Seminar on the impact of new technologies on criminal procedures
ESPMU, Brasilia, 5-6 December 2024

Convention on Cybercrime and the Second Procotol on e-evidence:

Main points and links to the forthcoming United Nations treaty

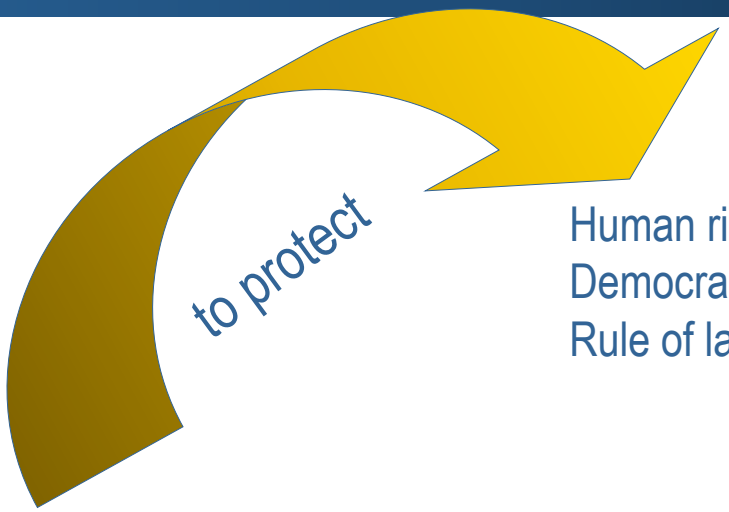
Alexander Seger, Head of Cybercrime Division, Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

