Conference on ransomware and crypto investigations in Southeast Asia
Kuala Lumpur, 19 May 2025

Session 5: Legal frameworks and international cooperation:

- Convention on Cybercrime
- Second Protocol on Electronic Evidence

Alexander Seger, Cybercrime Division, Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MAJLIS KESELAMATAN NEGARA
NSC
MALAYSIA

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY

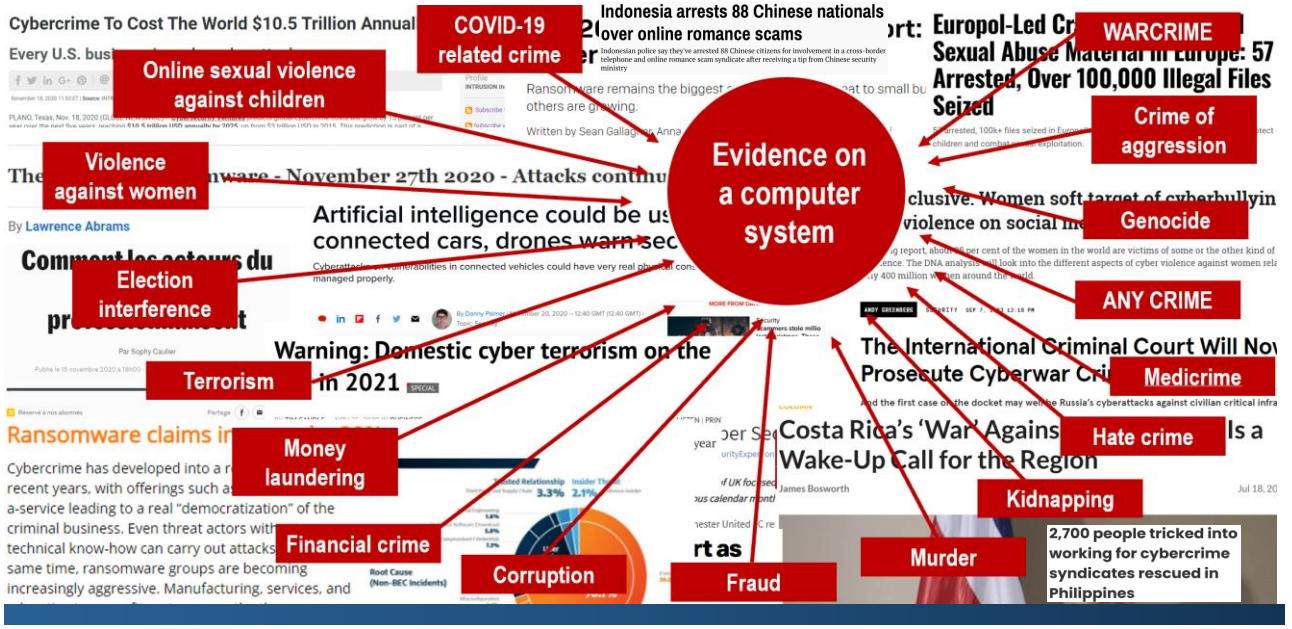
www.coe.int/cybercrime

1

Cybercrime …

2

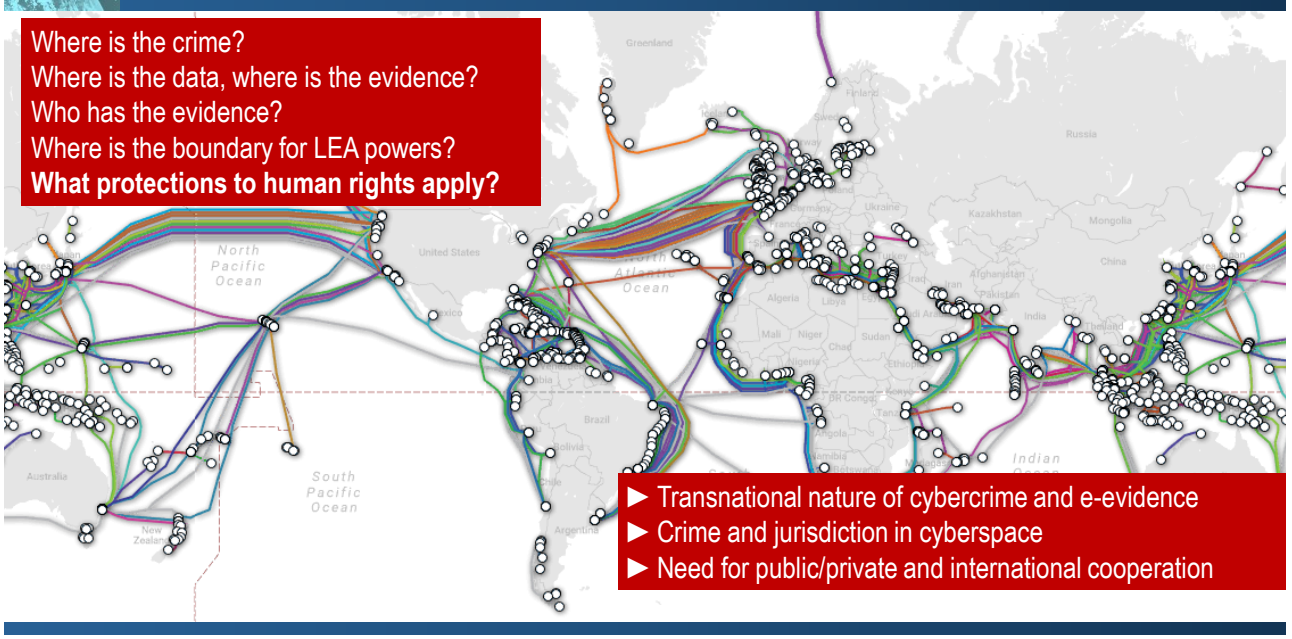
… and e-evidence re all types of crime



