EU Statement

By

Ms. Anne Kemppainen
Minister Counsellor
Head of Political Section for Non-proliferation and Disarmament
Delegation of the European Union in Geneva

First Committee
Thematic Discussion on Other Disarmament Measures and International Security
United Nations General Assembly
74th Session

United Nations
New York
25 October 2019
Mr. Chair,

I have the honour to speak on behalf of the European Union.

The Candidate Countries the Republic of North Macedonia*, Montenegro*, and Albania*, the country of the Stabilisation and Association Process and potential candidate Bosnia and Herzegovina, as well as the Republic of Moldova and Georgia, align themselves with this statement.

The EU and its Member States underline the importance of an open, free, stable and secure cyberspace, where human rights and fundamental freedoms, the rule of law and international law are fully respected and upheld.

We reiterate our strong concerns about the malicious use of Information and Communications Technologies (ICTs) by States and non-State actors, which affects the entire world community, its peoples and businesses. Unfortunately, the scope and severity of such incidents appear only to be increasing, as are the costs and consequences associated with them. This could lead to destabilising effects, effectively threatening international peace and security.

In this context, the EU and its Member States are committed to engaging constructively in the ongoing UN discussions on cybersecurity in the context of the First Committee issues. Our objective is to work, both within the UN Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG), in a complementary and coordinated fashion, to advance and further build on the achievements of the previous UN GGEs, as endorsed by consensus by the UN General Assembly, notably in Resolution 70/237. We want to underline the EU’s and Member States’ commitment in supporting both the Chair of the GGE and of the OEWG in arriving at consensus outcomes.

In this regard, the EU and its Member States welcome the excellent interactive discussions at the first substantial session of the OEWG and we look forward to continuing this constructive work during the upcoming sessions. We welcome the growing interest of the international community in the debate and the acknowledgement that deliberations do not start from scratch, in particular the acknowledgement of the applicability of international law, in particular the UN Charter.

We recall that the mandate of the OEWG was created with a view to making the UN negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent. In this context, we foresee a role for all relevant stakeholders to have their voices heard, to exchange positions and foster a stronger common understanding on how to face threats in cyberspace.

---

* The Republic of North Macedonia, Montenegro and Albania continue to be part of the Stabilisation and Association Process.
The EU and its Member States are committed to engaging and supporting constructively the work of the UN GGE in advancing responsible State behaviour in cyberspace in the context of international security that reaffirms the consensus views articulated in previous GGE discussions. We welcome the consultations which are taking place with UN Member States, as well as with other stakeholders, notably regional organizations, such as the African Union, the European Union, the Organization of American States (OAS), the Organization for Security and Cooperation in Europe (OSCE) and the Regional Forum of the Association of Southeast Asian Nations (ARF).

Another practical, very important effort relates to cyber capacity-building.

The EU supports cyber capacity-building work through its External Financing Instruments, which encompass a range of programmes with a global reach. The EU is currently investing more than €100 million in cyber capacity-building activities worldwide, in cooperation with its implementing partners, through projects such as EU’s Cyber-Resilience for Development, Glacy+ and EU Cyber Direct. The EU looks forward to deepening its cooperation with UN Member States in this regard.

These efforts are also contributing to bridging the digital divide and achieving the Sustainable Development Goals (SDGs). Indeed, we cannot imagine that ICTs can support the SDGs if there is no trust and confidence.

Mr. Chair,

We reaffirm our full support for the ‘strategic framework’ for conflict prevention, cooperation and stability in cyberspace, endorsed by the UN General Assembly. Promoting this framework is a long-standing priority for the EU and its Member States. The framework is based on the application of existing international law, in particular of the UN Charter in its entirety, international humanitarian law, international human rights law and fundamental freedoms, complemented by the implementation of norms of responsible state behaviour, regional confidence-building measures between States, and supported by capacity-building efforts. The confirmation of the application of international law in cyberspace by all States, as well as explanation of how they consider this law applies, will help achieve progress in the UN discussions, whilst denial could undermine ongoing practical efforts to tackle the real, pertinent and pressing problem of increasing cyber incidents.

The EU and its Member States at this moment neither call for nor see the necessity for the creation of new international legal instruments for cyber issues.

We strongly encourage focusing our collective efforts on building on the work repeatedly endorsed by consensus by the UN General Assembly, notably in Resolution 70/237, to further raise awareness, build common understanding, exchange best practices, and support and advance effective implementation of these agreed norms and confidence-building measures which offer
the greatest added value for conflict prevention. These norms create expectations for responsible State behaviour and allow the international community to assess the activities and intentions of States in order to prevent conflict and increase stability and security.

In order to further advance the accountability in cyberspace, the Council of the EU in 2017 established a framework for a joint EU diplomatic response to malicious cyber activities – the so-called Cyber Diplomacy Toolbox. This allows the EU, inter alia, to impose targeted restrictive measures to discourage and respond to cyber-attacks and contribute to conflict prevention, cooperation and stability in cyberspace by detailing how measures within the EU’s Common Foreign and Security Policy 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.

Complementing the norms for responsible State behaviour, the EU and its Member States underline the importance of confidence-building measures, their development and their implementation, in the OSCE, ARF, OAS and other regional frameworks, and support further exchanges on the confidence-building measures which have been developed in particular by the OSCE.

Mr. Chair,

We encourage all States to recognise their responsibility in advancing the implementation of the above-mentioned norms of responsible State behaviour and confidence-building measures as repeatedly endorsed by the UN General Assembly. The EU looks forward to further cooperation with all stakeholders, including governments, private sector, technical community, users and academia towards strengthening the strategic framework for conflict prevention, cooperation and stability in cyberspace.

Thank you, Mr. Chair