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,

6 March 2023

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

Dear colleagues,

Malicious cyber operations are on the rise worldwide and resilience against these threats form an essential part of national security. Open, secure, stable, accessible and peaceful ICT environment cannot be taken for granted; cyberspace is not something separate from the physical world. It is evident that increasing threats in the use of ICTs are leading to growing challenges, starting from negative effects on economic and social development, and ending with implications on national security and international stability. Therefore, Estonia welcomes an open discussion on the existing and potential threats and possible cooperative measures to prevent and counter such threats.

Estonia has continuously underlined during our last meetings how Russia's illegal and unprovoked 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 kinetic warfare, Ukrainian governmental authorities, critical infrastructure, local governments, the security and defence sector, and companies have been targeted in cyberspace. Equally, there has been an increase of politically motivated cyber operations against countries that support Ukraine.

In the Estonian systems, we have witnessed an unprecedented number of denial-of-service attacks against Estonia, mostly guided by political motives. Phishing continues to account for the largest proportion of incidents recorded by CERT-EE. For us, protection of critical infrastructure and services as well as safeguarding the security of democratic processes such as elections is an utmost priority. Another threat vector very relevant in the international context is the increasing number of ransomware attacks which may also be targeted against critical infrastructure providers and hence bring along devastating effects. We have witnessed how for some countries ransomware attacks have constituted a state of national emergency, therefore, we hope to see the issue of ransomware reflected also in the next Annual Progress Report.

How to prevent and counter such threats? With the goal of information sharing and developing a deeper understanding of the threats, Estonia regularly publishes overviews about ICT threats as well as an analysis with lessons learned from incidents occurring in Estonia. For example, several reports and publications by the Estonian Information System Authority, Estonian Internal Security Service and the Estonian Foreign Intelligence Service are translated into English and publicly available. In order to enhance resilience domestically, Estonia has introduced new tools that provide better protection against attacks, increased monitoring capabilities, and developed capabilities for timely incident response. 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. We must constantly be ready for new cyber incidents, analyse ongoing threats, counter them, draw conclusions, and take the necessary steps to minimise their impact. Equally, we underline the value of education, cyber hygiene and awareness of the everyday user. The faster technology develops, the more extensive the attacks become, and the more resilient and capable our defences must be.

Finally, we would like to underline that any use of ICTs by Member 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 conflicts between States.

Thank you, Mr Chair.