1

Council of Europe: 40+ years countering cybercrime



Human rights
Democracy
Rule of law

Cooperation on cybercrime

Established 1949
46 member States

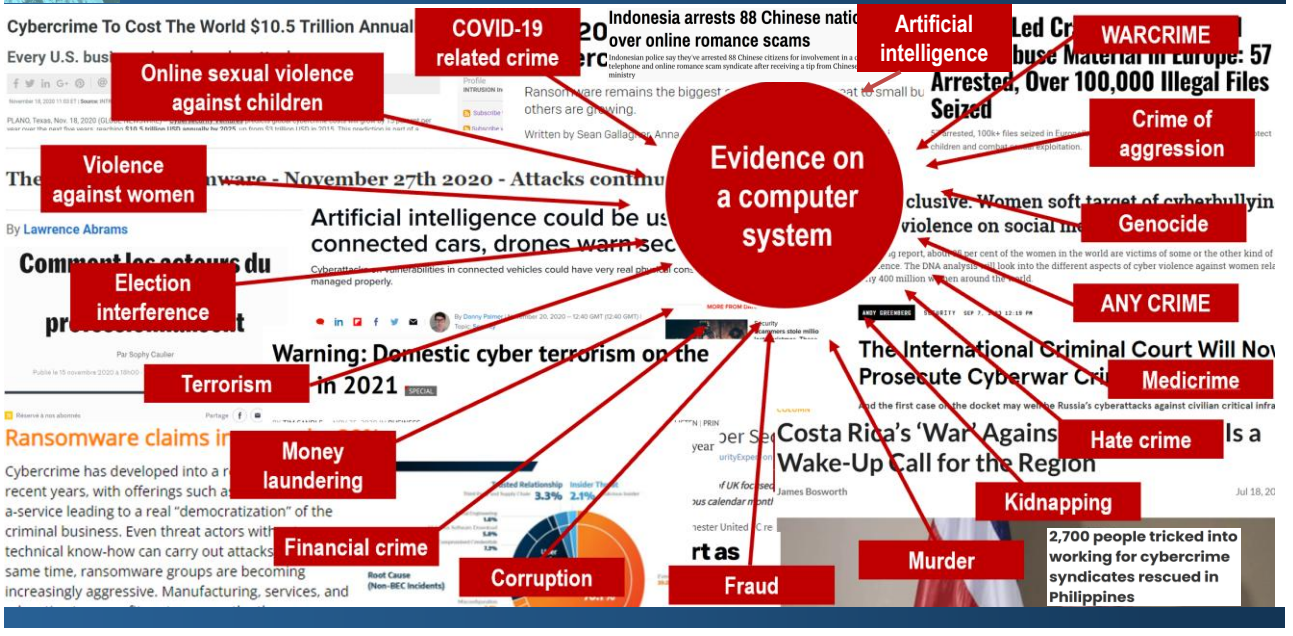
COUNCIL OF EUROPE
75
1949 - 2024
CONSEIL DE L'EUROPE

2

Cybercrime …

3

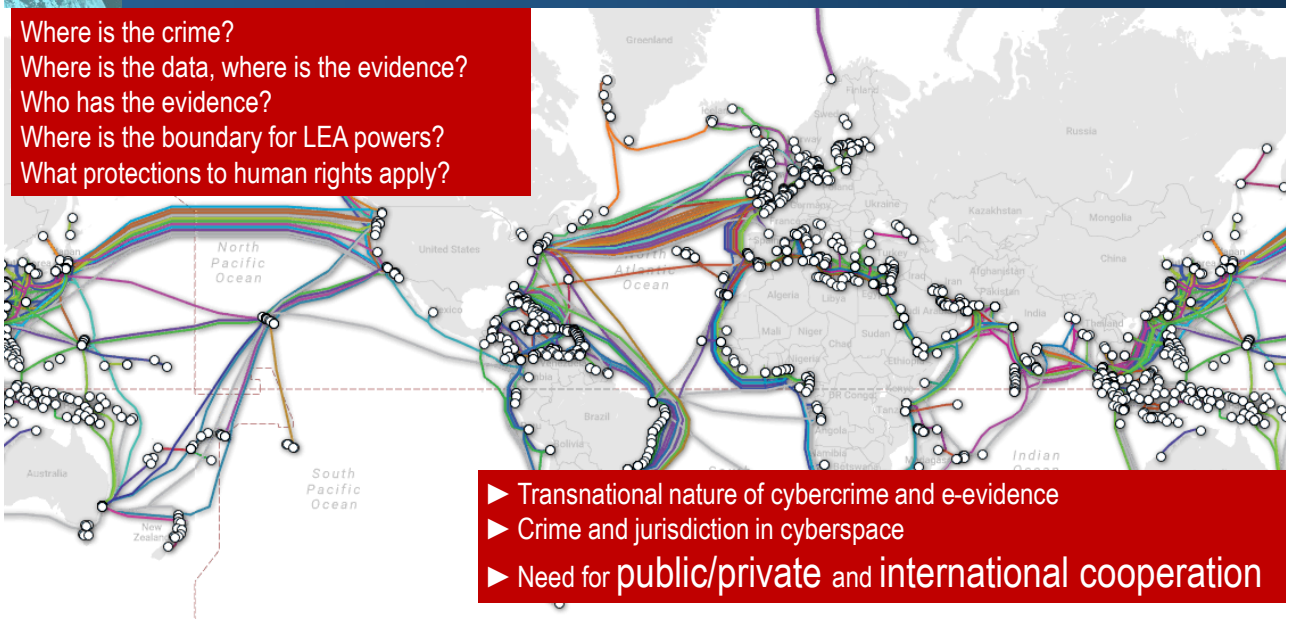
… and e-evidence re all types of crime



4

Cybercrime and e-evidence: the problem of territoriality and jurisdiction

Where is the crime?
Where is the data, where is the evidence?
Who has the evidence?
Where is the boundary for LEA powers?
What protections to human rights apply?



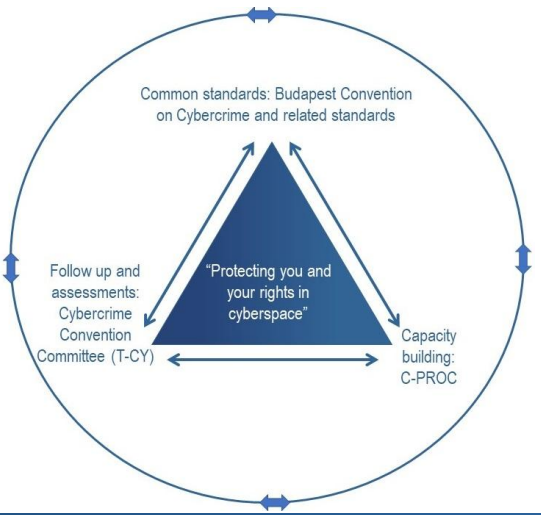
- Transnational nature of cybercrime and e-evidence
- Crime and jurisdiction in cyberspace
- Need for public/private and international cooperation

