Conventions on cybercrime: The Budapest Convention and the draft UN treaty

Briefing note version 27 August 2024

1 Background

In December 2019, the United Nations General Assembly (UNGA) had adopted Resolution 74/247 establishing an Ad Hoc Committee (AHC) tasked to elaborate "a comprehensive international convention on countering the use of information and communications technologies for criminal purposes".

On 8 August 2024, the "Reconvened concluding session" of this AHC agreed on the text of a "United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes". The draft UN treaty, together with a draft resolution, will be submitted to UNGA for formal adoption before it can then be opened for signature (possibly in 2025).

The Convention on Cybercrime (Budapest Convention, BC) of the Council of Europe was opened for signature in Budapest in 2001. A first Protocol on xenophobia and racism via computer systems was opened for signature in 2003; and a Second Protocol on enhanced cooperation and disclosure of electronic evidence in 2022. The BC is followed by the Cybercrime Convention Committee (T-CY) which consists of the Parties to this treaty, and backed up by the Cybercrime Programme Office of the Council of Europe (C-PROC) for worldwide capacity building.

Given that the BC – with its currently 76 Parties and 17 States that have signed it or been invited to accede – already has broad international membership, questions may arise concerning the relation between the existing BC and the future additional UN treaty.

2 Links between the Budapest Convention on Cybercrime and the draft UN treaty

The BC provides for (i) the criminalisation of conduct, ranging from illegal access, data and systems interference to computer-related fraud and child pornography; (ii) procedural powers to investigate cybercrime and secure electronic evidence in relation to any crime, and (iii) efficient international cooperation. The first Protocol provides for the criminalisation of xenophobia and racism via computer systems. The Second Protocol offers more effective and efficient means to obtain electronic evidence across borders, including through direct cooperation with service providers or the expedited disclosure of data in emergency situations.

Most of the provisions of the BC have been replicated in the draft UN treaty:

- The underlying definitions of Articles 1 and 18 of the BC ("computer system", "computer data", "service provider", "traffic data", "subscriber information") are identical with or similar to those of Article 2 of the draft UN treaty.

- In terms of criminalisation, the offences in Articles 7 to 14 of the draft UN treaty are more or less identical with those of Articles 2 to 9 of the BC. For example, "illegal access" in Article 2

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

BC corresponds to "illegal access" in Article 7 of the draft UN treaty, etc. The draft UN treaty goes beyond the BC, in that it criminalises the solicitation of children for sexual offences (Article 15) and the non-consensual dissemination of intimate images (Article 16). These articles add value to the UN treaty. It also covers money laundering (Article 17). On the other hand, the draft UN treaty does not cover offences related to copyright infringements. The articles of the draft UN treaty on the liability of legal persons (Article 18) and on participation and attempt (Article 19) have been adapted from the UN Convention on Transnational Organised Crime (UNTOC) and the United Nations Convention on Corruption (UNCAC). The thresholds and intent standards of these provisions are lower than those of corresponding articles of the BC.

- The procedural powers of Articles 23 to 30 of the draft UN treaty to investigate and prosecute cybercrime and to collect electronic evidence are again more or less identical with those of Articles 14 to 21 BC, including with respect to their scope and safeguards. The draft UN treaty comprises a few additional measures that have been adapted from UNCAC and UNTOC, such as the confiscation of crime proceeds or witness protection.

- The provisions of the draft UN treaty on international cooperation that are specific to computer systems and data (Articles 41 to 46) reproduce again corresponding articles of the BC. For example, the expedited preservation of data of Article 42 in the draft UN treaty corresponds to Article 29 BC; the 24/7 network in Article 41 of the draft UN treaty is derived from Article 35 BC, etc. The general provisions on international cooperation (general principles relating to international co-operation, extradition etc.) of the draft UN treaty have been adapted from UNTOC and UNCAC. None of the advanced tools for cross-border cooperation to obtain electronic evidence of the Second Protocol to the BC have been included in the draft UN treaty.

The scope of the draft UN treaty is both broader and narrower than that of the BC: Unlike the BC, the draft UN treaty also refers to crime prevention as well as the freezing, seizure, confiscation and return of the proceeds.

