CO-OPERATION ON CYBERCRIME & ELECTRONIC EVIDENCE

OCTOPUS CONFERENCE

Strasbourg, 4-6 June 2025

Plenary, 4 June 2025

The framework of the Convention on Cybercrime: Update

Alexander Seger, Council of Europe

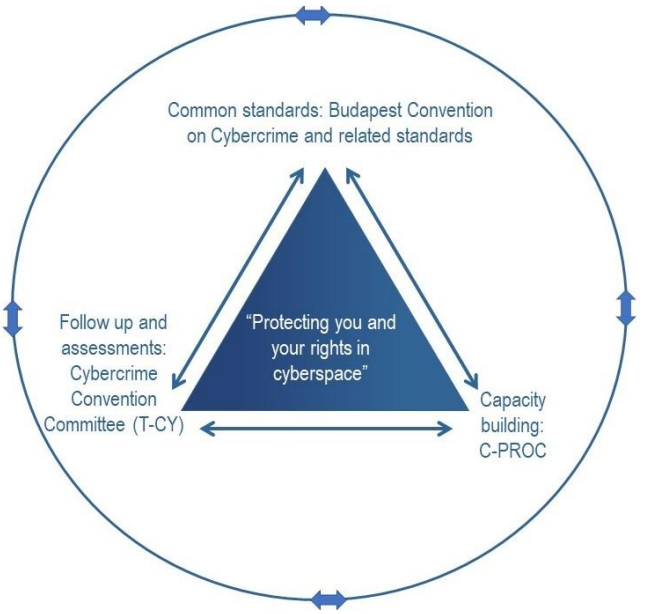
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

1

The framework of the Convention on Cybercrime

- Budapest Convention on Cybercrime (2001)
- 1st Protocol on Xenophobia and Racism via Computer Systems (2003)
- 2nd Protocol on enhanced cooperation and disclosure of electronic evidence (2022)
- Guidance Notes



2

The Convention on Cybercrime

Criminalising conduct
- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools
- Expedited preservation
- Production orders
- Search and seizure
- Interception of computer data

Limited by safeguards

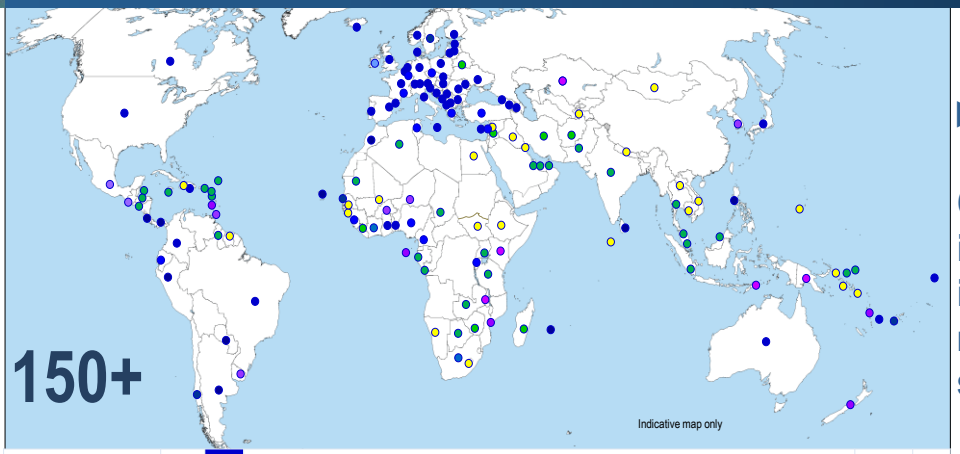
+

International cooperation
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Procedural powers and international cooperation for any criminal offence involving evidence on a computer system!

3

Reach of the Convention on Cybercrime



Parties:	78				
Signed:	2		Other States with substantive laws broadly in line with Budapest Convention:	30+	
Invited to accede:	14		Further States drawing on Budapest Convention for legislation:	15+	
=	**94**		=	**45+**	

► **NOTE:**

Considerable increase in interest and membership since 2022

4

The first Protocol on Xenophobia and Racism (ETS 189)

Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

Opening for signature 28 January 2003

Entry into force 1 March 2006

Currently 38 Parties + 9 Signatories

Key provisions

- Dissemination of racist and xenophobic material through computer systems (Article 3)
- Racist and xenophobic-motivated threat (Article 4) and insults (Article 5)
- Denial, gross minimisation, approval or justification of genocide or crimes against humanity (Article 6)
- Relation between the Convention and this Protocol (Article 8)

Need to counter increasing hate speech and hate crime online ► XR Protocol

5

Second Protocol on electronic evidence (CETS 224)

Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence

- Opened for signature May 2022
- By May 2025: 49 signatories (Japan and Serbia also ratified it)

► Make implementation in domestic law followed by ratification a priority!

6

Content of the Second Protocol on electronic evidence

Measures of the Second Protocol

Chapter II: Measures for enhanced cooperation

Article 6	Request for domain name registration information	→ Public-2-Private
Article 7	Disclosure of subscriber information	→ Public-2-Private
Article 8	Giving effect to orders from another party for expedited production of subscriber information and traffic data	→ Public-2-Public
Article 9	Expedited disclosure of stored computer data in an emergency	→ Public-2-Public
Article 10	Emergency mutual assistance	→ Public-2-Public
Article 11	Video conferencing	→ Public-2-Public
Article 12	Joint investigation teams and joint investigations	→ Public-2-Public

► Effectiveness/efficiency with data protection (Article 14) and other safeguards!

7

T-CY Guidance Notes

Guidance Notes are adopted by the Cybercrime Convention Committee (T-CY).

They represent "the common understanding of the Parties to this treaty regarding the use of the Convention".

