Council of the European Union

Brussels, 11 October 2021
(OR. en)

11925/2/21
REV 2

LIMITE

CYBER 237
COPEN 352
COPS 321
RELEX 774
JAIEX 98
TELECOM 341
POLMIL 139
CFSP/PESC 833

NOTE

From:	EEAS and European Commission services
To:	Delegations
Subject:	Draft position for a UN Convention on countering the use of information and communications technologies for criminal purposes

Delegations will find in Annex a revised 'draft position for a UN Convention on countering the use of information and communications technologies for criminal purposes', in view of the first negotiating session taking place from 17-28 January 2022 in New York.

This document was revised taking into account discussions at the Horizontal Working Party on Cyber Issues on 6 October and delegations' written comments, in view of the 13 October 2021 meeting of the Horizontal Working Party on Cyber Issues**.**

ANNEX

[DRAFT] Position to be expressed by the EU and its Member States for a UN Convention on countering the use of information and communications technologies for criminal purposes, notably in view of the first negotiating session taking place from 17-28 January 2022 in New York

This document presents a draft position to be expressed by the EU and its Member States to guide EU engagement towards and during the first negotiating session (New York, 17-28 January 2022) of the '*UN open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*' (hereafter, "the AHC"), established by UN General Assembly Resolution 74/247.[1] This position will also feed in the EU written contribution as requested by the AHC chair by 29 October 2021.

The position should enable the EU to share and build support for common positions with its like-minded partners, in particular regarding the scope and objectives of a future 'UN Convention on countering the use of information and communications technologies for criminal purposes' (hereafter also "UN Convention").

The position will also serve as a basis for outreach to third countries with the aim of building a broad coalition of countries in support of a UN Convention which adds value in the global fight against cybercrime as a practical instrument for criminal law enforcement and judicial authorities, is compatible with existing tried-and-tested international instruments[2] **- in particular the 2001 Council of Europe Budapest Convention on Cybercrime and its protocols and the 2000 United Nations Convention against Transnational Organized Crime and its protocols, but also other relevant international and regional instruments in the field of cybercrime or in particular relating to the protection of humans rights -** and in line with EU law, including the EU Charter of Fundamental Rights, as well as international human rights standards.

[1] https://undocs.org/A/Res/74/247

[2] ~~**In particular the 2001 Council of Europe Budapest Convention on Cybercrime and its protocols and the 2000 United Nations Convention against Transnational Organized Crime and its protocols, but also other relevant international and regional instruments in the field of cybercrime orin particular relating to the protection of humans rights;**~~

In addition, the position will provide a basis for seminars and workshops bringing together representatives and experts from a broad range of countries as well as civil society and other relevant stakeholders, to ensure that these organisations and stakeholders, in particular from the Global South, are involved in the process and can make their voices heard.

I. PROCEDURAL ISSUES

The EU and its Member States attach great importance to the fact that the negotiation process (as well as the process leading to the substantial negotiations) must be open, inclusive and transparent and based on cooperation in good faith. In particular:

a) all relevant documents should be published on the AHC website[3] and all States, the EU[4] and other participants should be consulted and have the possibility to share their views and be heard. The timeline for negotiations should allow for appropriate consultations.

b) the participation of all relevant stakeholders, including civil society, private sector, academia and non-governmental organisations in the process is crucial. Hence, swift implementation of the relevant operative paragraphs of the UN General Assembly Resolution on AHC modalities[5] is of the essence, to enable effective stakeholders' participation as from the first formal negotiating session of the AHC. Their participation should therefore be resolved as a matter of priority. In fact, according to the usual practice, the invitation of observers should take place before the beginning of the first meeting and stakeholders should be in a position to observe and participate in all discussions, including on the scope and objectives of the convention, and submit documents to be published on the website of the AHC.

c) the AHC Bureau was created to ensure a geographically balanced representation of all regional groups in steering the process. The EU **and its Member States** will encourage the Chair to make full use of the Bureau in steering the negotiations and building the broadest possible support for the work of the AHC. The EU **and its Member States** will also encourage the Chair to rely on **the expertise of** UNODC as the secretariat of the Ad Hoc Committee in the preparations of the sessions.

