The Convention on Cybercrime (Budapest Convention) v. UN treaty against cybercrime
Briefing for EU m/s
Vienna, 27 February 2025

The framework of the Convention on Cybercrime (Budapest Convention)

?

"United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes"

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Alexander Seger
Head of Cybercrime Division
Council of Europe
alexander.seger@coe.int

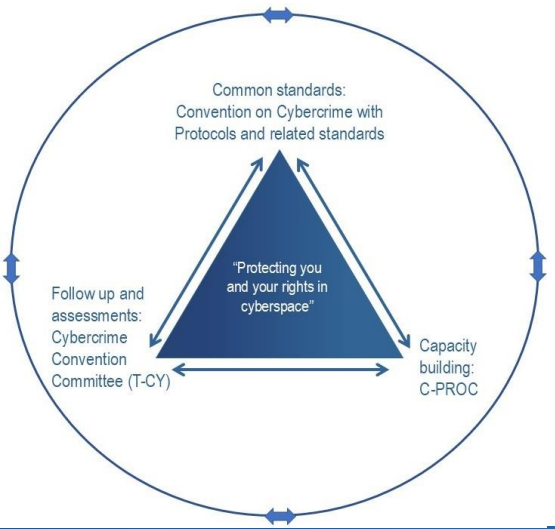
www.coe.int/cybercrime

1

The framework of the Convention on Cybercrime (Budapest Convention)

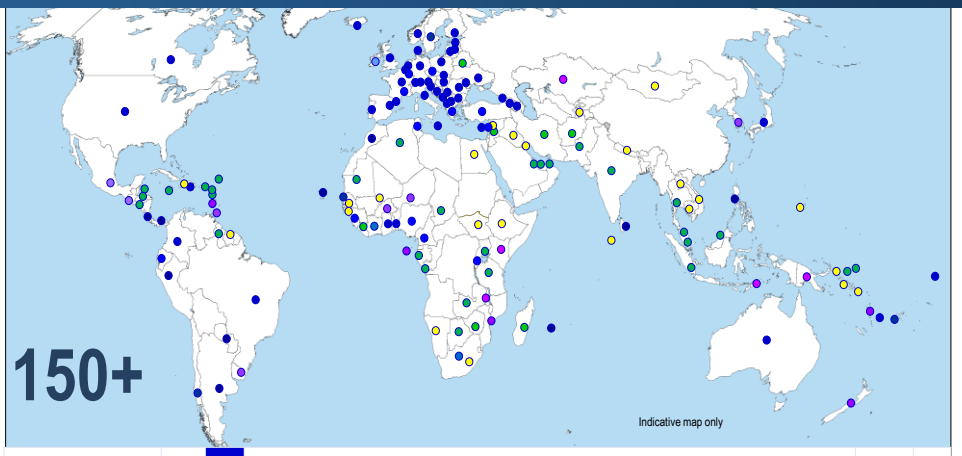
- Convention on Cybercrime (2001)
  1. Specific offences
  2. Procedural powers
  3. International cooperation
- 1st Protocol on Xenophobia and Racism via Computer Systems (2003)
- 2nd Protocol on enhanced cooperation and disclosure of electronic evidence (2022)
- Guidance Notes

By February 2025: 78 Parties and 17 "Observer States"



2

Reach of the Convention on Cybercrime



Parties:	78			
Signed:	2	Other States with substantive laws broadly in line with Budapest Convention:	35+	
Invited to accede:	15	Further States drawing on Budapest Convention for legislation:	15+	
=	**95**	=	**50+**	

3

C-PROC (2014 – 2024): 2300+ activities for 130+ countries

Cybercrime Programme Office of the Council of Europe (C-PROC)

in Romania:

- Support processes of change towards stronger criminal justice capacities on cybercrime and e-evidence in line with the Budapest Convention and with rule of law safeguards
- 7 ongoing projects with a cumulative budget of EUR 34+ million
- 50 staff
- Some 300 - 400 activities per year
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2024
- Joint projects with the European Union
- Voluntary contributions by France, Japan, UK, USA and others
- Support to T-CY

Current projects:

- ▶ Octopus Project
- ▶ GLACY-e
- ▶ CyberEast+
- ▶ CyberSouth+
- ▶ CyberSEE
- ▶ CyberUA
- ▶ CyberSPEX




ional delivery of an introductory course
ronic evidence in Benin

group of judges and prosecutors from Benin, who had
hop earlier in August, delivered for the first time an

he GLACY+ Project, organised the 9th Africa Working
om 18 to 22 July 2022. The AF-WGM is an annual
the region. This...

cybercrime and electronic evidence with the provisions of the Budapest Convention on...

