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 International Law,

7 December 2022

Thank you, Mr Chair for giving me the floor.

We align with the EU's position and would like to make additional remarks in our national capacity.

Dear colleagues,

Russian Federation continues to blatantly violate international law by its military aggression against Ukraine. Russia's unjustified military aggression against Ukraine has been accompanied by a significant increase of malicious cyber activities, including targeting critical infrastructure and conducting information campaigns. The international community must hold Russia accountable for its shockingly cruel and violent behavior in Ukraine.

Estonia stresses that the use of cyber operations during armed conflict is subject to the rules and principles of IHL just like the use of any other weapons, means and methods of warfare. Leaving cyberspace outside the scope of IHL rules would leave civilians, civilian infrastructure and combatants without an additional layer of protection.

The international community needs now more than ever to join forces to strengthen the international rules-based order also through adhering to international law in cyberspace. We need more state practice in implementing international law which will also provide more clarity on any potential gaps, if any, or differences in interpretation that need to be addressed. Therefore and based on the previous consensus outcomes of the UN GGEs and OEWG, Estonia supports further discussions on how international law applies in cyberspace. This includes, inter alia, IHL and human rights law, and customary law such as the Articles for Responsibility of States for Internationally Wrongful Acts.

We have carefully considered the Concept Paper by Canada and Switzerland and find that this could serve as a good basis for moving forward. The topics proposed in that Concept Paper are in line with what Estonia has proposed at the first substantive session of this Working Group. We continue to believe that the discussions at this OEWG could focus on the topics of Peaceful Settlement of Disputes, building on the UN Charter, State Responsibility and IHL. Estonia reiterates that humanity, necessity, proportionality and distinction are fundamental principles of IHL and must be followed. Underscoring that these principles by no means legitimise or encourage conflict, the OEWG should further study on how these principles apply to the use of ICTs by states.

Estonia supports awareness raising and capacity-building efforts in the domain of international law. We believe that capacity building is not a one-time effort but needs to address the needs of different countries as well as take place continuously to address the rotation of national experts. In addition to OEWG efforts, regional organisations and individual countries can play a relevant role in providing platforms for multilateral discussions. For example, Estonia is organising a series of Tallinn Workshops on International Law and Cyber Operations with the main objective to create a forum for informal discussions between partners as well as offer the opportunity to examine the most pertinent international law issues related to State conduct in cyberspace.

Additionally, Estonia sees merit in academic projects such as Tallinn Manual 3.0 which is aimed at objectively restating international law as applied by States in the cyber context. The project is currently looking forward to receiving feedback for Tallinn Manual 2.0. Formal State engagement for Tallinn Manual 3.0 is expected to start at 2025. We also underline the added value of scenario-based legal analysis which allows to move further than theoretical discussions. A relevant example in this domain is the NATO Cooperative Cyber Defence Centre of Excellence Cyber Law Toolkit which consists of 25 scenarios complemented with legal analysis, available online.

Thank you, Mr Chair.