Octopus Project

Budapest Convention on Cybercrime: overview, impact and benefits

Alexander Seger
Council of Europe

Workshop on cybercrime and electronic evidence in Malaysia
and
Consultations with stakeholders on implementing regulations to the Cybersecurity Bill
organised by the
National Cyber Security Agency of Malaysia in cooperation with the Council of Europe

26-28 June 2024, Palm Garden Hotel, Putrajaya, Malaysia

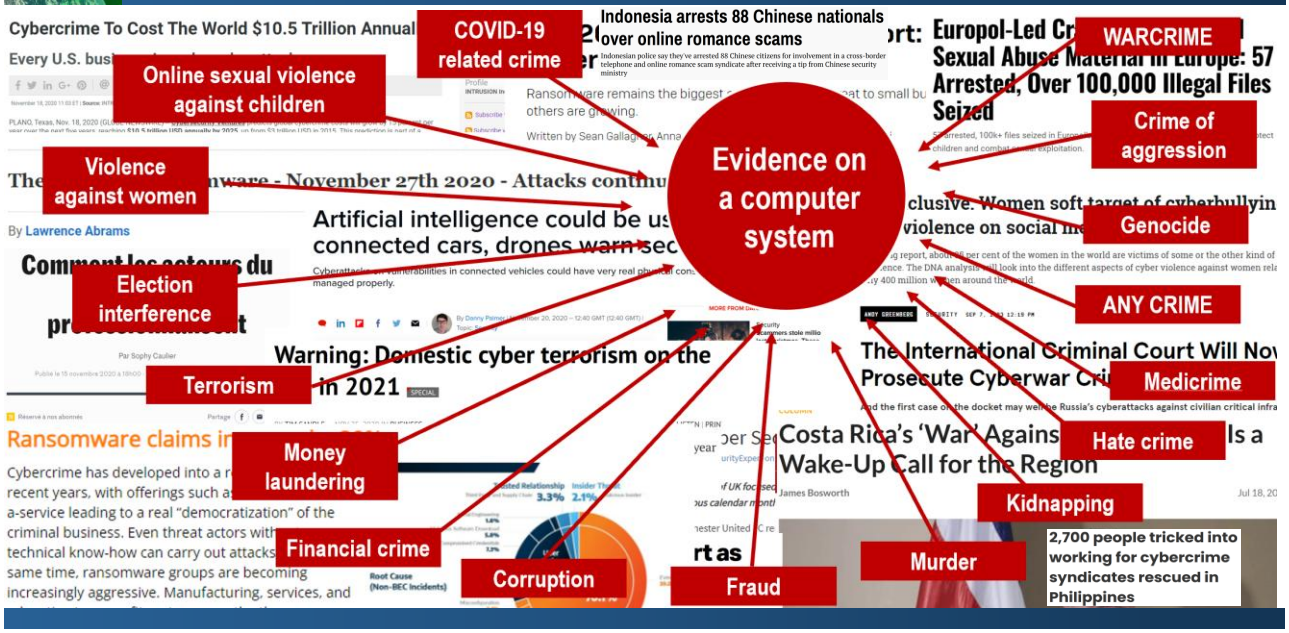
www.coe.int/cybercrime

1

Cybercrime …

2

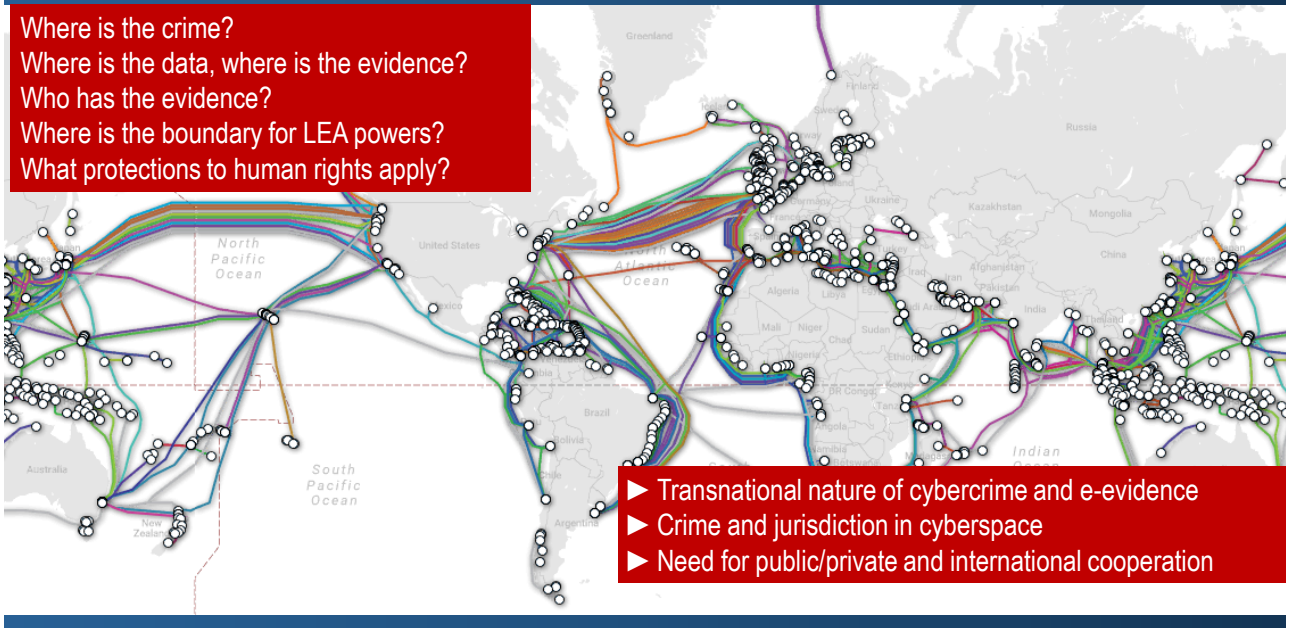
… and e-evidence re all types of crime



3

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?



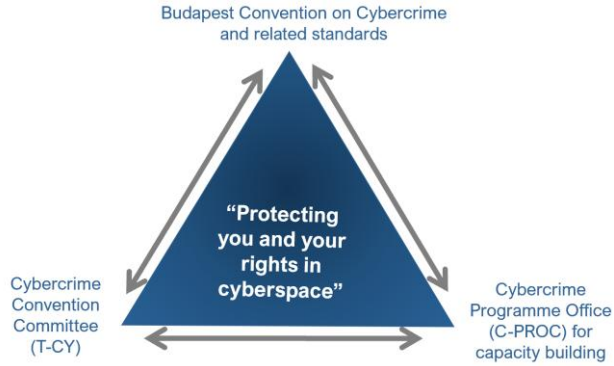
- Transnational nature of cybercrime and e-evidence
- Crime and jurisdiction in cyberspace
- Need for public/private and international cooperation

4

The mechanism of the Convention on Cybercrime

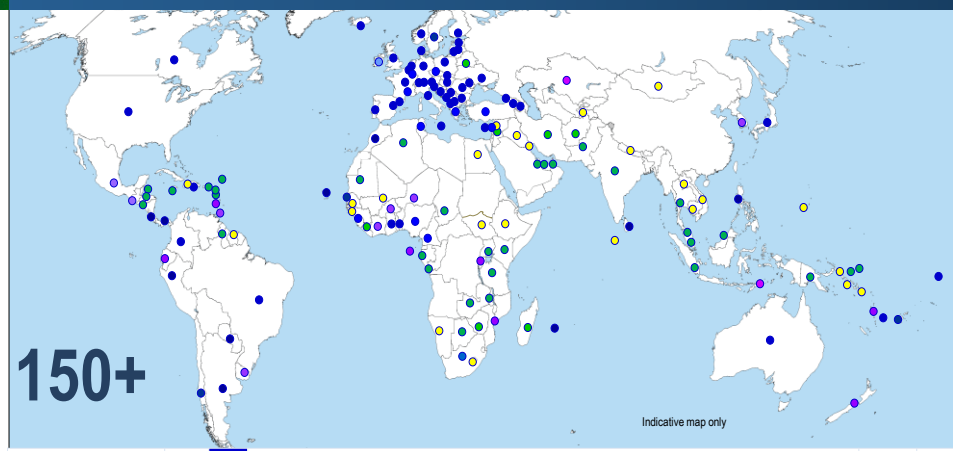
- Budapest Convention on Cybercrime (2001)
  1. Specific offences
  2. Procedural powers
  3. International cooperation
- 1st Protocol on Xenophobia and Racism via Computer Systems (2003)
- 2nd Protocol on enhanced cooperation and disclosure of electronic evidence (2022)
- Guidance Notes

By June 2024: 75 **Parties and 18 „Observer States“**



5

Reach of the Budapest Convention on Cybercrime



Parties:	75				
Signed:	2		Other States with substantive laws broadly in line with Budapest Convention:	35+	
Invited to accede:	16		Further States drawing on Budapest Convention for legislation:	20+	
=	**93**		=	**55+**	

Parties include:

- Australia
- Fiji
- Japan
- Kiribati
- Philippines
- Sri Lanka
- Tonga

6

How to accede to the Budapest Convention on Cybercrime

Treaty open for accession (article 37)

Phase 1:
- A country with legislation in place or advanced stage
- Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

Phase 2:
- Domestic procedure (e.g. decision by national Parliament)
- Deposit of the instrument of accession

For any query contact:
Alexander.seger@coe.int
Executive Secretary
Cybercrime Convention Committee
Council of Europe

7

Content of the Budapest 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!

8

Content of the Budapest Convention on Cybercrime

Article	Budapest Convention
Art. 1	Definitions
Art. 2	Illegal access
Art. 3	Illegal interception
Art. 4	Data interference
Art. 5	System interference
Art. 6	Misuse of devices
Art. 7	Computer-related forgery
Art. 8	Computer-related fraud
Art. 9	Child pornography
Art. 10	IPR offences
Art. 11	Attempt, aiding, abetting
Art. 12	Corporate liability

9

Content of the Budapest Convention on Cybercrime

Article	Budapest Convention
Art. 15	Conditions and safeguards
Art. 16	Expedited preservation
Art. 17	Expedited preservation and partial disclosure of traffic data
Art. 18	Production order
Art. 19	Search and seizure
Art. 20	Real-time collection traffic data
Art. 21	Interception of content data

10

Content of the Budapest Convention on Cybercrime

	International cooperation
Art. 23	General principles relating to international cooperation
Art. 24	Extradition
Art. 25	General principles relating to mutual assistance
Art. 26	Spontaneous information
Art. 27	Mutual assistance in the absence of applicable international instruments
Art. 28	Confidentiality and limitation on use
Art. 29	Expedited preservation of stored computer data
Art. 30	Expedited disclosure of preserved traffic data
Art. 31	Mutual assistance regarding accessing of stored computer data
Art. 32	Trans-border access to stored computer data with consent or where publicly available
Art. 33	Mutual assistance in the real-time collection of traffic data
Art. 34	Mutual assistance regarding the interception of content data
Art. 35	24/7 Network

11

Article 35: 24/7 network of contact points

Article 35 – 24/7 Network

Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice;

b) the preservation of data pursuant to Articles 29 and 30;

c) the collection of evidence, the provision of legal information, and locating of suspects.

Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis and each party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

12

Update on the functioning of the 24/7 Network of contact points

Secretariat of the Network

- Ensured by the Council of Europe
- Directory with contact details (institution, communication tools, availability, language, instructions)
- Annual meeting of the 24/7 Network (at EUROPOL, 18 October 2024)

Contact points established by Parties

- Parties with contact points: 71
- Parties with more than 1 contact point: 12

Types of contact point

- Police: 61
- Security services: 3
- Prosecution: 15
- Ministry of Justice: 4
- Cybersecurity: 1

Latest developments

- Tunisia: Direction Générale des Services Techniques
- Grenada: Royal Grenada Police Force
- Sierra Leone: National Cybersecurity Coordination Centre
- Cameroon: to be confirmed

G/7 Network of contact points

- Malaysia: Royal Malaysian Police's Computer Crime Investigations Division

13

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

Means for a more effective criminal justice response:

- Direct cooperation with service providers in other jurisdictions to obtain subscriber information
- Direct requests to registrars to obtain domain name registration information
- More effective means to obtain subscriber information and traffic data through government-to-government cooperation
- Expeditious cooperation in emergency situations
- Joint investigations and video-conferencing

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.

14

2nd Additional Protocol to the Convention on Cybercrime: content

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 **(gov2private)**
Article 7 Disclosure of subscriber information **(gov2private)**
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

15

2nd Additional Protocol to the Convention on Cybercrime: status

Second Protocol on electronic evidence: Status 21 June 2024		
Parties	2	Serbia (February 2023), Japan (May 2023)
+ Signatories	44	Most recent: Benin, Czechia, Georgia (June 2024)

5 ratifications needed for entry into force: ► 2024?

16

Content of the Convention on Cybercrime: example ransomware ▶ Guidance Note

Article	Budapest Convention on Cybercrime
Art. 2	Illegal access
Art. 3	Illegal interception
Art. 4	Data interference
Art. 5	System interference
Art. 6	Misuse of devices
Art. 7	Computer-related forgery
Art. 8	Computer-related fraud
Art. 11	Attempt, aiding, abetting
Art. 12	Corporate liability
Art. 13	Sanctions and measures

Article	Convention on Cybercrime
Art. 14-21	Procedural powers

Ransom-ware offences

Article	Convention on Cybercrime
Art. 23-35	International cooperation

Article	2nd Additional Protocol to Convention on Cybercrime
Art. 7	(Direct) Disclosure of subscriber information
Art. 8	Giving effect to orders from another party for expedited production of subscriber information and traffic data
Art. 9	Expedited disclosure of stored computer data in an emergency
Art. 10	Emergency mutual assistance
Art. 11	Video conferencing
Art. 12	Joint investigation teams and joint investigations

17

The Cybercrime Convention Committee (T-CY)

Cybercrime Convention Committee (T-CY)

- 75 members (= Parties to Convention), 18 Observer States (signatories and States invited to accede), 11 observer organisations (including EUROPOL, G7, INTERPOL, UNODC)
- Plenaries and working groups
- Assessing implementation of the Convention by the Parties
- Guidance Notes
- Preparation of new instruments ▶ Protocol to the Budapest Convention
- Exchanging information and sharing good practices
- Building trust

18

The Convention on Cybercrime: Backed up by capacity building




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
- 40 staff
- Some 400 activities per year
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2023
- Joint projects with the European Union
- Voluntary contributions by Japan, UK and USA and others
- Support to T-CY

delivery of an introductory course evidence in Benin

judges and prosecutors from Benin, who had ier in August, delivered for the first time an uring the first...

Current projects:

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

Union, held a hybrid workshop with the authorities of Panama in view of further harmonising national legislation on cybercrime and electronic evidence with the provisions of the Budapest Convention on...

event that aims to facilitate sharing of information and best practices in the region. This...

Y+ Project, organised the 9th Africa Working 22 July 2022. The AF-WGM is an annual

19

Joining the Budapest Convention on Cybercrime: benefits

Impact and benefits

- ✓ Stronger and more consistent legislation
- ✓ More efficient and trusted international cooperation between Parties
- ✓ More investigation, prosecution, adjudication of cybercrime and e-evidence cases
- ✓ Trusted partnerships and public/private cooperation
- ✓ Catalyst for capacity building
- ✓ Better cybersecurity performance
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)

"Cost": Commitment to cooperate

Disadvantages?

20