However, the international cooperation provisions of the BC (and its Second Protocol) are applicable to electronic evidence of any criminal offence, while the draft UN treaty is limited by a serious crime threshold where offences are not established in accordance with this treaty.

The AHC reached agreement on the draft UN treaty because it comprises safeguards beyond those of UNTOC and UNCAC. These include in particular:

- Article 6 on "respect for human rights" with its important paragraph 2;
- Article 21.4 with procedural guarantees;
- Article 24 on conditions and safeguards, which is similar to Article 15 BC, but with the addition of paragraph 4;
- Article 36 on the protection of personal data;
- Article 40.22 on non-discrimination within the context of mutual legal assistance.

Without these minimum safeguards, the AHC process would have failed or the scope of the draft UN treaty would have had to be narrowed down considerably. Adherence by Parties to these safeguards will be essential to permit international cooperation under this future UN treaty.

The draft UN treaty contains a number of articles that are not specifically foreseen in the BC or its Protocols, such as those of chapter VI on preventive measures or of chapter VII on technical assistance and information exchange.

On the other hand, the Council of Europe has carried out capacity building activities on cybercrime for more than 20 years even without a reference to it in the BC. With the establishment of the dedicated C-PROC in Bucharest in 2014, the Council of Europe has become a global leader for capacity building in this field.

3 Conclusion

Agreement by the AHC on the draft "United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes" is a major political achievement given the current international context.

The draft UN treaty represents a narrow criminal justice treaty that is largely consistent with the BC and that contains minimum safeguards necessary for international cooperation.

The core concepts and measures of the draft treaty are drawn from the BC on Cybercrime (2001) complemented by provisions adapted from the UN Conventions on Transnational Organised Crime (UNTOC, 2000) and Corruption (UNCAC, 2003).

The draft treaty thus confirms the timeless quality and relevance of the BC.

New provisions adding value to the draft UN treaty are the articles on the solicitation or grooming of children for sexual offences (Article 15) and on the non-consensual dissemination of intimate images (Article 16).

None of the advanced tools of the Second Protocol to the BC for enhanced cooperation and disclosure of electronic evidence (2022) have been included in the draft UN treaty.

The scope of application of the BC and its Second Protocol is broader in that the provisions on international cooperation are applicable to electronic evidence of any offence, while the draft UN treaty has a serious crime threshold.

While the draft UN treaty comprises human rights and rule of law safeguards beyond those of UNTOC and UNCAC, it also carries risks: A number of States expressed their disagreement with these requirements during AHC sessions. Concerns presented by civil society and industry stakeholders regarding risks of misuse of this treaty remain valid. It remains to be seen how compliance with safeguards can be ensured. The decision foreseen in the draft UNGA resolution to start work on a supplementary protocol within two years of adoption of the treaty to consider additional offences provides some States with a further opportunity to promote information control.

Parties to the BC that have also ratified UNCAC and UNTOC should be able to implement the UN treaty without requiring major changes in domestic legislation. For them, the UN treaty may serve as an additional instrument permitting them to cooperate with other States that for varying reasons are not able to join the BC.

States that first become Parties to the UN treaty may over time use that experience to also seek accession to the BC and its Protocols.

Synergies between the UN treaty and the BC should be feasible, in particular through capacity building activities between the Council of Europe's C-PROC and the United Nations Office on Drugs and Crime (UNODC). This may include support to the preparation of domestic legislation with particular attention to conditions and safeguards.

It will take some years before the UN treaty will be in force and operational. In the foreseeable future, the BC with its Protocols will remain the more relevant and trusted framework for cooperation on cybercrime and electronic evidence.

The AHC process generated considerable additional interest in the BC and its Protocols as reflected in the number of accessions since February 2022, and more States are expected to join this framework in the future.

Considering the experience of the AHC, a clear commitment to meeting human rights and rule of law conditions will be necessary when governments are seeking accession to the Budapest Convention on Cybercrime.

4 Contact

Council of Europe
Cybercrime Division
Strasbourg, France
Email cybercrime@coe.int

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE