Statement by Finland
UNGA72 First Committee 2017
Thematic Debate: Other Disarmament Measures and International Security

Statement by
Ambassador Marja Lehto
Ministry for Foreign Affairs of Finland

New York, 23 October 2017

(check against delivery)
Mr Chairman,

Finland fully aligns itself with the statement of the European Union.

There is a need for a broader agreement on how to address cyber threats in a changing global security environment. The challenges are increasingly complex: internal and external security threats are intertwined, and the same applies to the physical and digital aspects of security as well as to the safety and security of individuals and societies. Cyber security, as this Committee has recognized, may also pertain to international peace and security.

The United Nations has played an important role in promoting dialogue on different aspects of the use of information and communication technologies. The 2013 and 2015 Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security have considerably advanced the normative discussion on cybersecurity. The 2013 GGE Report affirmed that international law, and in particular the UN Charter, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. The 2015 Report added that the UN Charter applies in its entirety. These statements have been important reminders of the backdrop of general international law against which all new technologies and their uses have to be assessed.

Finland regrets that consensus was not within reach in the most recent GGE. International discussions on specific aspects of international law in relation to the use of ICTs will nevertheless continue, and should be encouraged. This applies, for instance, to International Humanitarian Law in view of the fact that cyber means are already being used in armed conflicts. Furthermore, exchange of views is needed on serious cyberattacks below the threshold of an armed attack: both concerning their prevention and the tools available to States that have been victimized by such attacks. With regard to questions of the use of force, I would recall the statement of the 2005 World Summit that the Charter provisions on the use of force provide a sufficient basis to address any security threat. More comprehensive assessments of international law in relation to cyber activities have been presented by academic scholars, most notably by the two International Expert Groups that prepared the 2013 and 2017 Tallinn Manuals.

The GGE’s recommendations on responsible State behaviour have been welcomed by the UN General Assembly, which called upon States to ‘be guided in their use of information and communication technologies by the 2015 [GGE] Report.’ These recommendations continue to deserve our attention. They outline standards as to what states should do at the national level and how they should cooperate with each other, for instance, to protect the critical infrastructure, ensure the integrity of the supply chain, or to prevent the proliferation of malicious ICT tools and techniques and to share information. It goes without saying that such recommendations are without prejudice to the rights and obligations of States under international law. At the same time, they can be seen as a practical contribution to the clarification of what ICT-specific steps States should take to comply with their obligation not to knowingly allow their territory to be used for activities that may cause significant harm to other States.

Developments in the field of cyber security are fast, complex, and hard to predict. This does not only mean that cybersecurity deserves our attention, but also that it is necessary to be cyber smart in order to keep up with the changes of the global security environment. Development of resilience is essential worldwide, and should be supported by appropriate capacity-building efforts.
In order to meet the challenges related to cybersecurity, it is also of utmost importance to build confidence among States. In this regard, I would like to emphasize the role of regional organizations. For instance, the Organisation for Security and Cooperation in Europe (OSCE) has done important work within this area by adopting a set of dedicated confidence-building measures. Now it is the time to emphasize the implementation of the agreed measures.

To conclude, I wish to recall that an open, secure, stable, accessible and peaceful ICT environment can only be built on full compliance with international law.

Thank you, Mr Chairman