Response to the General Assembly resolution 70/237 on "Developments in the field of information and telecommunications in the context of international security"

Executive summary

Estonia recognizes that the security in the cyber world has become a very important issue in the context of wider international security. Therefore, the role and involvement of the UN is getting increasingly relevant.

The security on the Internet has been one of the high priorities of the Estonian Government. The main guiding document on this issue is the National Cyber Security Strategy (2014-17). The Cyber Security Council of the Security Committee of the Government supports strategic level inter-agency cooperation and overseeing the implementation of Cyber Security Strategy objectives. The NATO Cooperative Cyber Defence Centre of Excellence was established in Tallinn, capital of Estonia and as of May 30th 2017, the CCDCOE has 20 contributing member states.

Estonia is convinced that the broad use of digital services demands a high level of cyber security. For Estonia, socio-economic and politico-military aspects of cyber security are intertwined. We consider it elementary that countries abstain from attacking national critical infrastructure. We also call for a responsible behaviour towards global communications infrastructure to promote access to information and trust towards ICTs. We consider it a responsibility of every country to draft and enforce national laws that help control malicious uses of ICTs by non-state actors and to seek ways to better formulate, disseminate and promote responsible and active cyber policy, respective narratives and argumentation.

Estonia is a member of the Group of Governmental Experts on the Developments in the Field of Information and Telecommunication in the Context of International Security for the fourth consecutive time. The GGE has been a very productive format of work. In future, it could be a useful instrument in not only studying the cyber threats and possible remedies, but also how different countries apply the existing international law and norms, rules and principles. In Estonia’s view, the GGE should continue its work on advancing dialogue among Member States, which facilitates the exchange of information and best practices. In addition, the GGE should discuss practical cooperation measures and mechanisms to advance Member States capacity building, with the ultimate goal to equip Member States with competence and capacity to tackle all aspects of Internet challenges.

It is important to take forward the progress achieved at the 2014/2015 UN GGE by further promoting norms of State behaviour that support openness, accountability and other democratic
values in cyber space. Estonia hopes to see yet another consensus report of the GGE in June 2017.

General appreciation of the issues of information security:

Estonia values highly the work done so far by the GGE and is proud to contribute to the work of the expert group with our high-level expert H.E. Ms. Marina Kaljurand. Estonia recognizes that the security in the cyber world has become a very important issue in the context of wider international security. The role and involvement of the UN is getting therefore increasingly relevant. We believe it is necessary to raise the awareness of all United Nations members regarding the nature and importance of cyber security as an issue that affects not only technologically advanced nations, but the entire world. Estonia emphasizes that simultaneously with the discussion on the Internet security the same amount of attention should be dedicated to the freedom of expression in the Internet. The Internet must be not only secure but also free.

Efforts taken at the national level to strengthen information security and promote international cooperation in this field:

In Estonia, the main guiding document on this issue is the National Cyber Security Strategy (2014-17). This is our second national strategy and we have recently started working on the third. Concerning internal oversight, as an inter-agency body, the Cyber Security Council of the Security Committee of the Government is supporting strategic level inter-agency cooperation and overseeing the implementation of Cyber Security Strategy objectives.

The Emergency Act (2009) provides the legal basis for crisis management, including emergency preparation and response, as well as ensuring the continuous operation of vital services. The Government has also established a national (technical) body named Computer Emergency Response Team (CERT) responsible for dealing with identification and mitigation of cyber/ICT security incidents.

Concerning international cooperation to achieve regional/international cyber/ICT security and stability between States, in our view, on an operational basis, CERT/CSIRT co-operation is the most functional. As a platform to address the issues and to raise awareness/ support in case of large-scale problems, relevant international/ regional organizations have their role to play.

European Union’s frameworks and other international documents are relevant for our policies, we are actively engaged in drafting the second European Union Cyber Security Strategy to be introduced in September 2017 and are focusing internally on the implementation of the European Union Network, and Information Systems (NIS) Directive introduced in August 2016.

The security on the Internet has been one of the high priorities of the Estonian Government. The NATO Cooperative Cyber Defence Centre of Excellence was established in Tallinn, capital of Estonia and as of May 30th 2017, the CCDCOE has 20 contributing member states.

Possible measures that could be taken by the international community to strengthen information security at the global level:

Considering the important goal of ensuring a free, open and secure Internet, Estonia is proud to host the European Dialogue on Internet Governance (EuroDIG) in Tallinn in June 2017. EuroDIG is - as the Internet Governance Forum (IGF) is an open network for the discussion and
exchange of ideas on emerging issues and challenges concerning our digital environment. It is a platform involving all stakeholders: governments, international organisations, technical community, businesses and civil society. Since its inception in 2008 the inclusive and continuous dialogue, which culminates in an annual event, has taken place in a different European country every year. The programme planning process is open to all interested European stakeholders. The results of the Dialogue are conveyed in the form of ‘Messages’ to the annual global IGF, which this year will take place in Switzerland.

Cyber Operations have become an integral part of international relations - the recent launch by the CCDCOE of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations is a practical handbook for state legal advisers of how to deal with these issues and should in our view be taken into consideration.

Estonia is convinced that the broad use of digital services demands a high level of cyber security. We consider it elementary that countries abstain from attacking national critical infrastructure. We also call for a responsible behaviour towards global communications infrastructure to promote access to information and trust towards ICTs. We consider it a responsibility of every country to draft and enforce national laws that help control malicious uses of ICTs by non-state actors and to seek ways to better formulate, disseminate and promote responsible and active cyber policy, respective narratives and argumentation.

**The content of the concepts mentioned in paragraph 2 (of the resolution):**

Turning back to the UN, Estonia is a member of the Group of Governmental Experts on the Developments in the Field of Information and Telecommunication in the Context of International Security – the GGE for the fourth consecutive time. The GGE has been a very productive format of work. In future, it could be a useful instrument in not only studying the cyber threats and possible remedies, but also how different countries apply the existing international law and norms, rules and principles. For Estonia, international law is the biggest authority, also in the use of ICTs. We therefore strive for clarity and certainty of norms as it not only reduces the risk of intolerable practices, but also provides transparency and predictability of behaviour that allows us to focus on peace rather than on conflict.

In Estonia’s view, the GGE should continue its work on advancing dialogue among Member States, which facilitates the exchange of information and best practices. In addition, the GGE should discuss practical cooperation measures and mechanisms to advance Member States capacity building, with the ultimate goal to equip Member States with competence and capacity to tackle all aspects of internet challenges.

It is important to take forward the progress achieved at the 2014/2015 UN GGE by further promoting norms of State behaviour that support openness, accountability and other democratic values in cyber space. For Estonia, such goals include unrestricted access to the Internet, protection of human rights and freedoms as well as improved cyber security by attitude, design and competence, Estonia hopes to see yet another consensus report of the GGE in June 2017.

Lastly, Estonia would like to reiterate the importance of the effective implementation of the Budapest Convention on Cybercrime that would ensure that national legislations provide appropriate sanctions for cases involving serious attacks, including terrorist attacks on IT-based or IT-general infrastructure.