



Brussels, 29.3.2022
COM(2022) 132 final

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**

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Cybercrime continues to be a growing threat to the security of citizens and businesses in the European Union (EU) according to the Europol Internet Organised Crime Threat Assessment.¹ Cybercrime is a global and borderless phenomenon, and stepping up international cooperation to fight cybercrime has been a priority for countries around the world for a number of years.

The 2001 Council of Europe Convention on Cybercrime (the ‘Budapest Convention’) is the first international treaty on cybercrime, defining cybercrime-related offences, providing for a series of powers and procedures to investigate cybercrime, such as the search of computer networks and interception, and secure electronic evidence in relation to any crime, and establishing a framework for international cooperation.² The Budapest Convention is open to non-Council of Europe members, and countries from all geographical regions have acceded to it. To date, there are 66 State Parties and fourteen additional countries have been invited to accede to it. It is the foundation for anti-cybercrime legislation in 80% of countries worldwide. The adoption of a Second Additional Protocol to the Budapest Convention by the Council of Europe’s Committee of Ministers on 17 November 2021 demonstrates the continued relevance of the Convention as a framework for international cooperation on cybercrime.³

The rise of information technology and the rapid development of new telecommunication and computer network systems and the use and abuse of technologies for criminal purposes have also featured on the agenda of the United Nations (UN). On 21 December 2010, the UN General Assembly adopted Resolution 65/230 requesting the Commission on Crime Prevention and Criminal Justice (CCPCJ) to establish an open-ended intergovernmental expert group (‘the IEG’) to conduct a comprehensive study of the problem of cybercrime.⁴ At its seventh (and last) meeting from 6-8 April 2021, the IEG took stock of all preliminary conclusions and recommendations suggested by UN Member States⁵ and agreed to transmit to the CCPCJ the 63 agreed conclusions and recommendations.⁶ In its study, the IEG did not come to a consensus about the need for a new international cybercrime treaty.

In parallel, some UN Member States stepped up their efforts to work towards such a treaty in the Third Committee deliberations of the UN General Assembly. The UN General Assembly

¹ 2021 Europol Internet Organised Crime Threat Assessment (iOCTA) www.europol.eu

² Council of Europe Budapest Convention on Cybercrime (CETS N° 185), 23 November 2001, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>.

³ [Result details \(coe.int\)](#).

[Second Additional Protocol to the Cybercrime Convention adopted by the Committee of Ministers of the Council of Europe - News \(coe.int\)](#).

⁴ General Assembly Resolution of 21 December 2010, [A/Res/65/230 - E - A/Res/65/230 -Desktop \(undocs.org\)](#).

⁵ Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020: [V2101012.pdf \(unodc.org\)](#).

⁶ Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 6 to 8 April 2021: [V2102595.pdf \(unodc.org\)](#).

consequently adopted resolution 73/187 of 17 December 2018 on ‘Countering the use of information and communications technologies for criminal purposes’.⁷ Subsequently, on 27 December 2019, the UN General Assembly adopted a second Resolution, 74/247, on the same topic, establishing an open-ended ad hoc intergovernmental committee of experts (‘the ad hoc Committee’) to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. The Resolution specified that the ad hoc Committee was to take into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the IEG.⁸ On 26 May 2021, the UN General Assembly adopted resolution 75/282 that determined the modalities for the negotiations.⁹ The UN General Assembly decided, inter alia, that the ad hoc Committee should convene at least six sessions, of 10 days each, to commence in January 2022, and a concluding session to provide a draft convention to the UN General Assembly at its seventy-eighth session in 2024. It further decided that the ad hoc Committee shall hold the first, third and sixth negotiating sessions in New York and the second, fourth and fifth sessions in Vienna. On 20 January 2022, the General Assembly decided to postpone the first session to a later date due to the Covid-19 pandemic situation in New York.

This proposal aims to ensure the appropriate participation of the European Union in these negotiations since the negotiations are expected to touch upon elements that relate to EU legislation and competence, notably in the area of cybercrime. Article 3(2) of the Treaty on the Functioning of the European Union (TFEU) provides that the Union has exclusive competence ‘for the conclusion of an international agreement (...) in so far as its conclusion may affect common rules or alter their scope.’ An international agreement may affect common rules or alter their scope where the area covered by the agreement overlaps with Union legislation or is covered to a large extent by Union law.

