Version 6 December 2023

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 co-operation 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 co-operation. 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 co-operation and disclosure of electronic evidence (CETS 224).

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.

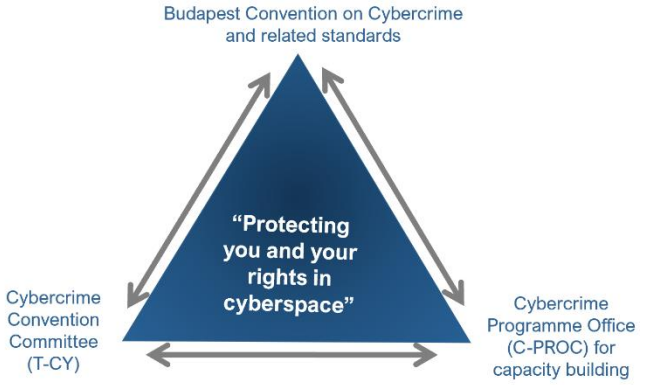
Whether becoming a Party through ratification or accession, the end-result is the same. Parties to the Convention can also become Parties to the two Protocols without the need for a further request for accession.

By September 2023, 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 21 countries had been invited to accede (Benin, Burkina Faso, Cameroon, Côte d'Ivoire, Ecuador, Fiji, Guatemala, Kazakhstan, Kiribati, Korea, Mexico, New Zealand, Niger, Rwanda, São Tomé and Príncipe, Sierra Leone, Timor-Leste, Trinidad and Tobago, Tunisia, Uruguay and Vanuatu).

These 89 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 co-operation** 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 co-operation and disclosure of electronic evidence**, such as direct co-operation with service providers across borders or co-operation 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 co-operation**. Indications are that private sector entities as well are more likely to co-operate 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 co-operate internationally.

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

The First Additional Protocol on xenophobia and racism

The First Additional Protocol covering the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189) entails an extension of the Cybercrime Convention's scope, including its substantive, procedural and international co-operation provisions, so as to cover also offences of racist or xenophobic propaganda. Thus, apart from harmonising the substantive law elements of such behaviour, the

Protocol aims at improving the ability of the Parties to make use of the means and avenues of international co-operation set out in the Convention in this area.
Benefits for Parties are:

- A stronger legal framework: the Protocol strengthens the legal framework for countering xenophobia and racism in cyberspace by providing a clear set of guidelines for the criminalisation of these crimes.
- Enhanced international co-operation: the Protocol promotes international co-operation in the investigation and prosecution of crimes relates to xenophobia and racism online, which is particularly important given the cross-border nature of many of these offences.
- Increased protection for victims: criminalisation of xenophobia and racism online permits victims to seek justice and receive support.

The First Additional Protocol was opened for signature on 23 January 2003. As of September 2023, 35 States were Parties and a further 10 had signed the First Protocol.

The Second Additional Protocol on electronic evidence

Considering the proliferation of cybercrime and the increasing complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, 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. As a response, the Second Additional Protocol to the Convention on Cybercrime (CETS 224) provides a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards.

Key features of the Protocol include:

- Direct request to registrars in other jurisdictions to obtain domain name registration information.
- Direct orders to service providers in other jurisdictions to obtain subscriber information.
- More effective means to obtain subscriber information and traffic data through government-to-government co-operation.
- Expedited co-operation in emergency situations.
- Joint investigation teams and joint investigations.
- Video conferencing.

The Second Additional Protocol was opened for signature on 12 May 2022. As of September 2023, 42 States had signed the Second Protocol (Albania, Andorra, Argentina, Austria, Belgium, Bulgaria, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Croatia, Dominican Republic, Estonia, Finland, France, Germany, Ghana, Greece, Hungary, Iceland, Italy, Japan, Lithuania, Luxembourg, Malta, Mauritius, Montenegro, Morocco, Netherlands, North Macedonia, Portugal, Republic of Moldova, Romania, Serbia, Slovenia, Spain, Sri Lanka, Sweden, Ukraine, United Kingdom and the United States of America) and two States had also ratified it (Japan and Serbia).

Contact

Council of Europe
Cybercrime Division, DGI

Strasbourg, France
Email cybercrime@coe.int

www.coe.int/cybercrime