Regional workhop on
COVID-19 related cybercrime and e-evidence in Asia
Colombo, 7-9 March 2022

Session on domestic and international frameworks on cybercrime and e-evidence: their relevance for the COVID-19 pandemic

International frameworks: The tools of the Budapest Convention on Cybercrime

Alexander Seger
Head of Cybercrime Division
Council of Europe

SRI LANKA CERT|CC

ICTA ideas actioned
Information and Communication Technology Agency

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

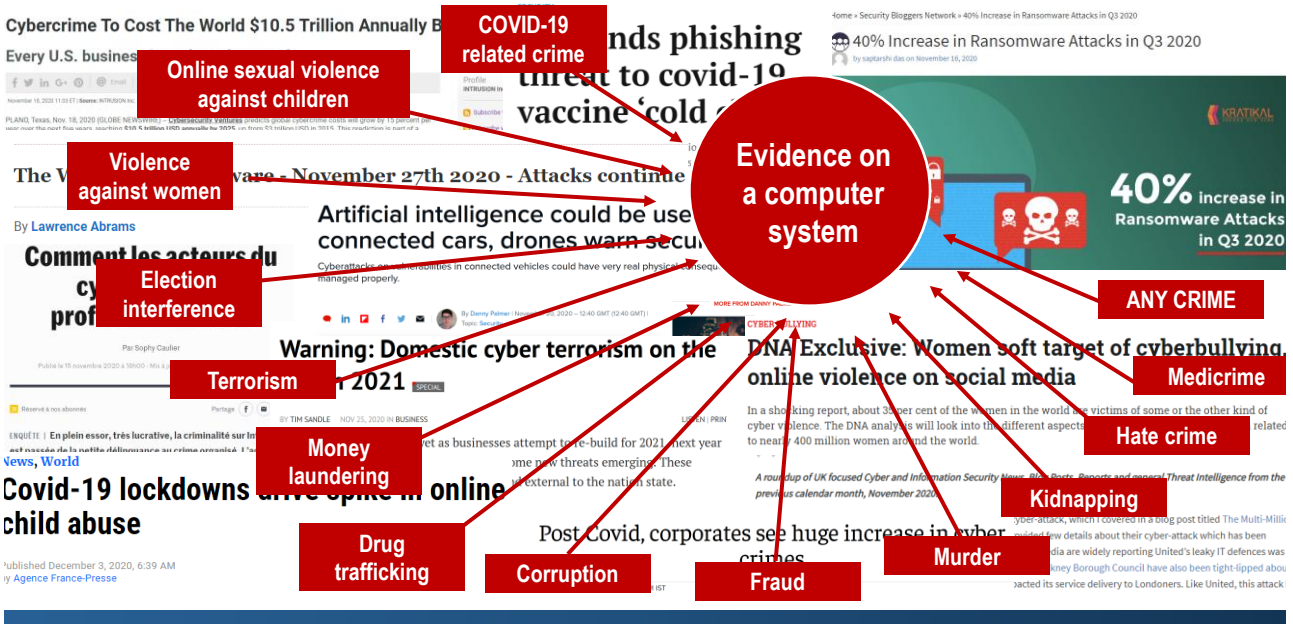
www.coe.int/cybercrime

1

Reminder: the problem of cybercrime …

2

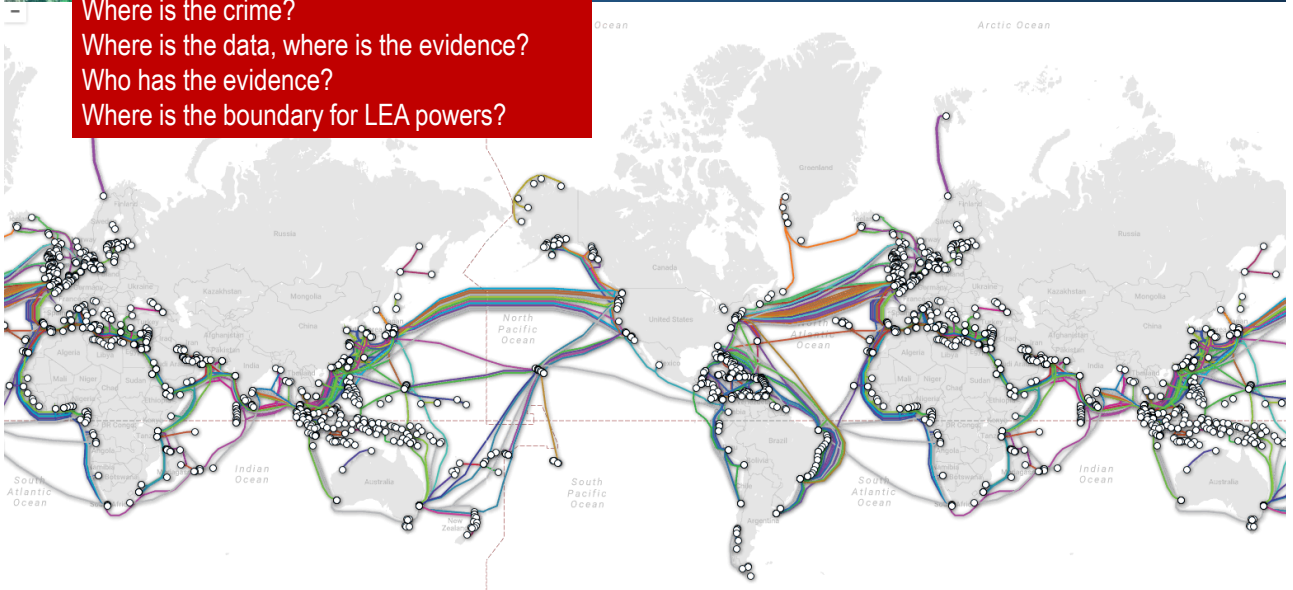
… and e-evidence re all types of crime



3

Where is the evidence?

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



4

What we need

Cybercrime + e-evidence + transnational/ubiquitous nature of crime and evidence

► Need an effective criminal justice response

5

The mechanism of the Budapest Convention

Budapest Convention on Cybercrime (2001):

1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1st Protocol on Xenophobia and Racism via Computer Systems