Given that the negotiations relate to matters of Union competence other than CFSP, which are expected to be the main components of the envisaged agreement, the Commission should be appointed as head of the negotiating team. In matters that relate to Common Foreign and Security Policy, the High Representative of the Union for Foreign Affairs and Security Policy conducts the negotiations as part of the team. The Chief Negotiator from the Commission will ensure the overall consistency of the agreement. Under the authority of the Chief Negotiator, the Commission services will be in the lead for the non-CFSP parts of the envisaged agreement and the EEAS will be in the lead for those parts of the envisaged agreements that fall under the CFSP.

This recommendation is submitted to the Council pursuant to Article 218 TFEU in order to receive authorisation to negotiate the future UN convention on behalf of the European Union, to provide negotiating directives, and to appoint the Commission as negotiator.

⁷ General Assembly Resolution of 17 December 2018, [A/RES/73/187](#).

⁸ General Assembly Resolution of 27 December 2019, [A/RES/74/247](#).

⁹ General Assembly Resolution of 26 May 2021, [A/RES/75/282*](#).

- **Consistency with existing policy provisions in the policy area**

The fight against cybercrime is a priority for the European Union as evidenced in the 2020 Security Union Strategy¹⁰, and the 2021 Organised Crime Strategy¹¹. In the 2021 Security Union third progress report, the Commission committed to ensuring effective participation of the Union in the negotiations for a comprehensive international convention on ‘countering the use of information and communications technologies for criminal purposes’ at the level of the United Nations.¹²

The Commission recognises the need to further advance and strengthen the capacities of law enforcement and judicial authorities in this field, to develop national cybercrime legislation, where not sufficiently provided. It also acknowledges the need to promote international cooperation in the fight against cybercrime and supports a range of capacity building programmes in a number of countries worldwide, including for developing countries.¹³ The Commission has supported the work of the UN Intergovernmental Expert Group on Cybercrime, the UN Commission on Crime Prevention and Criminal Justice, the United Nations Office on Drugs and Crime (UNODC), the Committee of the Budapest Convention on Cybercrime and other bodies.

The negotiations on the international convention are expected to relate to common EU rules to fight cybercrime. In particular, this may include Directive 2011/93/EU on combating the sexual exploitation of children online and child pornography¹⁴, which addresses new developments in the online environment such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse); Directive 2013/40/EU on attacks against information systems¹⁵, which aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cyber-crime laws and introduce a high level of criminal sanctions; and Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment¹⁶, which harmonises the criminal conduct of natural or legal persons in relation to non-cash means of payment and extends criminal liability to virtual currencies and digital wallets. Other EU instruments provide common rules for fighting crimes that may be enabled by the use of information systems, such as terrorism, trafficking in human beings, illicit drug trafficking, illicit arms trafficking, money laundering, corruption and organised crime.

The negotiations are also expected to cover criminal procedural and cooperation measures. The current EU legal framework includes instruments on law enforcement and judicial cooperation in criminal matters, such as the Directive 2014/41/EU regarding the European Investigation Order in criminal matters¹⁷, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union¹⁸, Regulation 2018/1727 on

¹⁰ [COM\(2020\) 605 final \(27.7.2020\)](#).

¹¹ [COM\(2021\) 170 final \(14.4.2021\)](#).

¹² [COM\(2021\) 799 final \(8.12.2021\)](#).

¹³ This includes programmes such as GLACY+, CyberEast and CyberSouth, co-funded by the EU and the Council of Europe and administered by the Council of Europe.

¹⁴ Directive 2011/93/EU (13.12.2011).

¹⁵ Directive 2013/40/EU (12.8.2013)

¹⁶ Directive (EU) 2019/713 (17.4.2019).

¹⁷ Directive 2014/41/EU (3.4.2014).

¹⁸ Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (29.5.2020)

Eurojust¹⁹, Regulation 2016/794 on Europol²⁰, Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor’s Office (‘the EPPO’)²¹, Council Framework Decision 2002/465/JHA on joint investigation teams²², Council Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings²³. The Commission’s April 2018 proposals on cross-border access to electronic evidence²⁴, and the Police Cooperation Package²⁵, currently undergoing the EU legislative procedure, are also relevant. Externally, the European Union has concluded a number of bilateral agreements with third countries, such as the Agreements on Mutual Legal Assistance between the European Union and the United States of America and between the European Union and Japan.²⁶

The Union has also adopted several directives that reinforce procedural rights of suspects and accused persons.²⁷ The protection of personal data is a fundamental right enshrined in Article 16 TFEU and in Article 8 of the Charter of Fundamental Rights of the European Union. Personal data must be processed in accordance with Regulation (EU) 2016/679 (the General Data Protection Regulation)²⁸ and Directive (EU) 2016/680 (the Police Data Protection Directive)²⁹. The fundamental right of individuals to the respect for their private and family life, home and communications is also enshrined in Article 7 of the Charter of Fundamental Rights. This includes the respect for the privacy of communications, as well as the protection of the terminal equipment of the user, as essential elements. Electronic communications data must be processed in accordance with Directive 2002/58/EC (the ePrivacy Directive).³⁰

The negotiations should ensure that the provisions of a future UN convention achieve the highest possible protection of human rights, and that Member States should be able to comply with EU law, also taking account of its future development.

