CONTRIBUTION FROM THE EUROPEAN UNION AND ITS MEMBER STATES

Preparation for the first session of the United Nations Ad Hoc Committee to elaborate a Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, taking place from 17-28 January 2022 in New York

This document reflects the views and position of the European Union ("the EU") and its Member States[1] on the scope, objectives and structure (elements) to be taken into account in elaborating a new United Nations *Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes* ("UN Convention") and to contribute to the preparation of the first session of the UN Ad Hoc Committee established for that purpose by UN General Assembly Resolution 74/247.[2]

This contribution is without prejudice to any future positions that the EU and its Member States may take during the course of future negotiations on the scope, objectives and structure of a future UN Convention.

I. Objectives

The EU and its Member States underline that a future UN Convention should serve as a practical instrument for criminal law enforcement and judicial authorities in the global fight against cybercrime, with the aim to add value to international cooperation. As reflected in UNGA resolutions 74/247 and 75/282[3], a future UN Convention should take into full consideration the existing framework of tried-and-tested international and regional instruments in the field of organised crime and cybercrime. Therefore, any new convention should complement and avoid impairing in any way the application of existing instruments or the further accession of any country to them and to the extent possible avoid duplication.

---

1 Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

2 UNGA Resolution 74/247 on "Countering the use of information and communications technologies for criminal purposes", adopted on 27 December 2019 - https://undocs.org/A/Res/74/247

3 UNGA Resolution 75/282 "Countering the use of information and communications technologies for criminal purposes", adopted on 26 May 2021 - https://undocs.org/en/A/RES/75/282

A future UN Convention should provide for the protection of human rights and fundamental freedoms, which apply both offline as well as online, and be compatible with relevant instruments in that area.

A future UN Convention, as agreed by UNGA Resolution 75/282, should take into full consideration the work[4] and outcomes[5] of the open-ended intergovernmental Expert Group ("IEG") to Conduct a Comprehensive Study on Cybercrime.

II. Scope

To that end, the EU and its Member States believe that the scope of a future UN Convention should be focused primarily on substantive criminal and criminal procedural law as well as associated mechanisms for cooperation. It should also comply with international human rights standards and strive to fight cybercrime most effectively and thus protect victims.

The EU and its Member States consider that this new instrument should precisely define the terms it uses and give preference to concepts already agreed in existing international texts.

The EU and its Member States recommend that the content of this Convention be compact and focus on the essential elements of criminal justice, and should thus exclude as much as possible any ancillary elements.

Based on the principles outlined above, the EU and its Member States consider that the following elements **should be included** in a future UN Convention:

1. Substantive criminal law provisions linked to cybercrime offences that should be criminalised by all State Parties of a future UN Convention. These provisions should in general relate only to high-tech crimes and cyber-dependent crimes, such as illegally gaining access to, intercepting or interfering with computer data and systems.[6]

Substantive criminal law provisions must be clearly and narrowly defined, and be fully compatible with international human rights standards and a global, open, free, stable and secure cyberspace. Vague provisions criminalising behaviour that are not clearly defined in a future UN Convention or in other universal legal instruments would risk unduly and disproportionately interfering with human rights and fundamental freedoms, including the freedom of speech and expression, while also resulting in legal uncertainty.

Provisions of substantive criminal law should, to the extent possible, be drafted in a technology neutral manner in order to encompass technical developments in the future[7]. At the same time, the

---

4 https://www.unodc.org/unodc/cybercrime/egm-on-cybercrime.html

5 https://undocs.org/UNODC/CCPCJ/EG.4/2021/2

6 In line with the adopted recommendation 5 (a, b, c) on criminalisation of the 7th session of the IEG on cybercrime.

7 See adopted recommendation 1 on Legislation and frameworks of the IEG.

exchange of views and information about new challenges posed by further technological developments should be encouraged.

Incompatibility with other international conventions must be avoided in particular where certain offences, such as arms trafficking or the distribution of narcotic drugs, are already widely covered by existing provisions in international conventions, such that the inclusion of these types of behaviour in a convention on cybercrime would not be of added value.

In general, a future UN Convention should refrain from setting (minimal) standards for sanctions or punishment for specific offences beyond existing models, such as Article 11(1) UNTOC.

As regards rules on jurisdiction, a future UN Convention should be modelled on the approach set out in existing legal instruments, such as Article 15 UNTOC.

2. Appropriate substantive and procedural conditions and safeguards to ensure compatibility with human rights and fundamental freedoms, including the principles of legality, necessity and proportionality of law enforcement action and specific substantive and procedural guarantees ensuring in particular the right to privacy and personal data protection, freedom of expression and information and the right to a fair trial. Such guarantees should build on and be at least on the same level as the safeguards included in other relevant international legal instruments.

3. Procedural measures and criminal procedural provisions regarding mechanisms for cooperation between the parties to a future UN Convention, including cooperation in investigations and other judicial proceedings and in obtaining electronic evidence where appropriate and relevant while ensuring they can be collected, preserved, authenticated and used in criminal proceedings[8]. Such measures and provisions would need to be consistent with and build on the model of those included in other relevant international legal instruments and complemented by appropriate guarantees, including cooperation in emergency situations.

4. Elements, in conformity with human rights, regarding **capacity building, sharing of best practices and lessons learned, and technical assistance**, including the significant role of the UNODC in these areas**.**

The EU and its Member States consider that the following must be **out of the scope** of a future UN Convention:

- Matters related to or regulating national security or state behaviour;
- Matters related to or regulating rules on Internet governance, which are already being addressed in the context of dedicated multi-stakeholder policies and forums.

Finally, as an intergovernmental instrument, a future UN Convention should refrain from directly imposing obligations upon non-governmental organisations, including the private sector, such as internet service providers.

[8] See adopted recommendation 16 on Electronic evidence and criminal justice of the IEG.

III. Structure

Based on the above, a future UN Convention could include the following different chapters:

Preamble (scope and objectives of a future UN Convention)

I. Types and precise definition of crimes;

II. Domestic Procedural rules and fundamental principles to be respected in that regard (i.e.: respect for human rights including privacy and personal data protection, necessity, proportionality);

III. International cooperation;

IV. Technical assistance, training, capacity building and role of the UNODC in that regard.

***