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

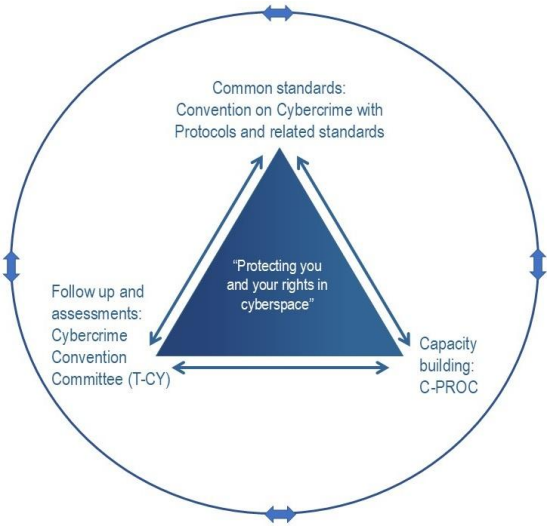
4

The framework of the Convention on Cybercrime

- Convention on Cybercrime (Budapest, 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

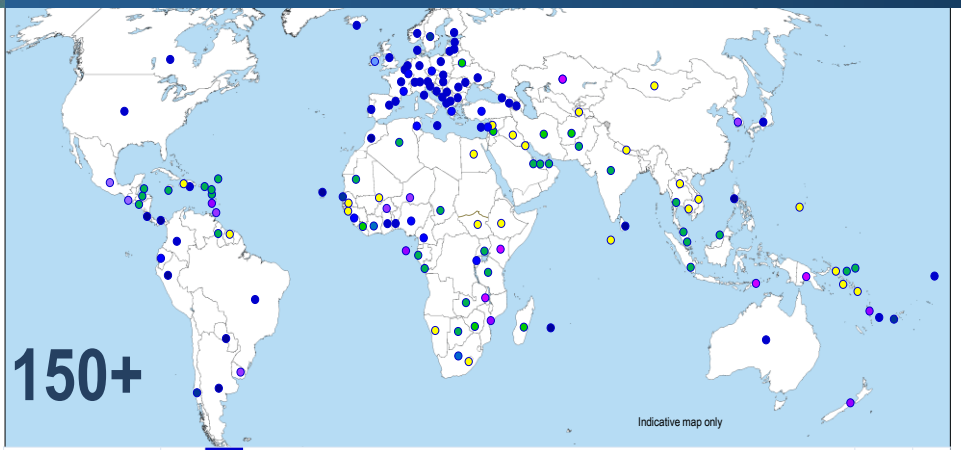
Cybercrime + e-evidence!

By May 2025: 78 Parties and 16 "Observer States"



5

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+**	

Parties include:

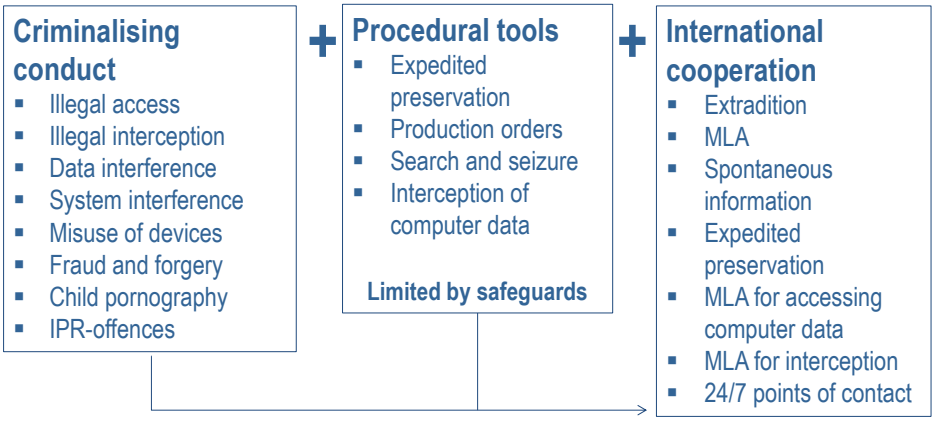
- Australia
- Fiji
- Japan
- Kiribati
- Philippines
- Sri Lanka
- Tonga

