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 6 - Preliminary exchange of views on key elements of the Convention

United Nations
New York

(Monday, 7 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.

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

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 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

We would like to present the following views on the key elements that we think could be included in the future Convention.

On substantive criminal law provisions, the European Union and its Member States consider that substantive criminal law provisions of the future Convention should in general focus on offences that can only be committed by information systems, often referred to as *cyber-dependent crimes*. This includes offences like illegal system access and illegal interception or illegal system interference.

Nevertheless, the European Union and its Member States are open to discussing the possible criminalisation of other types of behaviour, but *only* if those are limited to certain narrowly defined and universally recognised relevant offences, where the involvement of information systems substantially changes the characteristics or impact of the offence.

Madam Chair,

The European Union and its Member States consider it important to avoid including a long list of broadly defined cyber-enabled crimes for two main reasons.

First, because this approach seems unnecessary, as there are already other existing instruments dealing with offences where the involvement of information systems does not substantially change the characteristics or impact of the offence. For instance, the UN Convention against Transnational Organised Crime already provides for such definitions. Therefore, we should avoid the inclusion of offences that are already regulated by existing provisions in other international conventions.

Second, given the proposed timeframe, trying to reach an agreement on a long list of traditional crimes committed by means of ICTs is very ambitious; it might even seriously delay the conclusion of the negotiations. Therefore, we should aim for a realistic scope of criminal offences.

We should also avoid including broadly or vaguely defined criminal acts, since such vague definitions would risk leading to legal uncertainty, to unduly and disproportionately interfering with human rights and fundamental freedoms and lead to an ineffective application of the future Convention.

We should avoid as well the criminalisation of behaviour that, while perhaps harmful, may be more appropriately tackled through means other than criminal law.

Given the pace of future technological development, the Convention's provisions should be drafted in a technology neutral manner. At the same time, the future Convention should encourage the exchange of views and information about new challenges posed by future technological developments.

The Convention should refrain from setting minimal standards for sanctions or punishment for specific offences beyond existing models. The UN Convention against Transnational Organised Crime could serve as a model.

As regards rules on jurisdiction, these should be modelled on the approach set out in existing legal instruments. The UN Convention against Transnational Organised Crime or the UN Convention against Corruption could serve as a model.

Madam Chair,

On procedural criminal law provisions, the European Union and its Member States support the inclusion in the Convention of procedural measures and mechanisms for international cooperation in investigations and judicial proceedings, as well as for obtaining electronic evidence, while ensuring that such evidence can be collected, preserved, authenticated and used in criminal proceedings.

These measures should build on models included in other relevant international and regional legal instruments, such as the Budapest Convention, and should be coupled with appropriate guarantees, including cooperation in emergency situations. These measures should also complement existing cooperation mechanisms.

Furthermore, we could consider including provisions for cooperation in removal of specific and narrowly defined illegal content such as images or recordings of child sexual abuse. The Convention could provide for terms, conditions and safeguards for international cooperation in this regard.

On safeguards to protect human rights and fundamental freedoms, for the Convention to be universally acceptable, strong and effective safeguards should

guide the criminal law provisions. This is required by the rule of law and will create trust among the parties to the Convention. Such guarantees should build on the model of safeguards included in other relevant international and regional legal instruments, including the Budapest Convention on Cybercrime. As highlighted in the submission of the Office of the High Commissioner for Human Rights (OHCHR) to the Chair, human rights protection should be at the centre of the AHC discussions.

It is thus important to have clear provisions in the future Convention that ensure respect for human rights and fundamental freedoms. In particular with regard to the right to privacy, protection of personal data, freedom of expression and information and the right to a fair trial as well as to the principles of legality, necessity and proportionality of law enforcement action.

Any provisions on access to, seizure and storage of electronic evidence should be underpinned by minimum standards and norms, including safeguards to protect human rights and fundamental freedoms.

On other provisions, the future Convention should include a basis for capacity building, sharing of best practices and lessons learned, as well as for technical assistance.

The UNODC Secretariat will need to have a key role to play in the continuation of capacity building but also in the implementation of the future Convention in particular because of its experience and expertise on cybercrime matters and criminal matters, and as a repository of knowledge on cybercrime.

Thank you, Madam Chair.