COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

The Budapest Convention on Cybercrime at 15: Achievements and challenges

Achievements

The Convention on Cybercrime was opened for signature in Budapest, Hungary, in November 2001. It is a criminal justice treaty that requires Parties (a) to criminalise a set of offences against and by means of computers in their domestic law, (b) to provide their law enforcement authorities with powers to secure electronic evidence in relation to any crime, while limiting these powers by rule of law safeguards, and (c) to engage in effective international cooperation.

The Budapest Convention is backed up by the Cybercrime Convention Committee (T-CY) which represents the Parties to this treaty, and by the Cybercrime Programme Office of the Council of Europe (C-PROC) which supports countries worldwide in the strengthening of their criminal justice capacities on cybercrime and electronic evidence.

Achievements to date include:

- The Budapest Convention has proven to be an international treaty. By November 2016, 67 States (or about one third of States worldwide) were either Parties (European countries, as well as Australia, Canada, the Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka and the USA) or had signed it or been invited to accede (European countries, Argentina, Chile, Colombia, Costa Rica, Ghana, Mexico, Morocco, Paraguay, Peru, Philippines, Senegal, South Africa and Tonga). More countries are expected to join in the future.

- The treaty has helped countries worldwide develop a more consistent approach to legislation on cybercrime and electronic evidence. In addition to the States which are already Parties or committed to join, another third of all States have made use of the Budapest Convention as a guideline, or at least as a source of inspiration, when developing domestic legislation.

- In countries that have implemented the Budapest Convention an increase in criminal investigations and prosecutions on cybercrime and other offences involving electronic evidence is noted.

- International cooperation, that is, police-to-police and judicial cooperation improved considerably between many of the Parties to the Budapest Convention. All Parties have functioning 24/7 points of contact in line with Article 35.

- States that have joined the Budapest Convention have not just limited themselves to implementing the provisions of this treaty. Membership in the Budapest Convention is an indicator for political commitment to counter cybercrime and to strengthen cybersecurity.

- Guidance Notes help address new phenomena and keep the Convention relevant in an effective way through provisions already available in the treaty. Examples include Notes on "distributed denial of service attacks", "botnets", "identity theft" or "new forms of malware". Guidance Notes are adopted by the Cybercrime Convention Committee and represent the common understanding of the Parties.

- The quality of implementation of the Convention keeps increasing due to assessments carried out and Guidance Notes adopted by the Cybercrime Convention Committee.

- The Convention may be complemented through Protocols. In 2003, a Protocol on Xenophobia and Racism committed through computer systems was adopted. This Protocol also helps to address radicalization and violent extremisms leading to terrorism. By November 2016, it had been ratified by 24 and signed by another 15 States. Proposals to negotiate another Protocol are currently under consideration by the Cybercrime Convention Committee.

– The Convention serves as a catalyst for capacity building. Not only the Council of Europe, but also major donors such as the European Union now recognize that measures against cybercrime contribute to the rule of law and help countries make use of the development opportunities of information and communication technologies. In 2014, the Council of Europe established a Cybercrime Programme Office (C-PROC) in Romania responsible for worldwide capacity building to help States to implement the Budapest Convention and to follow up on recommendations of the Cybercrime Convention Committee. By November 2016, C-PROC was implementing projects with a volume of some EUR 20 million.

– Governments have a positive obligation to protect people through effective laws and law enforcement measures, for example, by implementing the Budapest Convention as noted by the European Court of Human Rights. Article 15 helps strike a fair balance between the need for effective law enforcement and procedural safeguards. The Convention is about "protecting you and your rights in cyberspace".

In a context where international agreement on matters regarding cyberspace is difficult to achieve, the Budapest Convention is in place and functioning and is scalable in terms of membership and contents.

Meeting new challenges

The scope, scale and complexities of cybercrime and e-evidence keep increasing. Access to electronic evidence on servers in foreign, multiple, shifting or unknown jurisdictions – that is, servers "in the cloud" – while at the same time meeting rule of law requirements is essential. Without data, no evidence, no justice and no rule of law. Proposals to address this challenge have been prepared by the Cloud Evidence Group of the Cybercrime Convention Committee:

1. Rendering mutual legal assistance more efficient.
2. Guidance Note on production orders for subscriber information (Article 18 Budapest Convention).
3. Review of domestic procedures for production orders, that is, full implementation of Article 18.
4. Practical measures to facilitate cooperation between service providers and criminal justice authorities.
5. Negotiation of a Protocol to the Budapest Convention.

Way ahead

During its first 15 years, the Budapest Convention evolved in 5-year cycles:

- During the first five years (2001 – 2006), the Convention was ratified by a sufficient number of countries to enter into force. The Protocol on Xenophobia and Racism was opened for signature.
- Between 2006 and 2011, the Cybercrime Convention Committee was established and the Global Project on Cybercrime was launched to reach out to States outside Europe.
- Between 2011 and 2016, following the tenth anniversary of the Convention, the Cybercrime Convention Committee began to assess implementation by the Parties, to adopt Guidance Notes and to set up working groups on transborder access to data and on access to evidence in the cloud. Capacity building activities expanded and the C-PROC was established. The dynamic triangle of common standards (Budapest Convention), follow up and assessments (T-CY) and capacity building (C-PROC) became fully operational.

The 15th anniversary has the potential of becoming another turning point. Should the Parties reach agreement on the negotiation of a Protocol to enhance the effectiveness of mutual legal assistance and to address the problem of criminal justice access to evidence in the cloud, this would determine the course of the Budapest Convention in the coming years.