4

The Convention on Cybercrime: Backed up by capacity building

Convention on Cybercrime: Ecuador becomes the 77th Party and Peru signs the Second Protocol on electronic evidence

12 DECEMBER 2024 | STRASBOURG, FRANCE

Today, 12 December 2024, Ecuador deposited the instrument of accession to the Conventio on Cybercrime (ETS 185). With Ecuador, the Convention now has 77 Parties while two have signed it and 18 have been

CyberSEE, CyberEast+, Octopus Project: Regional cybercrime exercise boosts interagency cooperation across East, South-East Europe and Türkiye

2-6 DECEMBER 2024 | TIRANA, ALBANIA

CyberSEE and CyberSouth+: Advancing justice for Online Child Protection: Regional workshop on OCSEA reporting and follow-up

28-29 NOVEMBER 2024 | ROME, ITALY

The joint initiatives of the European Union and the Council of Europe, CyberSEE and CyberSouth+ projects, with the support

CyberSouth+: Training on investigating OCSEA for law enforcement and criminal justice representatives in Morocco

19-20 FEBRUARY, 2025 | RABAT, MOROCCO

On 19-20 February 2025, the CyberSouth+ joint initiative of the European Union and the Council of Europe, with the support of MA-JUST programme, supported the delivery of a hands-on training on investigating Online Child Sexual Exploitation and Abuse (OCSEA) in Rabat, Morocco. This initiative was...

CyberSouth+: Regional training course on cybercrime and electronic evidence for women investigators and prosecutors

2-5 DECEMBER 2024 | TUNIS, TUNISIA

The CyberSouth+ joint initiative of the European Union and the Council of Europe, together

Octopus Project: Authorities of Kazakhstan coordinate on the next steps to complete accession to the Convention on

GLACY-e & INTERPOL: Completion of the 5th edition of Electronic Evidence Instructors' Workshop for english-speaking African countries

1-11 DECEMBER 2024 | KIGALI, RWANDA

INTERPOL, in the framework of the GLACY-e project and jointly with the Octopus Project of the Council of Europe, concluded its fifth edition of the Electronic Evidence National Trainers Workshop (eFR-ToT) in Kigali, Rwanda, from 1 to 11 December 2024. The workshop was attended by twenty-one...

Octopus Project: Malaysia pilots judicial training on cybercrime and electronic evidence

10 – 13 DECEMBER 2024 | PUTRAJAYA, MALAYSIA

The Office of the Chief Registrar of Malaysia and the Attorney General's Chambers of Malaysia, with the support of the Octopus Project of the Council of Europe, organised a judicial training course on cybercrime and e-evidence. The course includes two standard modules - introductory and advanced...

Regional meetings on the implementation of the Second Additional Protocol

12 - 13 FEBRUARY 2025 | TALLINN, ESTONIA

On 12 and 13 February 2025, the CyberSPEX project organised in Tallinn, Estonia, its first Regional Meeting on the implementation of the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention). This first meeting gathered Ministry of Justice representatives, advisors and...

Empowering Experts: C-PROC Launches the First Cyber-Skills Sharing Programme!

NOMINATIONS: BY 1 MARCH 2025; APPLICATIONS: BY 15 APRIL 2025 | GLOBAL

Exciting news for the cybercrime experts: the Cybercrime Programme Office (C-PROC), through the CyberSEE joint project of the European Union and the Council of Europe, is launching the first edition of the Cyber-Skills Sharing Programme! This initiative aims to enhance global collaboration and...

