OSCE visit to C-PROC

Bucharest, 23 November 2023

Criminal justice action on trafficking in human beings: the tools of the Budapest Convention on Cybercrime and the Second Protocol

Alexander Seger, Head of Cybercrime Division, Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

1

THB, cybercrime and e-evidence

- **Internet as enabler**
  - Recruiting victims (dating/job sites)
  - Identification of targets
  - Grooming
  - Sextortion and other forms of coercion
- **Sexual exploitation and sexual abuse of children**
  - Production, dissemination , procuring of CAM
  - Live streaming

→ **Cybercrime**

- **Cont'd exploitation**
- **Logistics of THB**
  - Communication, organisation, planning, coordination
  - Surveillance of victims
  - Forgery of documents

→ **Cybercrime**

- **Laundering proceeds from THB**
- **THB and on-line environment**
  - Attract virtual national markets (fraud, carding etc)
  - Mass audience and anonimity
  - Reduce the risk of detection

→ **Cybercrime**

2

THB, cybercrime and e-evidence

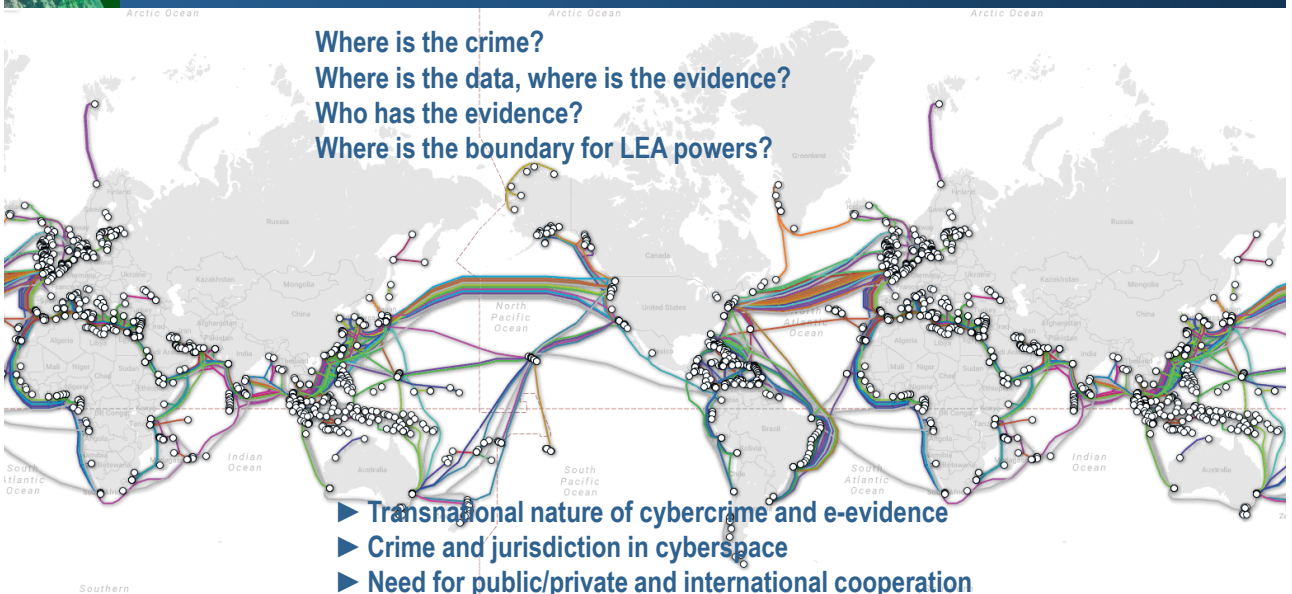
- **Internet as enabler**
  - Recruiting victims (dating/job sites)
  - Identification of targets
  - Grooming
  - Sextortion and other forms of coercion
- **Sexual exploitation and sexual abuse of children**
  - Production, dissemination , procuring of CAM
  - Live streaming
- **Cont'd exploitation**
- **Logistics of THB**
  - Communication, organisation, planning, coordination
  - Surveillance of victims
  - Forgery of documents
- **Laundering proceeds from THB**
- **THB and on-line environment**
  - Attract virtual national markets (fraud, carding etc)
  - Mass audience and anonimity
  - Reduce the risk of detection

Electronic evidence on computer systems

3

3

THB, cybercrime and e-evidence



Where is the crime?
Where is the data, where is the evidence?
Who has the evidence?
Where is the boundary for LEA powers?

