Version 16 December 2022

Joining the Convention on Cybercrime: Benefits

The Convention on Cybercrime

The Convention on Cybercrime ("Budapest Convention") is regarded as the most comprehensive and coherent international agreement on cybercrime and electronic evidence to date. It serves as a guideline for any country developing domestic legislation on cybercrime and as a framework for international cooperation between State Parties to this treaty.

The Budapest Convention 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) for efficient international cooperation. The treaty is open for accession by any country.

The Convention is supplemented by a first Additional Protocol covering the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189) and a Second Additional Protocol on enhanced international cooperation and disclosure of electronic evidence (CETS 224) which was opened for signature on 12 May 2022[1].

States which participated in the negotiation of the Convention (members of the Council of Europe, and Canada, Japan, South Africa and USA) can sign and ratify the treaty. Under Article 37 any other State can become a Party by "accession" if the State is prepared to implement the provisions of this treaty.

The accession procedure involves:

1. Once a (draft) law is available that indicates that a State already has implemented or is likely to implement the provisions of the Budapest Convention in domestic law, the Minister of Foreign Affairs (or another authorised representative) would send a letter to the Secretary General of the Council of Europe stating the interest of his or her State to accede to the Budapest Convention.
2. Once there is agreement among the current Parties to the Convention, the State would be invited to accede.
3. The authorities of that State would complete their internal procedures similar to the ratification of any international treaty before depositing the instrument of accession at the Council of Europe.

Whether becoming a Party through ratification or accession, the end-result is the same. Parties to the Convention can also become Parties to the two Protocols without the need for a further request for accession.

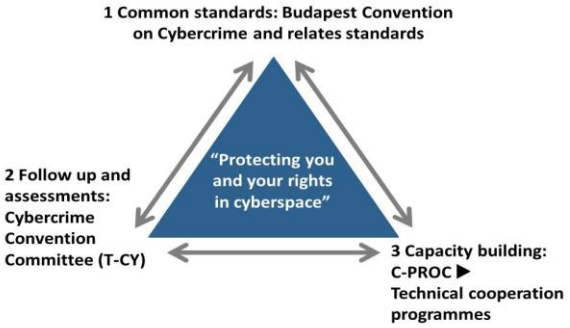
By December 2022, 68 States were Parties to the Convention (European countries as well as Argentina, Australia, Brazil, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ghana, Israel, Japan, Mauritius, Morocco, Nigeria, Panama, Paraguay, Peru, Philippines, Sri Lanka, Senegal, Tonga and the USA), an additional 2 countries had signed it (Ireland and South Africa), and 13 countries had been invited to accede (Benin, Burkina Faso, Côte d'Ivoire, Ecuador, Fiji, Guatemala, Mexico, New Zealand, Niger, Timor-Leste, Trinidad and Tobago, Tunisia and Vanuatu).

[1] As of December 2022, the 2nd Additional Protocol has been signed by 30 Parties to the Convention: Andorra, Austria, Belgium, Bulgaria, Chile, Colombia, Costa Rica, Croatia, Estonia, Finland, Iceland, Italy, Japan, Lithuania, Luxembourg, Moldova, Montenegro, Morocco, Netherlands, North Macedonia, Portugal, Romania, Serbia, Slovenia, Spain, Sri Lanka, Sweden, Ukraine, the United Kingdom and the United States of America

These 83 States participate as members (Parties) or observers (signatories or invitees) in the Cybercrime Convention Committee (T-CY).

The T-CY, among other things assesses implementation of the Convention by the Parties, adopts Guidance Notes or prepares additional legal instruments.

Capacity building programmes – managed by the specialised Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania – help countries worldwide to build the necessary capacities to implement the Budapest Convention, its protocols or to follow up to recommendations of the Cybercrime Convention Committee.



Benefits for Parties

Any country may make use of the Convention on Cybercrime as a guideline, check list or model law, and a large number already makes use of this opportunity. However, becoming a Party to this treaty entails additional advantages:

- The Convention provides a **legal framework for international cooperation** not only with respect to cybercrime (offences against and by means of computers) but with respect to any crime involving electronic evidence.
- Parties to the Convention can sign and ratify the Second Additional Protocol to the Budapest Convention, which provides **additional and expedited tools for enhanced cooperation and disclosure of electronic evidence**, such as direct cooperation with service providers across borders or cooperation in emergency situations.
- Parties are **members of the Cybercrime Convention Committee (T-CY)** and share information and experience, assess implementation of the Convention, or interpret the Convention through Guidance Notes.
- Even if a State did not participate in the negotiation of the original treaty, a new Party is able to participate in the **negotiation of future instruments** and the further evolution of the Convention.
- Parties to the Convention engage with each other in **trusted and efficient cooperation**. Indications are that private sector entities as well are more likely to cooperate with criminal justice authorities of Parties to the Convention given that Parties need to have a domestic legal framework on cybercrime and electronic evidence in place, including the safeguards of Article 15.
- States requesting accession or having acceded may become **priority countries for capacity building** programmes. Such technical assistance is to facilitate full implementation of the Convention and to enhance the ability to cooperate internationally.

Experience after more than 20 years since the opening for signature indicates that there are no disadvantages in joining this treaty

Contact

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

www.coe.int/cybercrime