final

EU General Statement

OEWG on cyber, First Session

New York, 9 September 2019

Mr. Chairman,

I have the honour to speak on behalf of the European Union and its Member States.

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 recognise that cyberspace, in particular the global, open and interoperable Internet, has become one of the backbones of our societies. We underline the importance of a global, open, stable and secure cyberspace, where human rights and fundamental freedoms, rule of law and international law fully apply, as it supports societal well-being, sustainable and inclusive economic growth and prosperity.

The EU and its Member States reiterate their concerns about the malicious use of Information and Communications Technologies (ICTs). Misusing ICTs for malicious purposes 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. The EU and its Member States are concerned that these incidents could lead to destabilising and cascading effects, threatening international peace and security.

In this light we see the increased attention devoted to cyber matters at the UN as an opportunity to further build on the work in the UN over recent years to advance peace and stability in cyberspace. This forum offers the UN Membership the opportunity to strengthen common understanding and support for further implementation of the norms, rules and principles as endorsed by the General Assembly on multiple occasions. We are committed to working within both the OEWG and the GGE to advance cyber stability and openness, and welcome close coordination between the two bodies.

Indeed, we are not starting from zero. Notably, past GGE reports, which were endorsed by consensus by the UN General Assembly, have established a 'strategic framework' for responsible state behaviour. The EU and its Member States are committed to promoting, further advancing and implementing this framework. Implementation by the entire UN community would significantly advance cyber stability. As such, we believe that the

---

* *The Republic of North Macedonia, Montenegro, Serbia and Albania continue to be part of the Stabilisation and Association Process.*

OEWG could add most value by providing a forum for addressing the most pertinent issues in this regard. This includes raising awareness around, building common understanding on, and supporting and advancing effective implementation of the rules, norms and principles of responsible State behaviour, as well as advancing confidence building measures and global cyber resilience through cyber capacity building.

With this in mind, we welcome the breadth and relevance of the programme of work as proposed by the Chair, as it includes several important work streams that have been undertaken, including the work on cyber capacity building – which has been a long-standing priority for the EU and its Member States.

Mr. Chairman,

The EU and its Members States underline their full support to the 'strategic framework' for conflict prevention, cooperation and stability in cyberspace as endorsed by the General Assembly. The framework is based on the application of existing international law, and in particular of the UN Charter in its entirety, complemented by the development and implementation of universal norms of responsible state behaviour, regional confidence building measures between States, and supported by capacity building efforts.

The strategic framework reminds us that despite the many challenges associated with ICTs, cyberspace is not lawless domain. Rule of law and international law fully applies to cyberspace, and denying this may encourage miscalculation, erode accountability for actions and in result contribute to increased instability in cyberspace.

In addition, these norms that exist to guide the behaviour of States in cyberspace reflect an agreed consensus and shared expectations of the international community. These norms set standards 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.

One of the key opportunities before us is now to build on this work to advance peace and stability in cyberspace. By doing so, we firmly believe that we will not only allow our societies and economies to benefit from open, free, secure, peaceful and accessible ICT environment, but we will also advance peace and stability in cyberspace. In this regard, I take this opportunity to note that all EU Member States have supported the Paris call for Trust and Security in Cyberspace, launched in November 2018.

Mr. Chairman,

The EU and its Member States recognize that cooperation through effective multilateralism remains the best way to advance national as well as collective interests. We strongly support an effective multilateral system, underpinned by a rules-based international order, which delivers results in tackling present and future global challenges in cyberspace. We look forward to engaging in the OEWG in a spirit of consensus and mutual respect to that end.

International law

A truly universal cyber security framework can only be grounded in existing international law, including the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law.

The EU and its Member States also underline that human rights and fundamental freedoms as enshrined in the relevant international instruments must be respected and upheld equally online and offline. We welcome that these principles have been also affirmed by the UN Human Rights Council and General Assembly.

In order to build trust and stability, we reaffirm our support for continued dialogue and cooperation to advance a shared understanding on the application of international law to the use of ICTs by States. In that regard, we encourage all UN Member States to share with other countries their national positions on their understanding of the application of international law as applied to the use of ICTs by States.

The corollary of this position is that we neither call for, nor see the necessity for the creation of new international legal instruments for cyber issues. Moreover, there are a number of reasons why we believe that it would be unwise to cast doubt as to whether already existing international law applies in cyberspace. It could have a counter-productive effect – including undermining ongoing practical efforts to tackle a real, pertinent and pressing problem of increasing cyber incidents.

Implementing norms

We rather encourage focusing collective efforts on building on the work repeatedly endorsed by the UNGA, notably in resolution 70/237, and on further implementation of these agreed norms and confidence building measures which offer the greatest added value for conflict prevention. The OEWG furthermore offers the opportunity to seek a full range of views and perspectives, and to take into account how challenges to implement these norms are perceived, across the UN membership but also non-governmental stakeholders. In this regard we welcome transparency and exchanges of best practices to implement the norms of responsible state behaviour, including through the OEWG.

Confidence building measures

The EU and its Member States underline the importance of confidence-building measures as a practical means of preventing conflicts.

Building effective mechanisms of state interaction in cyberspace is essential to reducing the likelihood of conflict. Regional fora have proven to be a relevant platform to create space for dialogue and cooperation among actors with shared concerns but common interests in order to address effectively challenges in regards with regional specificities. Confidence building measures developed in regional organisations such as the Organisation for Security and Co-operation in Europe could be exchanged upon in the OEWG as examples of practical efforts to advance cyber stability. We believe that implementing cyber confidence building measures in the OSCE, ARF, OAS and other

regional settings will increase the predictability of State behaviour and could reduce the risk of conflict.

Resilience and capacity building

Another practical effort that is important to the EU and its Member States is cyber capacity building.

In order to prevent conflicts and reduce tensions stemming from the use of ICTs, including reducing the ability of potential perpetrators to misuse ICTs for malicious purposes, we aim to strengthen cyber security in an interconnected world.

We need to focus our collective efforts on developing the skills and capacity to address cyber threats adequately and to advance peace and stability through effective implementation of the norms, rules and principles of responsible state behaviour and the application of international law in cyberspace. For our part, the EU stands ready to supporting cyber capacity building work through its external financing instruments and welcomes further engagement in this regard, both in this and other relevant fora. To take an example, the EU's Cyber-Resilience for Development project promotes the adoption of consistent, actionable national cyber-security strategies.

Mr. Chairman,

The EU and its Member States reaffirm that all stakeholders should embrace their responsibilities to keep cyberspace open, free, stable and secure and work together to address them.

We underline that the OEWG's mandate provides a role for all stakeholders, and is a valuable platform for the exchange of positions and discussion, that can foster a stronger common understanding of threats faced in cyberspace and a common approach. We recognize the fact that the OEWG presents an important opportunity for an inclusive process where all relevant actors can have their voice heard.

We support the recommendation to engage in an open and regular dialogue with all relevant actors, including where appropriate the private sector, academia and civil society, and through relevant existing regional and international fora.

In conclusion, the EU and its Member States look forward to engaging constructively in OEWG discussions with a view of to promoting and further building, notably, on the cumulative achievements of work undertaken in the previous UN GGEs.

Thank you Mr. Chairman.