- **Transnational nature of cybercrime and e-evidence**
- **Crime and jurisdiction in cyberspace**
- **Need for public/private and international cooperation**

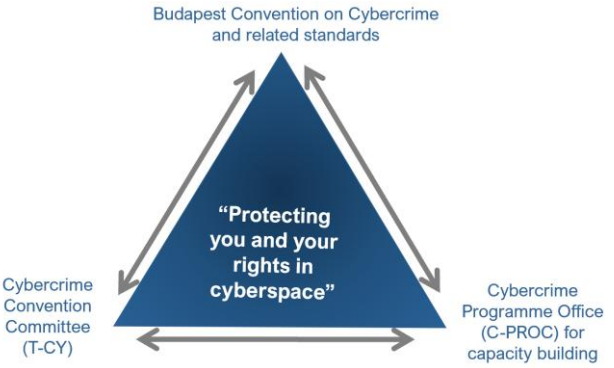
4

4

The framework of the Convention on Cybercrime

- Budapest 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 November 2023: **68 Parties and 23 Observer States**



5

The scope of the Convention on Cybercrime

Criminalising conduct	+	Procedural tools	+	International cooperation
▪ Illegal access ▪ Illegal interception ▪ Data interference ▪ System interference ▪ Misuse of devices ▪ Fraud and forgery ▪ Child pornography ▪ IPR-offences		▪ Expedited preservation ▪ Production orders ▪ Search and seizure ▪ Interception of computer data Limited by safeguards		▪ Extradition ▪ MLA ▪ Spontaneous information ▪ Expedited preservation ▪ MLA for accessing computer data ▪ MLA for interception ▪ 24/7 points of contact

Harmonisation

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

6

The scope of the Convention on Cybercrime

Cybercrime

- Offences against computer systems and data
- Offences by means of computer systems and data

+

Electronic evidence

- Any crime may involve evidence in electronic form on a computer system
- Needed in criminal proceedings
- No data, no evidence, no justice

7

The reach of the Convention on Cybercrime

Budapest Convention (2001):

By November 2023:

- Parties: 68 (European, Argentina, Australia, Canada, Chile, Costa Rica, Ghana, Japan, Mauritius, Nigeria, Philippines, Senegal, Sri Lanka, Tonga, USA etc.)
- Signatories: 2 (Ireland, South Africa)
- Invited to accede: 21 (Cameroon, Fiji, Kazakhstan, Korea, New Zealand, Uruguay, Vanuatu etc.)
- 130+ States have legislation aligned with BC

Second Protocol on enhanced cooperation and disclosure of e-evidence (2022):

By November 2023:

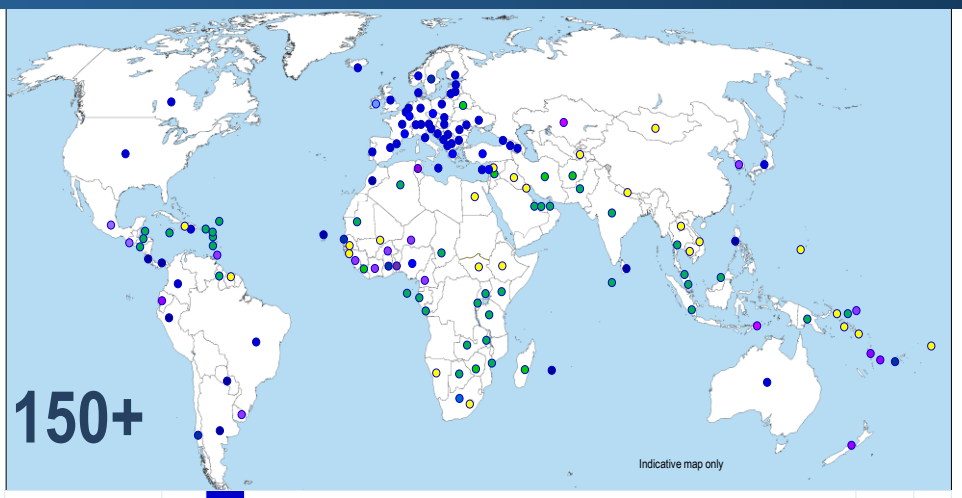
- Signed: 41 States (European, Argentina, Canada, Japan, Sri Lanka, USA etc.
- Ratified: 2 (Japan, Serbia)

