REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

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

Discussion under agenda item 5 in relation to norms, 15 December 2021

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

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

In response to your guiding questions related to norms, Estonia wishes to express the following.

As a nation that has benefited immensely from digital transformation, Estonia knows first-hand the advantages of an open, free, interoperable and secure cyberspace and its responsible use. Digital services, including governmental e-services, are used widely in Estonia because trust towards them and the service providers is high. This has been enabled by several factors: 1) a long-term commitment to building a secure and transparent digital society where respect for human rights and fundamental freedoms such as the right to privacy is not an afterthought but ingrained from the very start, 2) a holistic approach to cybersecurity, 3) a stringent emphasis on preventing and mitigating risks, 4) raising awareness and enhancing cyber hygiene, and 5) endeavouring never to rest on our laurels.

However, the surge in the number and sophistication of the malicious use of cyberspace, their possibility for widespread impact, including on critical infrastructure, and the potential ramifications for international peace and security remain of real concern.

Mr Chair, esteemed colleagues,

As has been emphasised multiple times during this substantive session, the work of the UN Groups of Governmental Experts (GGE) since 2004 has allowed to outline and agree on a solid and effective framework for responsible state behaviour in cyberspace. This consists of existing international law, eleven voluntary non-binding norms, confidence-building measures and capacity building. It has also been noted by many other delegations that all these elements of this framework are interlinked but we will focus for now on norms. The 2015 GGE consensus report, building on previous GGE reports, made headway by setting out eleven voluntary non-binding norms of responsible state behaviour in cyberspace including several norms pertaining specifically to critical infrastructure protection. The 2021 consensus report furthermore reaffirmed the *acqui* and provided an important additional layer of understanding to these norms. While highlighting that norms do not replace or alter States' obligations or rights under international law, but rather supplement and support them, Estonia considers that adherence to these norms can help prevent conflict in the ICT environment,

reduce risks to international peace, security and stability and provide essential guidance for responsible state behaviour in cyberspace.

Estonia regards the agreed normative framework as a crucial footing for everything we do in the field of cybersecurity but given the lack of borders in the traditional sense in cyberspace, we also rely on this commitment to responsible behaviour, both in word and action, from other actors. Building on the rich material provided by the latest GGE report, the OEWG can play a crucial role in strengthening the eleven norms by further clarifying the expectations that the norms reflect and exploring further opportunities to support states in its implementation.

We have listened carefully to the interventions made during the discussion so far. Estonia believes that as a matter of priority, the international community needs to make a concerted effort to implement the existing norms, together with other aspects of the framework. While we appreciate the temptation of the new, we believe that the most appropriate course of action need not be the one that is the most tempting — it needs to be the one that ensures transparency, flexibility and scalability. This approach — focused on behaviour, rather than technology in itself — is appropriate in our view for reasons outlined by a number of delegations already.

One concrete example includes discussions that would contribute to the further development of the national survey of implementation of the UN General Assembly Resolution 70/237, which emerged as one practical outcome from the latest OEWG and GGE reports at the initiative of Australia and Mexico, or other such initiatives that allow to identify existing efforts and needs for norm implementation. Supporting states in reporting their implementation efforts through better utilising existing resources such as UNIDIR could prove invaluable. We also emphasise the importance of bringing in the regional dimension wherever possible to support the development and operationalisation of confidence-building measures, with the aim to support norm implementation.

While all eleven norms are important and form a sufficient package, given the urgency of preventing damage to critical infrastructure stemming from malicious cyber activities, we welcome that the Chair's guiding questions raise specifically initiatives related to the norms pertaining to critical infrastructure protection.

Supported by a stringent legislative basis and a broad definition of essential services, Estonian authorities have close communication and information exchange with essential service providers. Our national cybersecurity centre, the Estonian Information System Authority, offers free of charge security tests to essential service providers, facilitates the exchange of best practices and offers advice to the private sector. Penetration testing such as to the healthcare sector and the energy sector help to keep standards high. We believe that the OEWG could provide a helpful space to share best practices and lessons learnt related to

critical infrastructure protection, including on topics such as public-private partnerships mentioned also by other delegations such as Switzerland.

Mr Chair,

One of the key issues under focus during this week has been the engagement of the multistakeholder community. We want to stress our deepest gratitude and support to you in your efforts to find a solution on this matter swiftly and support the updated modalities you put forward for consideration at the informal consultations yesterday evening.

Estonia also welcomes your question on the role of the private sector and the technical community in norm implementation. We believe that while the norms pertain to state behaviour, the effective implementation of norms make close cooperation with other stakeholders indispensable. We believe that the role of different stakeholders should be further elaborated, with the aim of advancing common understandings on respective responsibilities and providing future guidance. The contributions from the technical community will be particularly important to help us to identify the most pertinent areas. It will also be important to take into account gender considerations in cybersecurity. In this regard, we welcome the options paper submitted by Canada which provides a very constructive menu of options for mainstreaming gender in the work of the OEWG.

We look forward to continuing conversations on how to implement the existing norms, including through capacity building — and initiatives that support it — which will be under focus later this week.

Thank you, Mr Chair.