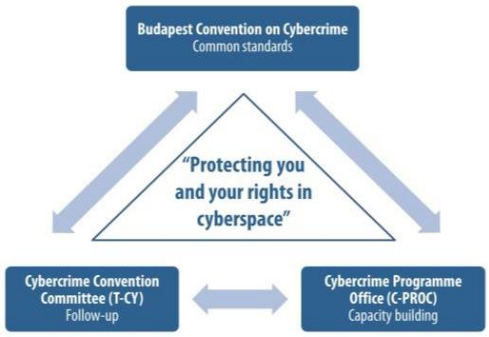
Version 14 April 2021

Enhanced cooperation on cybercrime and electronic evidence:

Towards a Protocol to the Budapest Convention

The Budapest Convention on Cybercrime was opened for signature in 2001. Membership in this treaty increases continuously and any country able to implement its provisions may seek accession. By April 2021, 65 States had become Parties and a further 12 had signed it or been invited to accede. In addition to these 77 States a further 30 are believed to have legislation largely in line with this treaty and a further 50 to have drawn on it at least partially. The Budapest Convention is supplemented by an additional Protocol on Xenophobia and Racism committed via computer systems.



The quality of implementation is assessed by the Cybercrime Convention Committee (T-CY) representing the Parties to the Budapest Convention, with signatories and States invited to accede participating as observers.

States committed to cooperate under this Convention are furthermore supported through capacity building projects managed by a dedicated Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania.

The evolution of information and communication technologies – while bringing unprecedented opportunities for mankind – also raises challenges, including for criminal justice and thus for the rule of law in cyberspace. While cybercrime and other offences entailing electronic evidence on computer systems are thriving and while such evidence is increasingly stored on servers in foreign, multiple, shifting or unknown jurisdictions, that is, in the cloud, the powers of law enforcement are limited by territorial boundaries. As a result, only a very small share of cybercrime that is reported to criminal justice authorities is leading to court decisions, and most often victims do not obtain justice.

The Parties to the Budapest Convention have been searching for solutions for some time, that is, from 2012 to 2014 through a working group on transborder access to data and from 2015 to 2017 through the Cloud Evidence Group. In 2014, they also adopted a set of Recommendations to enhance the effectiveness of mutual assistance, and in 2017 a Guidance Note on Article 18 Budapest Convention on production orders with respect to subscriber information. This Note explains how domestic production orders for subscriber information can be issued to a domestic provider irrespective of data location (Article 18.1.a) and to providers offering a service on the territory of a Party (Article 18.1.b).

The Cloud Evidence Group in 2017 recommended the preparation of a new, second additional Protocol to the Budapest Convention. In June 2017, the T-CY agreed on the Terms of Reference for the preparation of the Protocol and negotiations commenced in September 2017. Since then, the T-CY held 9 Protocol Drafting Plenaries and 16 Protocol Drafting Group sessions to prepare the text of the draft Protocol. And further to COVID-19 related restrictions, between April 2020 and April 2021 over 50 meetings of subgroups of the Protocol Drafting Group were held in virtual format.

Whenever draft Articles had been provisionally agreed upon by the Protocol Drafting Plenary, they were made public, and civil society, data protection and industry stakeholders were invited to submit comments or participate in hearings. Five rounds of such consultations were held between July 2018 and December 2020. Many of the contributions received have been taken into account in the operative text or have led to additional clarifications in the explanatory report.

On 12 April 2021, the Protocol Drafting Plenary agreed to publish a complete draft of the Protocol and to invite stakeholders to provide further comments and participate in an online meeting on 6 May 2021.

The draft "Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence" provides for:

- Direct cooperation with service providers (Article 6) and entities providing domain name registration services (Article 7) in other Parties for the disclosure of information to identify suspects;
- Expedited forms of cooperation between Parties for the disclosure of subscriber information and traffic data (Article 8);
- Expedited cooperation and disclosure in emergency situations (Articles 9 and 10);
- Additional tools for mutual assistance (Articles 11 and 12);
- Data protection and other rule of law safeguards (Articles 13 and 14).

The scope of this Protocol – like that of the Convention on Cybercrime – is limited "to specific criminal investigations or proceedings concerning criminal offences related to computer systems and data, and to the collection of evidence in electronic form of a criminal offence" (Article 2).

In addition to Articles 13 and 14, a range of other safeguards has been built into individual provisions, and Parties to this Protocol may make use of reservations and declarations if required under their domestic law. For example, they may require simultaneous notification when an order is sent directly to a service provider in their territory (see Article 7, paragraph 5).

As a result, the current draft reconciles (a) the need for an effective criminal justice response to strengthen the rule of law and protect victims and their rights online, and (b) the need for strong human rights and rule of law safeguards, including for the protection of personal data.

The provisions of this Protocol will be of operational and policy benefit and will ensure that the Budapest Convention continues to stand for a free Internet where governments meet their obligation to protect individuals and their rights in cyberspace.

It is expected that the Protocol will be finalized and adopted in the course of 2021.

For further information please contact

Secretariat of the Cybercrime Convention Committee
Cybercrime Division, DGI
Council of Europe
Strasbourg, France
Email cybercrime@coe.int

www.coe.int/cybercrime