itself fully with the statement of the European Union. We would also like to deliver some remarks in our national capacity.

One of the phrases heard often during the first Open-ended Working Group and this morning was that we are not starting from scratch. It was this approach of aiming high but being grounded in previous achievements that led the group to success. On this occasion, as we embark upon the substantive work of the new OEWG, it is fitting to repeat this once again — even if to some it may sound like a familiar tune. It remains pertinent to recall that international discussions on the use of cyberspace in the context of international peace and security over more than the past decade have allowed us to elaborate and agree on a solid framework on responsible state behaviour in cyberspace, comprised of four concrete pillars: international law, voluntary norms, confidence-building measures and capacity-building. We regard the consensus reports agreed in the previous OEWG as well as the latest Group of Governmental Experts this spring as an overwhelming reaffirmation of this framework and believe their observations and recommendations offer a rich basis to build upon. We also welcome the adoption of the consensus resolution 76/19, co-sponsored also by Estonia.

Estonia is committed to engaging constructively and welcomes the practical focus the Chair is seeking to bring to our deliberations this week. We are positive that the contributions will form invaluable input for a programme of work for the group, to be adopted by consensus. Estonia would particularly like to highlight five areas on which the OEWG could focus.

First, we find that the OEWG is well placed to support states in deepening understanding on how the provisions of international law, including international human rights law and international humanitarian law, apply in cyberspace. Continuing such exchanges is clearly recommended by both the 2021 OEWG and GGE reports. We welcome that more countries have shared their positions on international law in recent months and encourage others to do so.

Topics for study could include the peaceful settlement of disputes, attribution and the law of state responsibility regarding internationally wrongful cyber operations, as well as the intersection of human rights and cybersecurity. The 2021 GGE report for the first time also mentioned international humanitarian law and as one specific topic for further study recommended established legal principles including
the principles of humanity, necessity, proportionality and distinction noted in the 2015 GGE report. This offers a clear opportunity for the OEWG. While we acknowledge that there is still wide scope to build consensus on how IHL applies in relation to cyber operations amongst all UN Member States, this should not preclude the OEWG from striving towards achieving a better acceptance and understanding of how IHL applies in cyberspace — to the contrary.

Second, the OEWG should support practical opportunities for the implementation of the 11 voluntary, non-binding norms of responsible state behaviour, set out in the 2015 GGE report and given an important additional layer of understanding in the 2021 GGE consensus. The OEWG could start by considering this rich material and how it can support states in following the norms. Furthermore, during the previous OEWG, several practical ideas emerged such as the national survey of implementation and the Programme of Action proposal. Estonia co-sponsors the PoA proposal and believes that the OEWG should remain seized on progress made with this initiative and provide an important additional venue to provide input for its imminent creation.

Third, cybersecurity demands a national and regional approach in order to be successful on a global level. Therefore, the regional dimension needs to play a key role in our work going forward. Allowing space to highlight the efforts of regional organisations — such as the OSCE, the ASEAN Regional Forum, the OAS — and sharing best practices on regional initiatives including confidence-building measures should be part and parcel of deliberations in the OEWG.

Fourth, both the latest OEWG and GGE discussions brought to the fore the importance and urgency of cyber capacity building and international cooperation. As a founding donor of the World Bank Cybersecurity Multi-Donor Trust Fund and one of the implementers of the EU CyberNet project, Estonia is eager to share lessons learnt and learn from others. In addition, the OEWG could help to identify and discuss the urgent capacity needs of states. We should also further discuss and support the implementation of the principles agreed in the previous OEWG report, such as the principle that capacity-building should respect human rights and fundamental freedoms and be gender sensitive and inclusive.

Last but not least, the OEWG should, to the greatest extent possible, harness the expertise of the multi-stakeholder community. Sustainable success cannot happen in siloes. The success of the OEWG is determined not only by how much we can advance consensus between states but also how it will involve the latest expertise and insight from the technical community at the heart of the open, free and secure cyberspace, international law practitioners, human rights experts, gender equality champions.

We look forward to our discussions over the coming week.

Thank you!