- Computer system # 1
- Botnets # 2
- Transborder access (Article 32) # 3
- Identity Theft # 4
- DDOS attacks # 5
- Critical infrastructure attacks # 6
- Malware # 7
- Spam # 8
- Election interference # 9
- Production orders for subscriber information # 10
- Terrorism # 11
- Ransomware #12
- Scope of powers #13
- In preparation: Spontaneous information (Article 26)

8

Cybercrime Convention Committee (T-CY)

Composition:

- Parties to the Convention on Cybercrime (members)
- States that have signed it or been invited to accede (observers)
- Relevant international organisations (observers)
- Bureau + Chair + Vice-chair

Activities:

- Negotiated the Second Protocol on electronic evidence
- Assesses the implementation of the Convention by the Parties
  - ► Example: Assessment of Article 19 on search and seizure (report adopted December 2024)
- Prepares Guidance Notes to facilitate the implementation of the Convention
- Consultations with stakeholders
- Support common positions in international fora
  - ► UN treaty process ► UN Ad Hoc Committee
- Address emerging challenges
  - ► T-CY Working Group on artificial intelligence (mapping study 2025/2026
  - ► Work on virtual assets (2025/2026)

9

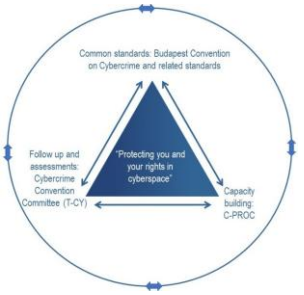
C-PROC capacity building (2014 – 2025): 2500+ activities for 140+ countries

10

C-PROC capacity building: 11 years of impact

- Thousands of criminal justice practitioners trained + capacities for training
- Contribution to human rights and rule of law in cyberspace
- Legislation:
  - 2013: 70 States with offences in line with Budapest Convention
  - 2025: 132 States
- Partnerships, synergies, trusted cooperation
- Membership in Convention on Cybercrime:
  - By 2013: 53 States were parties (41) or had signed it (2) or been invited to accede (10)
  - By May 2025: 94 States were parties (78), or had signed it (2) or been invited to accede (14)
- Successful investigations, prosecutions and international operations all over the world
- Support to the T-CY

Capacity building by C-PROC has been an essential factor for the impact and relevance of the Convention on Cybercrime …

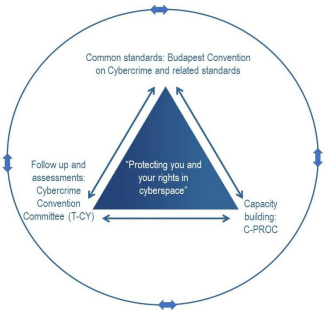


… and for criminal justice action on cybercrime globally.

11

C-PROC: Future priorities

- Implementation of the **Convention** and in particular the **Second Protocol on e-evidence**
- Strengthening **cyber resilience** (such as countering ransomware and threats to cyber security)
- Capacities to address the criminal use of **virtual assets and online fraud**.
- Addressing challenges of cybercrime and electronic evidence in relation to **artificial intelligence**.
- Capacities to address cyberviolence, including **CSAM** and **NCDII**
- Capacity building on cybercrime and e-evidence in relation to **war crime**
- Fostering an effective response to cybercrime (including **disinformation and interference with democracy**) while protecting fundamental rights, in particular the **freedom of expression**
- Synergies/implementation of the **United Nations treaty on cybercrime** ("Hanoi Convention") with a focus on **safeguards and consistency with the Budapest Convention**.



Pipeline projects in preparation

Extra-budgetary funding needed!

12

Framework of the Convention on Cybercrime 2001 – 2025: Some lessons

1. Dynamism: constant innovation

Second (e-evidence) Protocol

Octopus Conferences

New capacity building projects

Virtual assets

Artificial intelligence

Cyberviolence

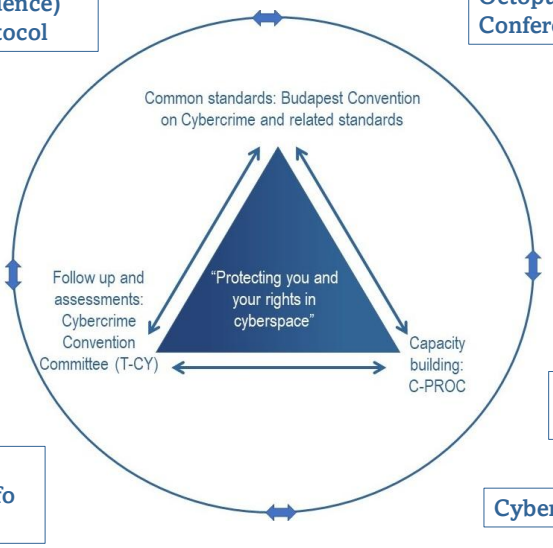
Draft GN Spontaneous info Article 26

GN Election interference

GN Election Article 18

GN Ransomware

Guidance Notes



13

Framework of the Convention on Cybercrime 2001 – 2025: Some lessons

2. Assure quality of treaty implementation & application

Treaty implementation in domestic law BEFORE ratification

Domestic legislation

Capacity building

Safeguards

Assessing implementation / compliance

Partnerships

14

Framework of the Convention on Cybercrime 2001 – 2025: Some lessons

Implement and apply safeguards

Capacity building

3. Build trust

Assess implementation of / compliance with treaty and safeguards

Engage with civil society and private sector stakeholders

Establish partnerships

Safeguards:

"What if?"

- **Refuse cooperation**
- **Apply soft power**
- **Selected counterparts**
- **Call out violations**

15

Framework of the Convention on Cybercrime: Update

16