(5 ratifications needed for entry into force)

8

8

The reach of the Convention on Cybercrime



Parties:	68			
Signed:	2	Other States with substantive laws broadly in line with Budapest Convention:	40+	
Invited to accede:	21	Further States drawing on Budapest Convention for legislation:	30+	
=	**91**	=	**70+**	

9

9

Convention and Protocols backed up by …

Cybercrime Convention Committee (T-CY)

- 68 members (Parties to Convention), 23 observer States, 10 observer organisations (including EUROPOL and INTERPOL)
- Plenaries and working groups
- Assessing implementation of the Convention by the Parties
- Guidance Notes to use existing provision to address new challenges
- Preparation of new instruments ▶ Protocol to the Budapest Convention

10

The Convention on Cybercrime: Backed up by capacity building


Workshop


detectives
male) incre

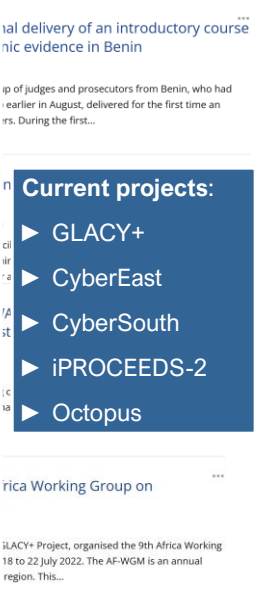

This is the


Union, hel
cybercrime

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
- 5 ongoing projects with a cumulative budget of EUR 40 million
- 40 staff
- Some 400 activities per year (2000+ since 2014)
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2022
- Joint projects with the European Union
- Voluntary contributions by Canada, Hungary, Italy, Japan, Netherlands, UK and USA in 2022/23
- Support to T-CY



11

2nd Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence: content

Tools for a more effective criminal justice response:

- Scope: criminal investigations and proceedings related to computer systems and data and collection of e-evidence re **any** criminal offence
- Direct cooperation with service providers and registrars in other Parties
- Giving effect to production orders from other Parties
- Expedited cooperation in emergencies
- Video conferencing
- Joint investigation teams and joint investigations
- Data protection and other safeguards

Subject to a particularly strong system of safeguards:

- Article 2 – scope of Protocol: specific criminal investigations or proceedings related to cybercrime and e-evidence
- Article 13 incorporates Article 15 of the Convention to ensure the adequate protection of human rights and liberties and that provides for the principle of proportionality.
- Article 14 provides for detailed data protection safeguards that are unique for a criminal justice treaty.
- Articles specify types of data to be disclosed.
- Articles specify information to be included to permit application of domestic safeguards
- Reservations and declarations to permit domestic safeguards and limit information to be provided.

12

THB and the Budapest Convention: Take-aways

- Procedural powers and international cooperation provisions of the Budapest Convention and its Second Protocol ▶ secure e-evidence of THB + rescue victims
- Cooperation with 3rd countries (currently 68 Parties)
- Cooperation with service providers
- Interagency cooperation: involve experts on cybercrime investigations and computer forensics in measures against THB and the protection of victims
- Capacity building

13

Q & A

Alexander.seger@coe.int

www.coe.int/cybercrime

14