EU Statement

By

Ms. Judit Körömi
Chair of the EU Working Party for Non-Proliferation (CONOP)
European External Action Service

UN General Assembly 72nd Session
First Committee Thematic Discussion on
Other Disarmament Measures and International Security

United Nations
New York
23 October 2017
Mr. Chairman,

1. I have the honour to speak on behalf of the European Union. The Candidate Countries Turkey, the former Yugoslav Republic of Macedonia*, Montenegro* and Albania*, the country of the Stabilisation and Association Process and potential candidate Bosnia and Herzegovina, as well as Ukraine, the Republic of Moldova and Georgia, align themselves with this statement.

2. The EU and its Member States recognise the role of the United Nations in further developing frameworks for responsible state behaviour in cyberspace. The EU commends the efforts of the consecutive United Nations Groups of Governmental experts on Developments in the Field of Information and Telecommunications in the Context of International Security to advance understanding of the application of international law, norms, rules and principles of responsible behaviour of States, and promote confidence building measures, as well as capacity for the use of Information and Communication Technologies (ICTs).

3. The EU emphasises that UN Groups of Governmental Experts, over the years, have reached consensus on a number of views contributing to greater cyber stability, including that the UN Charter applies in cyberspace. The EU recalls the outcomes of the Group of Governmental Experts discussions, which the General Assembly has repeatedly endorsed, and important recommendations that States should fully implement. The EU regrets that the GGE of 2017 did not reach consensus on an additional report but will continue to implement the consensual views articulated in previous GGE reports, and invites other international actors to do so.

4. The EU will continue to promote the establishment of strategic frameworks for conflict prevention, cooperation and stability in cyberspace. Such frameworks must be based on the application of existing international law, and in particular of the UN Charter in its entirety. The EU reaffirms that "International law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment." The EU supports the development and implementation of universal norms of responsible State behaviour, supported by targeted regional confidence building measures between States.

5. In this context, we emphasize the following which, inter alia, apply to State use of ICTs: sovereign equality; non-intervention in the internal affairs of other States; the obligation to settle international disputes by peaceful means in such a manner that international peace, security, and justice are not endangered; the right to respond, including by non-forcible countermeasures, to internationally wrongful acts committed through the use of ICTs; the obligation to refrain in international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; the inherent right to self-defence; and international humanitarian law, including the principles of precaution, humanity, necessity, proportionality and distinction.

6. The EU recalls, among others, the following norms in UN GGE reports: "States should respond to appropriate requests for assistance by another State whose critical infrastructure is

---

* The former Yugoslav Republic of Macedonia, Montenegro and Albania continue to be part of the Stabilisation and Association Process.
subject to malicious ICT acts emanating from their territory”, “States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs”, and “States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account, inter alia, General Assembly resolution 58/199 (2003) “Creation of a global culture of cybersecurity and the protection of critical information infrastructure “. The EU recalls that the 2015 GGE emphasized that States should guarantee full respect for human rights, including privacy and freedom of expression.

7. The EU supports and encourages the development of regional confidence building measures, which are an essential element to increase cooperation and transparency and reduce the risk of conflict. Implementing cyber security confidence building measures in the OSCE, ARF, OAS and other regional settings will increase predictability of state behaviour and further contribute to stabilising cyberspace.

8. In order to build trust and strengthen cooperation among States, as well as to implement the currently agreed cyber norms, the EU acknowledges the role of capacity building, and stands ready to provide necessary support. The EU is committed to address cyber threats globally by assisting third countries in responding to such threats and increasing law enforcement capabilities to investigate and prosecute cybercrime. The EU considers it essential to advance cyber security capacity building through the development of appropriate domestic policies or legislation, protection of infrastructure, provision of training as well as upholding the rule of law and respect for human rights in cyberspace.

9. Recognising the challenges posed by cyber threats, EU Member States have adopted a “Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities”. This Framework contributes to conflict prevention, cooperation and stability in cyberspace by detailing how measures within the Common Foreign and Security Policy, including restrictive measures, can be used to prevent and respond to malicious cyber activities. The measures within the Framework aim to protect the integrity and security of the EU, its Member States and their citizens, encourage cooperation, facilitate mitigation of threats and influence the behaviour of potential aggressors, both State and non-State actors, in the long term. By providing clarity on EU response to malicious cyber activities, the Framework contributes to international peace and security.

Mr Chairman,

10. In conclusion, the EU and its Member States reaffirm their commitment to better protect Europeans in the digital age, including respect for human rights and fundamental freedoms and to improve and strengthen security and stability in cyberspace. We call on all United Nations member States to apply existing international law, fully implement agreed cyber norms and advance the development and implementation of confidence building measures.

I thank you Mr. Chairman.