[3] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home
[4] In line with UNGA resolution 65/276
[5] 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

d) the EU and its Member States consider it important to agree on the scope and objectives of a possible future convention before the structure and content of the convention are discussed. **The EU and its Member States appreciate the entire UN Membership has the possibility to submit to the Chair their views on the scope and objectives of the future Convention prior to the commencement of substantial negotiations. At the same time they are of the view that all inputs received by the AHC Bureau and the UNODC Secretariat in this respect should be considered on equal basis and serve as elements for substantive discussion on the scope and objectives of the future UN Convention during the first substantial AHC meeting.**

e) the calendar of AHC meetings, once agreed by the AHC, should as soon as possible include indications for intersessional consultations according to OP10 of resolution 75/282. **Depending on whether the first substantive session in January 2022 can agree on a structure of a Convention, the EU and its Member States are open to the idea of establishing a programme of work for the subsequent negotiating sessions of the AHC, as well as for informal consultations with participating Member States and stakeholders, and intersessional consultations.**

II. SUBSTANTIVE ISSUES

Scope and objectives of a UN Convention on countering the use of information and communications technologies for criminal purposes

To add value from the perspective of the EU and its Member States, a new UN convention would need to usefully complement the existing framework for international cooperation, notably the Council of Europe "Budapest" Convention on Cybercrime, which harmonises definitions of cybercrimes and sets out a number of mechanisms to facilitate cooperation between its State Parties, and also the United Nations Convention against Transnational Organized Crime and other relevant instruments, in particular relating to the protection of human rights. Any new convention should therefore be compatible with the existing framework, not impair in any way the application of the above-mentioned instruments or the further accession of any country to them and, to the extent possible, avoid duplication.

To that end, the EU and its Member States should ensure that the scope of a possible future UN Convention on countering the use of information and communications technologies for criminal purposes is focused primarily on substantive criminal and criminal procedural law, as well as associated mechanisms for cooperation. In the negotiations, the EU will firmly promote its human centric vision and human rights-based approach and will strive for compliance of the future Convention with standards of international human rights. The EU and its Member States should also ensure the UN Convention enables States to join their efforts to fight cybercrime effectively and thus protect victims. The EU and its Member States consider that this new instrument should precisely define the terms used and give preference to concepts already agreed in existing international texts.

In determining the scope and objectives of the UN Convention, the AHC as agreed by the RES 75/282, should take into full consideration the work[6] and outcomes[7] of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime.

On the basis of the principles outlined above, the EU and its Member States should:

1. *promote* the inclusion of certain **substantive criminal law provisions** linked to cybercrime that should be criminalised ~~**in**~~**by** all State Parties.

   In general, ~~**these**~~ **such provisions** should relate to high-tech crime**s** and cyber-dependent crime, such as illegally gaining access to, intercepting or interfering with computer data and systems[8]. The criminalisation of other types of behaviour that may be conducted by means of ICTs, so-called cyber-enabled crimes, could be accepted, but only if limited to certain narrowly defined and universally recognised relevant offences, **where the involvement of information systems substantively changes the characteristics or impact of the offence,** such as child sexual abuse and exploitation,[9] computer-related fraud and computer-related forgery, and offences related to infringements of copyright and related rights.

[6] https://www.unodc.org/unodc/cybercrime/egm-on-cybercrime.html
[7] https://undocs.org/UNODC/CCPCJ/EG.4/2021/2
[8] In line with the adopted recommendation 5 (a, b, c) on criminalisation of the 7th session of the IEG on cybercrime.
[9] Preference for the most recently and widely accepted and accurate terminology "child sexual abuse and exploitation" instead of the outdated and incorrect term "child pornography". Due to the reference to "pornography" this term makes it seem like it concerns (consensual) engagement in erotic behaviour in recordings for the purposes of sexual excitement. This connotation is inappropriate in the context of minors.

Substantive criminal law provisions of the future UN Convention must be clearly and narrowly defined, fully compatible with international human rights standards and a global, open, free, stable and secure cyberspace. ~~**Criminalisation of**~~ **Vague provisions criminalising** behaviour that is not clearly defined in the Convention or in other universal legal instruments would risk ~~**resulting in vague provisions,**~~ potentially unduly **and disproportionately** interfering with human rights and fundamental freedoms: ~~**it**~~ **such provisions** should therefore be opposed **by the EU and its Member States**. 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. **The Convention should therefore avoid using or defining technical terms which may be linked to specific technologies and at any rate lack an internationally agreed definition. At the same time, the exchange of views and information about new challenges within the scope of the convention posed by further technological developments should be encouraged.**
Incompatibility with other international conventions must be avoided and where certain offences, such as arms trafficking or the distribution of narcotic drugs, are already widely covered by existing provisions in international conventions, the inclusion of these types of behaviour in a convention on cybercrime would not be of added value. The EU and its Member States must **also** firmly oppose any attempt to unduly limit rights or criminalise online activities that are generally considered legal in open and democratic societies.

