**Statement on behalf of the EU and its Member States**

**First negotiating session of the Ad-hoc Committee set up to elaborate a 'UN Convention on countering the use of information and communications technologies for criminal purposes'**

**Agenda Item 4 – Objectives and scope of the Convention**

**United Nations**
**New York**

**(Wednesday, 2 March 2022)**

***Check against delivery***

Madam Chair, Your Excellencies, Distinguished Delegates, I have the honour to speak on behalf of the European Union and its Member States.

The Candidate Countries 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.

At the outset let me express the EU and its Member States' full solidarity with Ukraine and the Ukrainian people. The EU condemns in the strongest possible

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

terms Russia's military aggression against Ukraine, which grossly violates international law and the UN Charter, and undermines international security and stability. The EU demands that Russia immediately ceases its military actions and stops its disinformation campaign and cyber-attacks. These circumstances and the continued cyber-attacks against Ukraine are not conducive to a constructive engagement with Russia on a legally binding convention in the cyber field

The European Union and its Member States are of the view that the future Convention should focus on and provide clear definitions of cyber-dependent crimes, include provisions on criminal procedural measures as well as mechanisms for international cooperation within the criminal justice system, including capacity-building, all of which should be consistent with existing international instruments.

With regard to the definitions of activities that should be criminalized, the EU and its Member States consider that the new instrument should primarily focus on activities that can only be committed through the use of information systems, i.e. cyber-dependent crimes.

These crimes should be precisely defined and give preference to concepts already agreed in existing international agreements. In particular, we should avoid the criminalisation of broadly or vaguely defined activities, especially where such regulations may disproportionately limit freedom of speech and the expression of opinions, ideas and beliefs.

With regard to possible procedural provisions, those should complement and reinforce the existing cooperation mechanisms. These procedural provisions should enable the swift exchange of electronic evidence among operational entities, with due regard for the necessary safeguards.

An important aspect that we cannot overlook is the need to ensure that the law enforcement and judicial authorities of UN Member States have sufficient capabilities to fight cybercrime effectively. The future Convention should

provide a framework for sustainable capacity building and technical assistance, thereby reinforcing existing tools and instruments such as UNODC's Global Programme on Cybercrime and the Council of Europe's GLACY+. Practical tools to prevent cybercrime may thus also be considered.

The EU and its Member States already have a track record in funding and providing capacity building measures, in partnership with the Council of Europe and UNODC, to a large number of countries across the globe. We will continue to do so.

The future Convention should, for all of these elements, ensure the protection of human rights and fundamental freedoms, and be compatible with international legal obligations and relevant instruments in that area. The role of victims of cybercrime should also be considered.

Finally, I should clarify that the EU and its Member States consider that elements that fall outside the criminal justice system should also fall outside the scope of the future Convention. More specifically, it should not cover aspects relating to national security, state behaviour, critical infrastructure, rules regulating Internet governance and provisions directly imposing obligations upon non-governmental organisations including the private sector.

Thank you, Madam Chair.