- **Consistency with other Union policies**

The European Union has consistently promoted the Budapest Convention as a valuable and flexible legal framework of reference for international cooperation in the fight against

¹⁹ Regulation (EU) 2018/1727 (14.11.2018).

²⁰ Regulation (EU) 2016/794 (11.5.2016).

²¹ Council Regulation (EU) 2017/1939 (12.10.2017).

²² Council Framework Decision 2002/465/JHA (13.6.2002).

²³ Council Framework Decision 2009/948/JHA (30.11.2009).

²⁴ Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final, and Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final (17.04.2018).

²⁵ Proposal for a Council Recommendation on Police Cooperation, COM(2021)780, Proposal for a Directive on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM(2021)782, and Proposal for a Regulation on automated data exchange for police cooperation (“Prüm II”), COM(2021)784, (8.12.2021).

²⁶ Agreement on mutual legal assistance between the European Union and the United States of America (25.6.2003).

Agreement between the European Union and Japan on mutual legal assistance in criminal matters (2009).

²⁷ Directive 2010/64/EU (20.10.2010); Directive 2012/13/EU (22.05.2012); Directive 2013/48/EU (22.10.2013); Directive (EU) 2016/1919 (26.10.2016); Directive (EU) 2016/800 (11.05.2016); Directive (EU) 2016/343 (9.03.2016).

²⁸ Regulation (EU) 2016/679 (27.04.2016).

²⁹ Directive (EU) 2016/680 (27.04.2016).

³⁰ Directive 2002/58/EC (12.07.2002), amended by Directive 2009/136/EC (25.11.2009).

cybercrime. It has supported third countries in acceding to the Convention, enabling them to introduce a minimum national legal framework to combat cybercrime as well as to develop the necessary investigation and prosecution capacities, facilitating cooperation with other parties to the Convention.³¹

The EU, represented by the Commission, has also been actively involved in the negotiations for the Second Additional Protocol to the Budapest Convention.³² The Protocol will be open for signature in May 2022. Given that the matters covered by the Second Additional Protocol are covered by Union exclusive competence, on 25 November 2021, the Commission adopted two proposals for Council Decisions to authorise EU Member States to sign³³ and to ratify³⁴, in the interest of the European Union, the Second Additional Protocol to the Budapest Convention on Cybercrime.

The negotiations will therefore also need to ensure consistency and coherence with the Budapest Convention on Cybercrime and its Additional Protocols.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

Article 218(3) of the Treaty on the Functioning of the European Union (TFEU) provides that the Commission shall submit recommendations to the Council, which shall adopt a decision authorising the opening of negotiations and nominate the Union negotiator. According to Article 218(4) of the TFEU, the Council may address directives to the negotiator.

- **Subsidiarity (for non-exclusive competence)**

Unilateral action would not provide an alternative as it would not provide a sufficient basis for cooperation with non-EU countries. Adhering to a multilateral agreement such as a possible future UN Convention, which the Union has been able to negotiate, is more efficient than entering into negotiations with individual non-EU countries at bilateral level.

- **Proportionality**

This initiative does not go beyond what is necessary to achieve the policy objectives at stake.

- **Choice of the instrument**

A Commission Recommendation for a Council Decision authorising the opening of negotiations is in line with Article 218(3) of the TFEU, which provides that the Commission shall submit recommendations to the Council, which shall adopt a decision authorising the opening of negotiations.

³¹ See e.g., Council Conclusions on Cyber Diplomacy, 10 February 2015, document 6122/15.

³² Decision of the Council authorising the European Commission to participate, on behalf of the EU, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime, reference 9116/19.

³³ Proposal for a Council Decision authorising Member States to sign, in the interest of the EU, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, COM/2021/718 final (25.11.2021).

³⁴ Proposal for a Council Decision authorising Member States to ratify, in the interest of the EU, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, COM/2021/719 final (25.11.2021).

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

Not applicable.

