REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

Statement by Estonia at meeting 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 Existing and Potential Threats,
11 December 2023

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

Dear colleagues,

Cyber threat landscape has become more complex and challenging. In addition to financially motivated cyber criminals, State-sponsored cyber operations are on the rise. Several countries, including Estonia, are witnessing a steady rise in malicious cyber operations targeting public and private targets alike. Additionally, we can observe the increasing occurrence of ideological hactivism as a global phenomenon. This has an effect on national security and international stability as well as the way our societies operate. We are reminded that open, secure, stable, accessible and peaceful ICT environment cannot be taken for granted and we must work on bolstering cyber resilience on domestic, regional and global levels.

Estonia is carefully monitoring the threat landscape and we welcome an open exchange of views on the existing and potential threats and possible cooperative measures to prevent and counter such threats. We continue to be concerned by advanced persistent threats, ransomware and supply chain attacks among others. In the aftermath of the ongoing Russia's illegal aggression in Ukraine, the protection of critical infrastructure and services as well as safeguarding the security of democratic processes such as elections is our utmost priority. On 7 December 2023 we, among many others, have supported the United Kingdom in condemning Russia for their attacks against the UK's democratic processes. The international community must not accept behaviour breaching the obligations stemming from international law and norms of responsible State behaviour.

Part of the OEWG discussions focus on how to prevent and counter cyber threats. Estonia believes that these discussions are increasingly relevant for all the countries in the world. Based on our own experience, we have learned that effective prevention and mitigation of cyber

threats can not be founded merely on one-off campaigns and trainings. Instead, this effort must be systematic and persistent. In order to enhance cyber resilience, we need to adopt a holistic view to cyber threats and keep in mind that an effective response depends on multiple aspects such as policy frameworks, crises management mechanisms, international cooperation, organizational aspects, legal frameworks, education and general awareness, etc. Cyber security implications must be kept in mind when building information systems, establishing organisations and designing domestic processes.

One of our priorities is also to conduct trainings and exercises for the providers of essential services and critical infrastructure as well as gather these providers for exchange of information and best practices. Our National Cyber Security Centre (NCSC) focuses on enhancing cyber security of the public sector and protecting critical infrastructure; as well as being the competent authority and contact point for cyber security for the purposes of the EU Directive on Network and Information Security. We see that in today's volatile security environment, we must all prepare for being a target of malicious cyber operations, and investing in prevention is more reasonable than having to deal with costly consequences.

Finally, I would like to underline that enhancing cyber security across the society is a long-term project which depends on the participation of different actors such as the public and private sector, academia and civil society. It is essential to nurture good cooperation and trusted partnerships within the domestic environment as well as with our international counterparts. In addition, we underline the value of training, cyber hygiene and awareness of the everyday user as well as the education of younger generations.

Thank you, Mr Chair.