# Statement on behalf of the European Union

**by**


## Mr. Pawel HERCZYNSKI

**Managing Director for CSDP and Crisis Response**
**European External Action Service**


**at the Arria-Formula Meeting on**
**Cyber Stability, Conflict Prevention and Capacity Building**

**United Nations**
**22 May 2020**

Mr. President, distinguished colleagues,

I'm grateful to Estonia and colleagues for organizing this timely event. I have the honour to speak on behalf of the European Union.

Mr. President,

Cyberspace is increasingly central to our lives. It is a place of opportunity, but also a source of new challenges. There is a clear and concerning rise in cyber threats and malicious cyber activities, conducted by both state and non-state actors. Such malicious activities can lead to destabilising and cascading effects with enhanced risks of conflict. In such circumstances, especially given the COVID-19 context, we urgently need to strengthen global cooperation to prevent conflicts and advance stability in cyberspace.

As the coronavirus pandemic continues, the European Union and its Member States have observed cyber threats and malicious cyber activities targeting essential operators, including in the healthcare sector, which can put people's lives at risk. Any attempt to hamper the ability of critical infrastructures is unacceptable in all circumstances, at all times, as well as contrary to existing norms of responsible State behaviour.

In the recent declaration on malicious cyber activities exploiting the coronavirus pandemic, the EU and its Member States have called upon all UN Member States to exercise due diligence and take appropriate actions against actors conducting malicious activities from their territories, consistent with international law and the universally agreed norms of responsible State behaviour.

In order to prevent conflicts and reduce tensions stemming from the use of ICTs, the EU and its Member States aim to strengthen cyber security and resilience as well as build capacities of our international partners. Global resilience is a crucial element, as a means to address the challenges associated with the digitalisation of economies and societies, as well as to reduce the ability of potential perpetrators to misuse ICTs for malicious purposes.
Our strong commitment to peace and stability is based on three pillars. Firstly, on developing and meaningfully implementing confidence-building measures between States; secondly, on demonstrating our willingness to settle international disputes by peaceful means, while also responding to incidents, when appropriate, through the framework for a joint EU diplomatic response to malicious cyber activities; and thirdly, on deepening our regular dialogue with partners as well as with regional organizations.

Mr. President,

We live in an interconnected and rapidly changing world, therefore applying existing international law and upholding UN agreed rules and norms of responsible state behaviour is the sole basis we have for handling increasingly complex challenges. Such commitment contributes to the rules-based order, effective multilateralism and effective global governance, which keep cyberspace open, stable and secure.

The EU and our Member States are committed to the further discussions in the UN on security and stability in cyberspace.

To this end, we continue to support ongoing efforts to promote the application of existing international law and encourage focusing our collective efforts on advancing the implementation of existing norms of responsible State behaviour.

Mr. President,

In order to contribute to the advancement of global cyber stability and to the full respect and meaningful implementation of the rules-based order, our efforts must be supported by capacity building. One of the key challenges for the international community is strengthening its resilience and capability to respond to cyberattacks.

The EU has been implementing cyber capacity building programmes worldwide, and we are committed to close global coordination on this issue, with our international partners. We reaffirm that all stakeholders must embrace their specific responsibilities and believe in the role of other stakeholders and further cooperation to implement existing UN GGE reports. The private sector has specific responsibilities, including due diligence, and should play a role in building resilience in the digital domain, as we all should in our respective responsibilities.

Thank you