- **Stakeholder consultations**

The Commission published a call for evidence for this initiative on its website on 14 January 2022, which was available for comments for four weeks. The (five) individual responses to the call for evidence were published on the consultation website. These considerations have been taken into account in the preparation of the present proposal.

- **Collection and use of expertise**

The Commission took into account views expressed by Member State experts during discussions in the relevant Council working groups in the preparation of the negotiations.

- **Impact assessment**

Not applicable.

- **Regulatory fitness and simplification**

Not applicable.

- **Fundamental rights**

The negotiations are likely to cover elements that could constitute an interference with fundamental rights such as procedural criminal measures, definitions of criminal offences that may be the basis for a criminal proceeding, or access to a person's private data obtained in the context of a criminal proceeding. The provisions to be negotiated may lead to interferences with e.g. the right to a fair trial, the right to privacy and the right to the protection of personal data. As the participation in the negotiations on behalf of the European Union should not compromise the level of protection of fundamental rights in the Union, this initiative proposes to pursue a high level of protection of fundamental rights.

4. BUDGETARY IMPLICATIONS

There are no budgetary implications for the Union budget. EU Member States may have one-off costs for the implementation of the Convention once the negotiations are concluded, but it is not possible to determine these costs at this stage as negotiations have not yet fully started.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The negotiations process is expected to span a period until 2024, after which the signature and conclusion of the Convention may take place. The initiative proposes to pursue a negotiation process that is open, inclusive and transparent.

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

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 218(3) and (4) thereof,

Having regard to the Recommendation from the European Commission,

Whereas:

- (1) On 27 December 2019, the United Nations General Assembly adopted resolution 74/247 on countering the use of information and communications technologies for criminal purposes, deciding to establish an 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.³⁵ The Union should participate in the negotiations on this convention.
- (2) The Union has adopted common rules that overlap with several elements being considered for such a convention. Those common rules include in particular a comprehensive set of instruments on substantive criminal law³⁶, on police and judicial cooperation in criminal matters³⁷, on minimum standards of procedural rights³⁸, as

³⁵ Resolution adopted by the General Assembly on 27 December 2019 on the report of the Third Committee (A/74/401), Countering the use of information and communications technologies for criminal purposes, [A/RES/74/247](#)

³⁶ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, [OJ L 335, 17.12.2011, p. 1–14](#); Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, [OJ L 218, 14.8.2013, p. 8–14](#); Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, PE/89/2018/REV/3, [OJ L 123, 10.5.2019, p. 18–29](#).

³⁷ Council Act of 29.5.2000 establishing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C197, 12.7.2000, p.1; Regulation (EU) 2018/1727 of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust) and repealing Council Decision 2002/187/JHA, OJ L 295, 21.11.2018; Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53; Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams, OJ L 162, 20.6.2002, p. 1; Council Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, OJ L328, 15.12.2009, p.42; Directive 2014/41/EU regarding the European Investigation Order in criminal matters, OJ L130, 1.5.2014, p.1.

³⁸ Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings, OJ L 280, 26.10.2010, p. 1; Directive

well as data protection and privacy safeguards³⁹. Future common rules should also be taken into account.⁴⁰

- (3) Therefore, a new international convention on countering the use of information and communications technologies for criminal purposes may affect common Union rules or alter their scope.
- (4) In order to protect the integrity of Union law and to ensure that the rules of international law and Union law remain consistent, it is necessary that the Union participate in the negotiations on a new international convention on countering the use of information and communications technologies for criminal purposes.
- (5) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on ...
- (6) [In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Decision and is not bound by it or subject to its application.]

[OR]

[In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European

2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, OJ L 142, 1.6.2012, p. 1; Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294, 6.11.2013, p. 1; Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, OJ L 297, 4.11.2016, p. 1; Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, OJ L 132, 21.5.2016, p. 1; Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016, p. 1.

³⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

⁴⁰ Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17 April 2018, COM/2018/225 final; Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 17 April 2018, COM/2018/226 final.

Union, and without prejudice to Article 4 of that Protocol, Ireland has notified [, by its letter of ... ,] its wish to take part in the adoption and application of this Decision.]

- (7) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Decision and is not bound by it or subject to its application.

HAS ADOPTED THIS DECISION:

Article 1

The Commission is hereby authorised to negotiate, on behalf of the Union, a comprehensive convention on countering the use of information and communications technologies for criminal purposes.

Article 2

The negotiating directives are set out in the Annex.

Article 3

The negotiations shall be conducted in consultation with a special committee to be designated by the Council.

Article 4

This Decision and its attachment will be made public immediately after their adoption.

Article 5

This Decision is addressed to the Commission.

Done at Brussels,

*For the Council
The President*