5

The framework of the Convention on Cybercrime (Budapest Convention)

- 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 2024: **76 Parties and 20 "Observer States"**



6

Content of 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

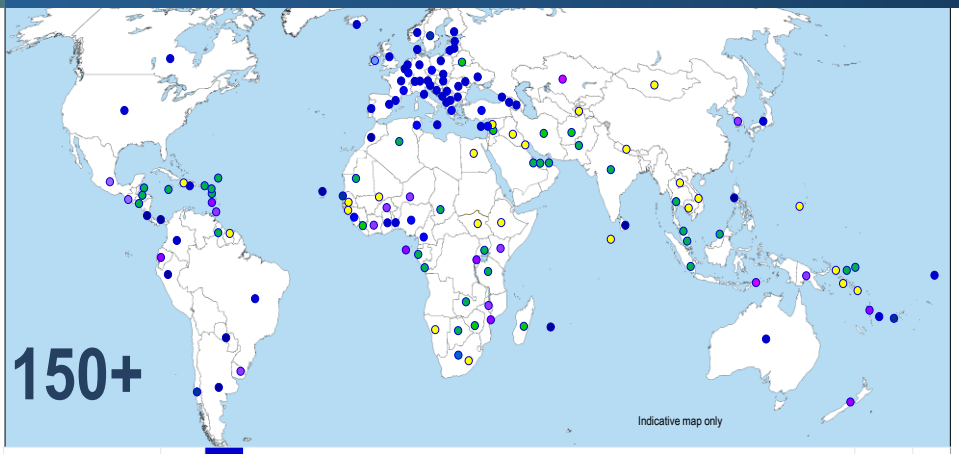
+

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!

7

Reach of the Convention on Cybercrime



Parties:	76				
Signed:	2		Other States with substantive laws broadly in line with Budapest Convention:	30+	
Invited to accede:	18		Further States drawing on Budapest Convention for legislation:	20+	
=	**96**		=	**50+**	

Latest Parties:
- Benin
- Cameroon
- Côte d'Ivoire
- Fiji
- Grenada
- Kiribati
- Sierra Leone
- Tunisia

Latest invitees:
- Kenya
- Malawi
- Papua New Guinea

8

Rationale: Why the Second Protocol?

Cybercrime: Threat to

- Human rights
- Democracy
- Rule of law

Positive obligations:

- Provide the means to protect the rights of individuals, also against crime

Problem:

- Proliferation of cybercrime
- Any type of crime now involving e-evidence
- Evidence somewhere in foreign, multiple, shifting or unknown jurisdictions
- Effective means not available to obtain the disclosure of e-evidence
- Less than 0.1% of offences in cyberspace lead to prosecutions and convictions
- Do victims obtain justice?

2nd Protocol to help address these challenges

9

Rationale: Why the Second Protocol?

Specific issues:

- How to obtain subscriber information efficiently?
- How to cooperate directly with a service provider in another Party?
- How to obtain WHOIS data (domain name registration information) from registrars?
- How to obtain stored data, including content, in an emergency situation?
- How to make mutual assistance more effective?
- How to reconcile efficient and effective measures with rule of law and data protection requirements?

10

Rationale: Why the Second Protocol?

Example subscriber information

"Subscriber information" is data most often needed in a criminal investigation (to identify the owner of a webmail account, user of an IP address)

► How to obtain it from a provider in another Party?

11

Rationale: Why the Second Protocol?

Issue: Voluntary disclosure [of subscriber information] by service providers

Current practices:

- >300,000 requests/year by BC Parties/Observers to major US providers
- Disclosure of subscriber information (ca. 64%)
- Providers decide whether to respond to lawful requests and to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No disclosure by non-US providers
- No admissibility of data received in some States

► Clearer / more stable framework required

Article 7 of the Second Protocol on

► "Direct disclosure of subscriber information"

12

Rationale: Why the Second Protocol?

Example emergency situations

Hostage situations, kidnappings, ongoing sexual abuse of a child, anticipated terrorist attack, cyber attacks on critical infrastructure resulting in imminent death or injury

►How to obtain data – including content data – from another Party in an expeditious manner?

