



Council of the
European Union

Brussels, 2 May 2022
(OR. en)

8486/22
ADD 1

LIMITE

CYBER 148
COPEN 150
JAI 565
COPS 182
RELEX 551
JAIEX 40
TELECOM 182
POLMIL 99
CFSP/PESC 555
ENFOPOL 227
DATAPROTECT 123

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	7860/22 ADD 1
Subject:	ANNEX to the Recommendation for a Council Decision authorising the negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes

ANNEX ADDENDUM

DIRECTIVES FOR THE NEGOTIATION OF A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

Regarding the process of the negotiations, the Union should aim to achieve that:

- (1) The negotiation process is open, inclusive and transparent, and based on cooperation in good faith.
- (2) The negotiation process enables participation in a meaningful way of all relevant stakeholders, including **representatives of** civil society, the private sector, academia and non-governmental organisations.
- (3) ~~All the i~~Inputs received from the entire United Nations ~~Membership~~ **Members** are considered on an equal basis to ensure an inclusive process.
- (4) The negotiation process is based on an effective and realistic work programme.

Regarding the general objectives for the negotiations, the Union should aim to achieve that:

- (5) **Whilst ensuring a high level of protection of human rights and fundamental freedoms, T**~~the~~ Convention serves as an effective instrument for ~~criminal~~ law enforcement and judicial authorities in the global fight against cybercrime, with the aim to ~~add value to international cooperation~~ **promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively, to also promote and facilitate international cooperation, to ensure a high level of protection of victims' rights, and to support capacity building and technical assistance in the fight against cybercrime.**

- (6) The existing framework of tried-and-tested international and regional instruments and efforts as reflected in United Nations General Assembly Resolutions 74/247 and 75/282 is taken into full consideration. Accordingly, the Convention is compatible with ~~and complement~~ existing international instruments, in particular ~~the 2001 Council of Europe Budapest Convention on Cybercrime and its protocols~~, the 2000 United Nations Convention against Transnational Organized Crime and its protocols, the 2003 United Nations Convention against Corruption and its protocols, the 2001 Council of Europe Budapest Convention on Cybercrime and its protocols, but also other relevant international and regional instruments, in particular relating to the protection of human rights and fundamental freedoms. The Convention avoids any impact on their application or the further accession of any country to these existing instruments ~~them~~ and, to the extent possible, avoid unnecessary duplication.
- (7) The work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime as agreed by United Nations General Assembly Resolution 75/282 are taken into full consideration.
- (8) The provisions of the Convention achieve the highest possible protection of human rights and fundamental freedoms. EU Member States should be able to comply with international and EU law, including the fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and the Charter of Fundamental Rights. The provisions of the Convention should also be compatible with the EU's and its Member States' international trade obligations, especially in the context of the WTO.

Regarding the substance of the negotiations, the Union should aim to achieve that:

- (9) The Convention provides for definitions of offences that can only be committed using ~~information~~ computer systems.

- (10) **[Provided that sufficient conditions and safeguards and an adequate protection of human rights and fundamental freedoms are guaranteed,** The Convention ~~provides~~ **could provide** for definitions of offences that can be committed without using ~~information~~ **computer** systems but that can be enabled by the use of ~~information~~ **computer** systems in certain circumstances, but only in cases where the involvement of ~~information~~ **computer** systems substantially changes the characteristics or impact of the offences.]
- (11) The offences are clearly and narrowly defined in a technology neutral manner. The definitions are compatible with those in other relevant international or regional conventions in particular in the area of ~~organised crime or~~ cybercrime, and with international human rights standards **and fundamental freedoms**.
- (12) The Convention provides for rules on the ~~attempt~~, aiding and abetting **and, where appropriate, on the attempt** of such offences, on the liability of **both natural and** legal persons for such offences, for rules on the establishment of jurisdiction over such offences, and on **effective, proportionate and dissuasive** sanctions and measures in relation to such offences that are compatible with other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and with international human rights standards.
- (13) The Convention provides for procedural criminal measures that allow authorities to investigate cybercrimes effectively, **[which could include measures** ~~to freeze and confiscate proceeds of such crimes and~~ to preserve or obtain electronic evidence of any criminal offence as part of a criminal investigation or proceeding, taking due account of the proportionality, **legality and necessity** principles, **the protection of the rights concerning the respect for privacy and the protection of personal data.**]
- (14) Those procedural criminal measures ~~provide sufficient added value compared to~~ **do not contradict** other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and are compatible with such conventions and with international human rights standards and **fundamental freedoms**.