Invited to accede:

- Papua New Guinea
- Timor Leste
- Vanuatu

6

Content of the Budapest Convention



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

7

Content of the Second Protocol on electronic evidence

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)

8

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

9

Content of the Budapest Convention: 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

10

Convention on Cybercrime and Protocols: backed up by capacity building
► Cybercrime Programme Office of the Council of Europe (C-PROC): projects 2024+

OCTOPUS Project	Jan 2021 – Dec 2027	EUR 10 million	Voluntary contributions (USA, UK, Japan, Canada, Hungary, Iceland, Italy) [funding not fully secured]
GLACY-e project on Global Action on Cybercrime Enhanced	Aug 2023 – Jan 2026	EUR 5.55 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
CyberUA project on strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine	Feb 2024 – July 2026	EUR 3.5 million	Voluntary contributions to the Ukraine Action Planand Ordinary Budget [funding not fully secured]
CyberEast+ on enhanced action on cybercrime for cyber resilience in Eastern Partnership States	Mar 2024 – Feb 2027	EUR 3.89 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
CyberSouth+ project on enhanced co-operation on cybercrime and electronic evidence in the Southern Neighbourhood Region	Jan 2024 – Dec 2026	EUR 3.89 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
CyberSEE project on enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye	Jan 2024 – Jun 2027	EUR 5.55 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
CyberSPEX project on enhanced co-operation on e-evidence by EU Member States through the Second Additional Protocol to the Convention on Cybercrime	Mar 2024 – Feb 2026	EUR 2.23 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)

11

C-PROC: capacity building on ransomware (examples)

Glacy-e

- Case scenario exercise aiming to strengthen the interagency cooperation between CERTs and LEAs (July 2024, Dominican Republic)

CyberEast+:

- Training on ransomware investigations for Ukranian law enforcement (late April 2024)
- Training on malware and network investigations for Ukraine (25-27 June 2024 and 1-3 October 2024, Romania)
- Regional Technical Exercise on cybercrime/security coordination (8-11 October 2024, Bucharest)

CyberSEE

- Regional meeting of LEAs on emerging cyber threats and timely exchange of information (June 2024, Albania)
- Regional simulation exercise on response to cyber-attacks (Jointly with SEPCA, WB3C and OSCE, September, Montenegro)
- Regional workshop on ransomware investigation, (Jointly with WB3C, October, Montenegro)
- Underground Economy (with Team Cymru, September, Strasbourg)

CyberSouth+

- Regional workshop on ransomware attacks for Arab countries (Jointly with AICTO, 1-2 October 2024, Tunis)

CyberUA

12

UN treaty against cybercrime - Background

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 on 24 December 2024
- Opening for signature in Vietnam in October 2025

Result:

"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"

["Hanoi Convention"`?]

13

UN treaty against cybercrime: Content

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

14

UN treaty against cybercrime: Content

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

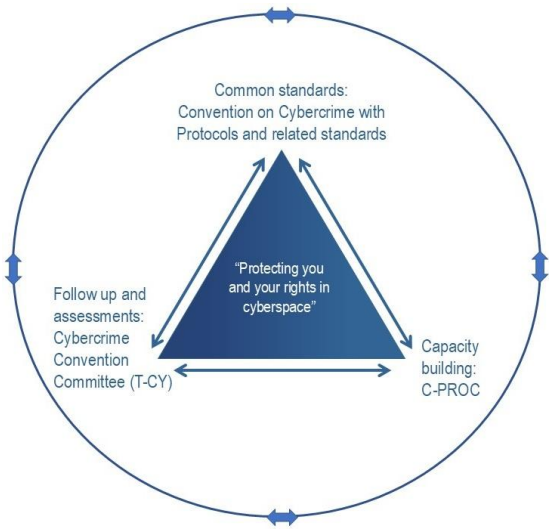
NOT in draft UN treaty:

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 and registrars in other Parties (articles 6 and 7)
- Expedited cooperation in emergency situations (articles 9 and 10)

15

Conclusion



and / or

"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"

["Hanoi Convention"`?]

16