Articles of the Second Protocol

- ► 3 Definition of emergency
- ► 9 Expedited disclosure of stored computer data in an emergency
- ► 10 Emergency mutual assistance

13

Content of the Second Protocol

Preamble

Chapter I: Common provisions

Article 1 Purpose
Article 2 Scope of application
Article 3 Definitions
Article 4 Language

Chapter II: Measures for enhanced cooperation

Article 5 General principles applicable to Chapter II
Article 6 Request for domain name registration information
Article 7 Disclosure of subscriber information
Article 8 Giving effect to orders from another party for expedited production of subscriber information and traffic data
Article 9 Expedited disclosure of stored computer data in an emergency
Article 10 Emergency mutual assistance
Article 11 Video conferencing
Article 12 Joint investigation teams and joint investigations

Chapter III – Conditions and safeguards

Article 13 Conditions and safeguards
Article 14 Protection of personal data

Chapter IV: Final provisions

Article 15 Effects of this Protocol
Article 16 Signature and entry into force
Article 17 Federal clause
Article 18 Territorial application
Article 19 Reservations and declarations
Article 20 Status and withdrawal of reservations
Article 21 Amendments
Article 22 Settlement of disputes
Article 23 Consultations of the Parties and assessment of implementation
Article 24 Denunciation
Article 25 Notification

14

Content of the Second Protocol

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

15

Content of the Second Protocol

Efficiency with 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

16

Content of the Second Protocol

Article 14 – Protection of personal data

1. Scope
2. Purpose and use
3. Quality and integrity
4. Sensitive data
5. Retention periods
6. Automated decisions
7. Data security and security incidents
8. Maintaining records
9. Onward sharing within a Party
10. Onward transfer to another State or international organisation
11. Transparency and notice
12. Access and rectification
13. Judicial and non-judicial remedies
14. Oversight
15. Consultation and suspension

Re scope:

Where Parties are already bound by a comprehensive framework between those Parties the terms of that framework shall apply.

Example: Data Protection Convention 108+ of the COE

► **Brazil to consider accession to Convention 108+**

17

Second Protocol: What next?

Second Protocol on electronic evidence: Status November 2024		
Parties	2	Serbia (February 2023), Japan (May 2023)
+ Signatories	45	Most recent: Czechia, Georgia, Paraguay, Sierra Leone

► Signature and ratification of the Second Protocol ► PRIORITY for 2025

► C-PROC capacity building projects available to support and share experience

Note:

- 5 ratifications needed for entry into forc

18

Towards a United Nations treatry against cybercrime

Background:

- UNGA initiative by Russia ▶ Dec 2019: UNGA Resolution 74/247 ▶ Decision to establish an Ad Hoc Committee (AHC) to elaborate "a comprehensive international convention on countering the use of information and communications technologies for criminal purposes"
- Feb 2022 – Aug 2024: 8 formal sessions and numerous informal and intersessional meetings of the AHC
- 8 Aug 2024: Agreement by AHC on the draft text of a UN treaty and a draft resolution for submission to and adoption by UNGA
- Adoption by UNGA expected by December 2024
- Opening for signature in Vietnam in 2025 [tbc]

Result:

Draft "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"

["Draft UN treaty"]

19

(draft) UN treaty: Core concepts copied from Budapest Convention

Core concepts and measures of the draft treaty

- are drawn from the BC 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 BC**

Example:

Art.	Budapest Convention		Draft 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

20

In and not in the draft UN treaty

New in draft 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 draft UN treaty:

None of the measures of the Second Protocol to the BC on enhanced cooperation and disclosure of electronic evidence (2022):

- Direct cooperation with service providers
- Expedited cooperation in emergencies
- Data protection conditions to permit the flow of personal data

21

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.

22

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 as per draft UNGA resolution.
- ► 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

23

Implications for BC

Implications for Convention on Cybercrime (Budapest Convention):

- BC with its Protocols will remain the more relevant framework in the foreseeable future.
- Synergies between both treaties (including capacity building) feasible.
- More States will seek accession to the BC because:
  - the political obstacle of BC being considered as preventing a UN treaty has been removed;
  - countries learned much about the BC during the AHC process;
  - the provisions of the BC form the backbone also of the draft UN treaty,
  - the advanced tools of the Second Protocol on electronic evidence are only available to Parties to the BC;
  - Governments need to act on cybercrime now and may not want wait for the UN treaty to become operational.
- However, a clear commitment to meeting human rights and rule of law conditions will be necessary when governments are seeking accession to the Budapest Convention on Cybercrime.

24

Q & A

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE