SUMMARY OF ESTONIA'S POSITION

ON HOW INTERNATIONAL LAW APPLIES IN CYBERSPACE

1. **International law applies to state behaviour in cyberspace.** The rights and obligations set out in international law, including the UN Charter, apply to the use of ICTs by states. This means that international law applies to relations between states in cyberspace as it does in the conventional domains of state interaction. The Tallinn Manual on the International Law Applicable to Cyber Operations is a sound point of departure for states when they wish to analyse their possible national positions on how international law applies in cyberspace.

2. **States are responsible for their activities in cyberspace.** State sovereignty entails not only rights, but also obligations. States are accountable for their internationally wrongful cyber operations just as they would be responsible for any other activity according to international treaties or customary international law. State responsibility applies regardless of whether such acts are carried out by states or by non-state actors directed or controlled by the state. States cannot waive their responsibility by carrying out malicious cyber operations via non-state actors. In addition, it is paramount that states respect the agreements of the UN Groups of Governmental Experts in regards to their conduct in cyberspace reflected in their consensus reports on international law and voluntary non-binding norms of responsible state behaviour.

3. **States have to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states.** Such easonable efforts are relative to national capacity as well as availability, and the accessibility of information. Meeting this expectation encompasses taking all feasible measures in order to end the ongoing malicious cyber activity. States should strive to develop means to offer support when requested by the injured state in order to identify, attribute or investigate malicious cyber operations.

4. **States have the right to attribute cyber operations both individually or collectively according to international law.** In order for a cyber operation to be considered an internationally wrongful act, it must be attributed to a State. Attribution is a political decision and requires assessing technical information and relevant information from other sources to determine whether the legal criteria for attribution are met. In addition to the technical information, such assessment may take into account, as appropriate on a case-by-case basis, the wider political and economic context, established behavioural patterns and other relevant information and indicators. What is required from the attributing state is not an absolute certainty but what is reasonable.

5. **States have the right to respond to malicious cyber operations, including using diplomatic measures, countermeasures, and, if necessary, their inherent right of self-defence.** Cyber operations that cause injury or death to persons, damage, or the destruction of objects could amount to the use of force or an armed attack under the UN Charter. The increasing digitalisation of our societies and services may amplify the harmful effect of a cyber operation. Estonia is very much dependent on a stable and secure cyberspace. Consequently, malicious cyber operations targeting essential digital infrastructure or services necessary for the functioning of the society may induce harmful effects. In order to prevent such effects, states maintain all rights, in accordance with international law, to respond to harmful cyber operations either individually or in a collective manner. Among other options for collective response, Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation. These countermeasures should follow the principle of proportionality and other principles established within the existing international customary law.