Criminalisation should remain *ultima ratio* and the EU and its Member States should not accept to be bound by provisions criminalising behaviour that, while considered harmful, may more appropriately be tackled through means other than criminal law.

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

As regards rules on jurisdiction, the EU and its Member States should support the approach set out in existing legal instruments, such as Article 15 UNTOC.

2. *support* the inclusion of **appropriate substantive and procedural conditions and safeguards** to ensure compatibility with human rights and fundamental freedoms, limiting any interference to what is necessary and proportionate for the purpose of specific criminal investigations. Safeguards for human rights and fundamental freedoms should include 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 data protection, and freedom of expression and information **and** the right to a fair trial ~~**and should allow**~~ thus allowing EU Member States to comply with their obligations under the EU Charter of Fundamental Rights and relevant EU law**s** (e.g. privacy and data protection rules). ~~**They**~~ **Such guarantees** should build on the model (and be at **least on** the same level) of the safeguards included in other relevant international legal instruments.

3. *support* the inclusion of ~~**domestic**~~ **procedural measures** and **criminal procedural provisions regarding mechanisms for cooperation between the parties to the Convention**, including cooperation in investigations and other judicial proceedings and in obtaining electronic evidence where appropriate and relevant[10] and in line with existing obligations of the EU and its Member States. 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. They could complement existing cooperation mechanisms, for instance by creating channels for cooperation with countries that are not parties to the Budapest Convention, including cooperation in emergency situations (24/7 network). ~~**Such mechanisms should be compatible with existing ones.**~~

4. **Since this treaty will imply, in practice, the exchange of information among the Parties (which may constitute personal data), the possible future UN Convention should also provide for international transfers of personal data, in line with and subject to the conditions of EU law.**

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

5. *show openness* ~~***(without proactively bringing this to the negotiating table)***~~ to the possible **specification of relevant procedures or the** inclusion of minimum standards and norms, including fundamental safeguards, for the access to**,** ~~**and**~~ the seizure **and the storage** of electronic evidence ~~**to preserve the chain of custody**~~.

6. *engage in negotiations* to consider *including* **provisions for cooperation in removal of specific and narrowly defined illegal content** such as images or recordings of child sexual abuse. The UN Convention could provide for terms, conditions and safeguards for international cooperation **in this regard**. The description of ~~**such**~~ **illegal** content needs to be clearly defined and limited so as not to disproportionately infringe upon fundamental freedoms. Moreover, State parties should be able to refuse cooperation in such matters and any such measure should be in line with EU and EU Member States' laws and obligations.

7. *oppose* the inclusion of matters related to national security or state behaviour.

8. *oppose* any criminalisation of a broad**ly and vaguely defined** ~~**range of**~~ activities, especially where such regulations may disproportionately limit legitimate speech and the expression of opinions, ideas and beliefs.

9. *defend* that, as an intergovernmental instrument, the convention should **refrain from directly imposing obligations upon non-governmental organisations including the private sector, such as internet service providers**~~**, based in the territory of other States**~~.

10. *oppose* any **regulation on or reference to rules on Internet governance**, which are already addressed in the context of dedicated multi-stakeholder policies and forums. **Further oppose possible efforts to establish new structures or to expand mandates of existing International Standardisation Organisations through provisions of this Convention.**

11. *Support* the inclusion of elements regarding **capacity building, sharing of best practices and lessons learned, and technical assistance, including the significant role of the UNODC in these areas.**

12. The EU and its Member States recommend that the content of this Convention be compact and cover only the essential elements of criminal justice, excluding as much as possible any ancillary elements

Based on the above, the UN convention may be structured as follows:

In a very first and general approach, a new treaty on cybercrime should include the following different chapters:

Preamble (scope and objectives of the Convention)

I. Types and precise definition of crimes;

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

III. International cooperation towards lawfully obtaining e**lectronic** evidence.

IV. Technical assistance**, training, capacity building** and role of the UNODC in that regard ~~**Role of UNODC and Training and technical assistance**~~

~~**Since this treaty will imply, in practice, the exchange of information among the Parties (which may constitute personal data), the possible future UN Convention should also provide for international transfers of personal data, in line with and subject to the conditions of EU law.**~~