COUNCIL OF EUROPE

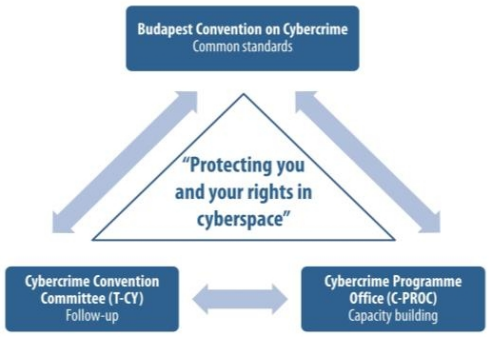
CONSEIL DE L'EUROPE

Version 19 March 2018

Enhanced international 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 March 2018, 56 States had become Parties and a further 15 had signed it or been invited to accede. In addition to these 71 States a further 25 are believed to have legislation largely in line with this treaty and a further 45 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.

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. The latter proposed that the following specific issues be addressed:

- the need to differentiate between subscriber, traffic and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations;
- the limited effectiveness of mutual legal assistance for securing volatile electronic evidence;
- situations of loss of (knowledge of) location of data and the fact that States increasingly resort to unilateral transborder access to data in the absence of international rules;
- the question as to when a service provider is sufficiently present or offering a service in the territory of a Party so as to be subject to the enforcement powers of that Party;
- the current regime of voluntary disclosure of data by US-providers which may help law enforcement but also raises concerns;
- the question of expedited disclosure of data in emergency situations;
- data protection and other rule of law safeguards.

Further to the results of the Cloud Evidence Group, the T-CY adopted the following Recommendations:

1. Enhancing the effectiveness of the mutual legal assistance process by implementing earlier Recommendations adopted by the T-CY in December 2014.
2. 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).
3. Full implementation of Article 18 by Parties in their domestic law.
4. Practical measures to enhance cooperation with service providers.
5. Negotiation of a 2nd Additional Protocol to the Budapest Convention on enhanced international cooperation.

In June 2017, the T-CY agreed on the Terms of Reference for the preparation of the Protocol during the period September 2017 and December 2019. The following elements are to be considered:

A. Provisions on more efficient mutual legal assistance (such as expedited MLA for subscriber information, international production orders, joint investigations, emergency procedures etc.).
B. Provisions on direct cooperation with providers in other jurisdictions.
C. Framework and safeguards for existing practices on transborder access to data.
D. Rule of law and data protection safeguards.

The T-CY agreed to extend regular plenary meetings for negotiation of the Protocol and to establish a "Protocol Drafting Group" to work on text in between plenary sessions.

Protocol Drafting Group meetings were held in September 2017 and February 2018 while a Protocol Drafting Plenary was held in November 2017. It was agreed among other things,

- to engage in close consultation with civil society, data protection organisations and industry during the drafting process. Specific meetings will be organised for this purpose once draft concepts and text are available. The Octopus Conference from 11 to 13 July 2018 will also be an opportunity for an exchange of views;
- that, taking note of developments at the level of the European Union regarding electronic evidence and criminal justice in cyberspace, "close coordination in the drafting of the Additional Protocol to the Budapest Convention and the preparation of relevant legal instruments by the European Union should be pursued".

The next Drafting Group meeting will take place on 11-13 May and the Drafting Plenary on 10-11 July 2018.

The matters to be resolved are complex and it may be difficult to reach consensus on the options currently on the table. However, unless solutions are agreed upon, governments may be less and less able to maintain the rule of law to protect individuals and their rights in cyberspace.

For further information please contact

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