REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

Statement by Estonia at inter-sessional 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,

7 December 2022

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

Dear colleagues,

While we discuss here in informal setting various topics, the threats remain real and do not turn into informal ones. As a segway to the previous session on CBMs, one way to build confidence is to follow the UN Charter. Let me refer to the SG who has emphasized that Russia's invasion of Ukraine is a violation of its territorial integrity and of the Charter of the UN. The illegal and unprovoked Russian invasion against Ukraine has clearly illustrated that cyber operations are employed to support military objectives and are part of the modern armed conflict. In addition to malicious cyber operations against Ukraine's critical infrastructure and essential services as well as disinformation campaigns we have seen an increase of politically motivated cyber operations by Russia also against countries that support Ukraine.

The rise of malicious cyber operations worldwide and their increasing complexity underline that the threat picture in cyberspace is dynamic. State and non-State actors, including terrorists and criminal groups, are constantly exploring new options to breach information systems, develop malware and disguise their activities, while also continuing to use previously successful methods. Threat actors keep on investing resources in cyber capabilities, learning from mistakes and updating their attack methods. This also includes replacing the infrastructure needed for conducting the attacks which has been exposed.

Estonia believes that security comes from information sharing and cooperation. In particular, States need to describe honestly the threats, different actors and their capabilities. Inter alia, it is very important to share information about security vulnerabilities, to learn from mistakes and keep the systems patched. Often, the consequences of the vulnerabilities depend on the speed

with which we act – whether we are able to patch them before criminals manage to exploit them. In particular, we need to describe honestly the cyber threats, threat actors and their capabilities.

Estonia regularly publishes overviews about ICT threats as well as an analysis with lessons learned from incidents occurring in Estonia. This includes reports and publications by the Estonian Information System Authority, Estonian Internal Security Service and the Estonian Foreign Intelligence Service. These documents are translated into English and publicly available. This is our contribution to transparency and common understanding in terms of threats that we are facing.

For example, according to the statistics, 35% of all the cyber incidents with an impact in Estonia included phishing. Another attack method which has received a lot of attention is ransomware which may potentially bring along serious consequences for both the public and private sector. Ransomware is of course very relevant today also on international scene, for example the recent attacks crippling the Costa Rica government in 2022. As another attack vector, let me bring out also viperware attacks against Ukraine during the ongoing Russian aggression.

Estonia has put a lot of effort over the years in building a comprehensive strategic approach for cyber security. National strategies are a prime tool for identifying domestic roles and responsibilities, outlining national priorities and challenges, building connections with other domestic policies as well as mapping relevant international processes. Estonian is currently in the process of reviewing its cyber security strategy and planning to publish an updated strategy in 2023.

Finally, we would like to reiterate that Member States have agreed that any use of ICTs by States in a manner inconsistent with their obligations under the framework of responsible State behaviour undermines international peace and security, trust and stability between States, and may increase the likelihood of future conflicts between States. Estonia calls upon Member States to upkeep their international commitments as well as take steps to bolster cyber security domestically which will feed into regional as well as global resilience.

Thank you, Mr Chair.