Estonia's Contributions to the GGE

30 September 2014

For Estonia, international cyber security is a guarantee of advancing democracy, human rights and fundamental freedoms. It is paramount to further the social and economic growth made available by Information and Communication Technologies (ICTs) and support Internet freedom.

1. Views on International Law

Estonia emphasizes the position taken by the 2013 GGE that international law is applicable to cyberspace and pertains to the uses of ICTs by States. In our view, it is necessary to analyze the application of both peacetime norms and international humanitarian law in the context of uses of ICTs that relate to national and international peace and security. These efforts should be complementary with the ongoing work addressing other issues, such as cybercrime, cyber terrorism, human rights, and internet governance, by other international organizations and forums.

International law relevant to uses of ICTs that relate to national and international peace and security resides in numerous treaties, which, albeit not explicitly adopted in response to the developments and requirements of the information age, by their object and purpose nevertheless govern cyberspace and State activities therein. Similarly, existing norms of customary international law apply to State conduct in cyberspace. Other norms of responsible State behavior may derive from accepted practices relating to uses ICTs.

Reaffirming the conclusions of the UN GGE 2013 report, we underline the need to address the question of how existing international legal norms are to be interpreted in the cyber context. Cyberspace has unique characteristics compared to other domains and kinetic activities. Such characteristics should not be viewed as impediments to the application of international law. Instead, they suggest the need for a more detailed analysis of the preconditions for, and implications of, the implementation of relevant norms. Therefore, Estonia urges the GGE members and other States, individually and cooperatively, to study, analyze and discuss how international law is to be applied. To that end, Estonia has supported the work of different academic groups in order to ascertain diverse expert views on this matter. Estonia is ready to further cooperate with governments and other experts to develop views on the application of international law to cyberspace and State actions therein.

2. Recommendations on Responsible State Behavior

Estonia has chosen to use ICTs as a tool for public and private sector efficiency and development and set up a national ICT infrastructure. As the functioning of the ICT

infrastructure is of existential importance, Estonia has developed practices at a national level to protect it. In addition to national efforts, international cooperation is required for the prevention and mitigation of threats and attacks against it.

Deriving from Estonia's experience in the field of cyber security we propose to discuss and aspire to achieve a common understanding on the following accounts:

2.1 Protection of critical financial infrastructure

Potentially the most harmful cyber attacks are those targeted against a nation's critical infrastructure and associated information systems. Failures of, or disruptions to, critical information systems may impact extensively upon the normal functioning of society with potentially disastrous consequences. Therefore it is vital to enhance international co-operation and mutual assistance for the purpose of critical information infrastructure protection.

In our view, the protection of ICT-based or ICT-dependent critical infrastructure subject to State's jurisdiction constitutes responsible State behavior. In the spirit of UN Resolution 58/199 States are encouraged to define their nationally critical infrastructure, assign responsible institutions and develop protection measures, including comprehensive national crisis preparedness and response procedures. In addition, States should facilitate cross-border cooperation to address vulnerabilities of critical information infrastructure transcending national borders.

While we consider it necessary to continue developing practices on the protection of all types of critical infrastructure, we would like to focus particularly on the issue of stability and security of the financial system, which we consider to be in the interest of all States due to its centrality for the functioning of individual economies as well as the global economy as a whole. Due to interdependencies, attacks against individual financial institutions as well as financial services can cause extensive damage and reduce public trust toward the digital economy.

Therefore, Estonia considers it essential for States to take steps to reduce potential damage resulting from cyber attacks against the financial system as an essential enabler of economic and social stability.

2.2 Cooperation in incident response

Cooperation between national institutions with computer incident response responsibilities, such as CERTs and CSIRTs, is one of the most important preconditions for preventing as well as solving both domestic and international cyber incidents.

States have developed commendable practice in CERT cooperation, such as information exchange about vulnerabilities, attack patterns, and best practices for mitigating attacks. We invite the GGE to support this practice and encourage its

expansion. This includes supporting the handling of ICT-related incidents, coordinating responses, and enhancing regional and sector-based cooperation practices.

2.3 Mutual assistance in resolving cyber crises

Considering the cross-border nature of cyber threats, States should assist other States in resolving cyber crises, particularly by mitigating ongoing incidents. This would build confidence that cyber crises will not be unnecessarily escalated as well as an expectation of reciprocation in the future.

The group should consider types of assistance to be expected and provided. Further mechanisms include creating procedures for expedited assistance, organizing relevant national and regional exercises to enhance preparedness for handling real incidents and promoting relevant implementation practices of existing multi- and bilateral agreements.

3. Views on Capacity Building

Enhanced capacity building and awareness raising in cyber security helps to improve means and methods to counter cyber threats. We deem it necessary to provide assistance and cooperation to technologically less developed countries in order to enhance their cyber security capabilities. Estonia is prepared to contribute to relevant programs and activities, including risk analysis, training, education, information exchange and research and development.