- (15) Procedural measures to preserve or obtain electronic evidence contain a clear and narrow definition of the type of ~~information~~ **data** covered. Procedural measures for cooperation with private sector entities ensure that the burden on such entities is proportionate and that private sector entities fully respect **laws protecting** the human rights of their users. The Convention provides legal clarity for online service providers (e.g., Internet service providers) in their interactions with law enforcement authorities of the State Parties to the Convention. [Procedural measures for the removal of illegal content only relate to illegal content that ~~can be~~ **is** sufficiently specific and narrowly defined **in the Convention.**]
- (16) The Convention provides for cooperation measures that allow authorities in different States that are party to the instrument to cooperate effectively **through mutual legal assistance, including by the establishment of contact points,** for the purpose of criminal investigations or proceedings concerning offences defined in the instrument. [It also provides for such cooperation measures for the purpose of preserving or obtaining electronic evidence of any criminal offence as part of a criminal investigation or proceeding, **provided that these measures are subject to sufficient conditions and safeguards under States' domestic law, which shall provide for the adequate protection of human rights and fundamental freedoms.**]
- (17) Those cooperation measures **are compatible with** ~~provide sufficient added value compared to~~ other relevant international or regional conventions in particular in the area of organised crime or cybercrime, and ~~are compatible with~~ **do not contradict** such conventions, ~~with~~ international human rights standards **and fundamental freedoms.**
- (18) Cooperation measures are subject to the conditions provided for by the law of the requested Party and provide for broad grounds for refusal such as to ensure the protection of fundamental rights, including the right to the protection of personal data, including in the context of personal data transfers, and, ~~where appropriate,~~ the existence of double criminality.

- (19) The Convention provides for strict conditions and strong safeguards to ensure that EU Member States can respect and protect fundamental rights, freedoms and general principles of EU law as enshrined in the European Union Treaties and the Charter of Fundamental Rights, including, in particular, the principles of proportionality, **legality and necessity of criminal offences and penalties**, procedural guarantees and rights, the right to effective judicial redress, the presumption of innocence, the right to a fair trial, and the rights of defence of persons subject to criminal proceedings, **the right not be tried or punished twice in criminal proceedings for the same criminal offence**, as well as the right to privacy, the right to the protection of personal data and of electronic communications data when such data is processed, including for transfers to authorities in countries outside the European Union, and the right to freedom of expression and information. The Convention ensures in particular that EU Member States are able to comply with requirements for the international transfers of personal data within the meaning of Directive (EU) 2016/680, Regulation (EU) 2016/679 and Directive 2002/58/EC. The conditions and safeguards also ensure the protection of human rights and fundamental freedoms in line with international human rights standards. This applies to the entire Convention, including procedural measures and cooperation measures, including those that may significantly interfere with individuals' rights, ~~such as the freezing and confiscation of proceeds of crime and extradition.~~
- (20) The Convention provides a basis for voluntary capacity building measures to support countries in their ability to conduct effective cybercrime investigations and proceedings and to obtain electronic evidence for investigations and proceedings of other offences, including by means of technical assistance and training. The UNODC has a clearly described role for the implementation of such measures.
- (21) The Convention takes due account of the position of natural and legal persons as victims of cybercrime. The Convention ensures that these victims of cybercrime receive appropriate assistance, support, and protection **and provide access to compensation.**

- (22) The Convention provides a basis for practical measures for the prevention of cybercrime that are clearly defined and strictly limited and distinct from criminal procedural measures that could interfere with the rights and freedoms of individuals or legal persons.

Regarding the functioning of the Convention, the Union should aim to achieve that:

- (23) The Convention preserves existing global and regional instruments and ongoing international cooperation in the global fight against cybercrime. In particular, the European Union Member States, in their mutual relations, are able to continue to apply the rules of the European Union.
- (24) The Convention provides for an appropriate mechanism to ensure its implementation and provide for final provisions, including on the settlement of disputes, signature, ratification, acceptance, approval and accession, entry into force, amendment, suspension, denunciation and depositary and languages that are modelled where possible and appropriate along the provisions of other relevant international or regional conventions in particular in the area of organised crime or cybercrime.
- (25) The Convention allows for the European Union to become a party to it.

Overall, the procedure for negotiation shall be as follows :

- (26) **The Commission should endeavour to ensure that the Convention is consistent with relevant Union legislation and policies, as well as the Union's commitments under other relevant multilateral agreements.**
- (27) **The Commission should conduct negotiations on behalf of the Union, for matters falling within its competence, in accordance with the Treaties, and in respect of which the Union has adopted rules.**
- (28) **The negotiations, including each negotiation round, must be prepared well in advance. To this end, the Commission shall inform the Council of the schedule anticipated and the issues to be negotiated and shall share the relevant information as early as possible.**

- (29) In accordance with the principle of sincere cooperation, the Commission and the Member States should cooperate closely during the negotiation process, including through regular contacts with the Member States' technical experts and representatives in Vienna and New-York, and Member States should actively participate to the negotiating process.
- (30) The negotiating sessions shall be preceded by a meeting of the Working Party on Judicial Cooperation in Criminal Matters in order to identify the key issues, formulate opinions and provide guidance, as appropriate.
- (31) The Commission shall report to the Working Party on Judicial Cooperation in Criminal Matters on the outcome of the negotiations after each negotiating session, including in writing.
- (32) The Commission shall inform the Council and consult Working Party on Judicial Cooperation in Criminal Matters on any important issue that may arise during the negotiations.
-