GLACY-e: First pool of national trainers set up in Colombia

20-21 NOVEMBER 2024 | BOGOTA, COLOMBIA

Between 20-21 November 2024, judges, magistrates, prosecutors, police and COLCERT (Colombian Cyber Emergency Response Group) representatives officially concluded the third phase of the Training of Trainers Programme supported by the GLACY-e project, a joint initiative of the European Union -...

5

UN treaty against cybercrime: structure

"United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes"

- Adopted by UNGA: 24 Dec 2024
- Opening for signature: Hanoi, Vietnam, 2025

Structure:

- Chapter I: General provisions
- Chapter II: Criminalisation
- Chapter III: Jurisdiction
- Chapter IV: Procedural measures and law enforcement
- Chapter V: International cooperation
- Chapters VI - IX: Preventive measures, Technical assistance, Mechanism of implementation, Final provisions

6

UN treaty: Core concepts adapted from Convention on Cybercrime

Core concepts and measures of the UN treaty against cybercrime

- are drawn from the Convention on Cybercrime (2001)
- complemented by provisions adapted from the UN Conventions on Transnational Organised Crime (UNTOC, 2000) and Corruption (UNCAC, 2003)

▶ confirms the timeless quality and relevance of the Convention on Cybercrime

Conventions on cybercrime: the Budapest Convention and the UN treaty

Examples:

Art.	Convention on Cybercrime	Art.	UN treaty
2	Illegal access	7	Illegal access
3	Illegal interception	8	Illegal interception
4	Data interference	9	Interference with electronic data
5	System interference	10	Interference with an information and communications technology system
6	Misuse of devices	11	Misuse of devices
7	Computer-related forgery	12	Information and communications technology system-related forgery
8	Computer-related fraud	13	Information and communications technology system-related theft or fraud
9	Child pornography	14	Offences related to online child sexual abuse or child sexual exploitation material

7

In and not in the UN treaty

New in UN treaty:

- Solicitation or grooming of children for sexual offences (Article 15)
- Non-consensual dissemination of intimate images (Article 16)
- (Adapted from UNTOC and UNCAC: measures on money laundering and crime proceeds)

NOT in UN treaty:

None of the provisions of the Convention on Cybercrime's:

- First Protocol on Xenophobia and Racism (2003)
- Second Protocol on enhanced cooperation and disclosure of electronic evidence (2022), e.g.:
  - Direct cooperation with service providers and registrars in other Parties (articles 6 and 7)
  - Expedited cooperation in emergency situations (articles 9 and 10)

8

Safeguards

Safeguards beyond UNTOC and UNCAC:

- Article 6 on "respect for human rights" with its important paragraph 2;
- Article 21.4 with procedural guarantees;
- Article 24 on conditions and safeguards, which is similar to Article 15 BC, and with the addition of paragraph 4;
- Article 36 on the protection of personal data [de facto a ground for refusal];
- Article 40.22 on non-discrimination within the context of mutual legal assistance.

9

Risks/concerns

Risks/concerns:

- Risk that some States will not respect human rights and rule of law conditions*. Conference of States Parties (COSP) unlikely to review compliance.
- Risk of targeting assets of individuals, private sector organisations, media or civil society organisations through combination of provisions on fraud, money laundering, corporate liability, participation and attempt, and crime proceeds.
- Risk of supplementary criminalisation through a protocol (negotiations to commence two years after adoption of the convention by UNGA).

► Some concerns raised by governments, civil society and industry stakeholders during the AHC and UNGA processes remain valid.

► Governments to decide on signature and ratification.

*See results of voting and disagreement expressed by some States during AHC

10

Framework of the Convention on Cybercrime v. UN treaty: synergies?

- Both treaties seem largely consistent or complementary. No obvious contradictions.
- UN treaty offers a framework for cooperation primarily between and with States not able to join the Convention on Cybercrime.
- Adherence to human rights and rule of law requirements essential to create the necessary trust for cooperation.
- Council of Europe has 20+ years experience in the implementation of provisions of the UN treaty that have been adapted from the Convention on Cybercrime.
- Synergies and cooperation between the United Nations and the Council of Europe may take the form of joint, coordinated or complementary capacity building activities by the UN Office on Drugs and Crime (UNODC) and the Council of Europe's Cybercrime Programme Office (C-PROC).

Q & A