+ Guidance Notes

+ Protocol on enhanced cooperation on cybercrime and electronic evidence (opening for signature 12 May 2022 in Strasbourg)

6

Content of the Budapest Convention

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

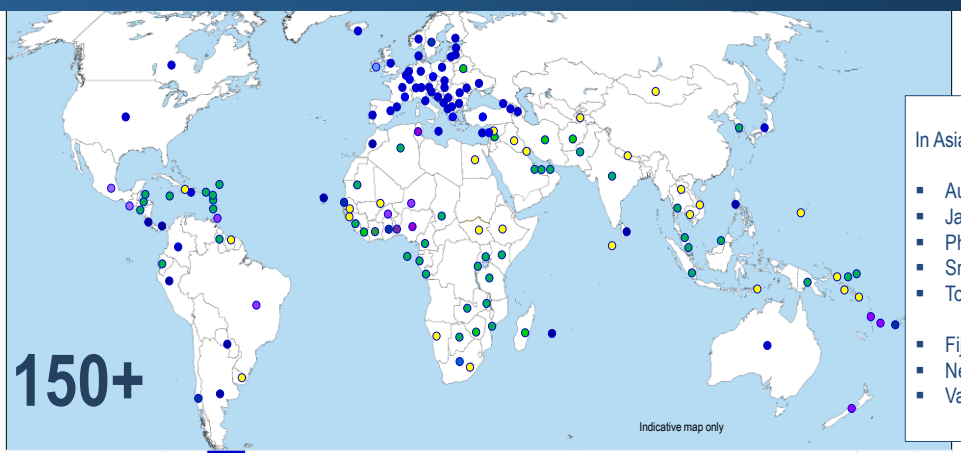
+

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 Budapest Convention



In Asia/Pacific:
- Australia
- Japan
- Philippines
- Sri Lanka
- Tonga

- Fiji
- New Zealand
- Vanuatu

Parties:	66			
Signed:	2	Other States with substantive laws broadly in line with Budapest Convention:	45+	
Invited to accede:	12	Further States drawing on Budapest Convention for legislation:	30+	
=	**80**	=	**75+**	

8

Reach of the Budapest Convention

- ✓ 20 years of Budapest Convention (2001-2021): global impact
- ✓ 66 Parties + 14 signatories and States invited to accede
- ✓ 120+ States with substantive laws aligned with BC
- ✓ 150+ States have used it as a guideline or source
- ✓ 180+ States have been participating in COE activities on cybercrime
- ✓ Promoting rule of law and human rights in cyberspace

► **Instrument with global impact**

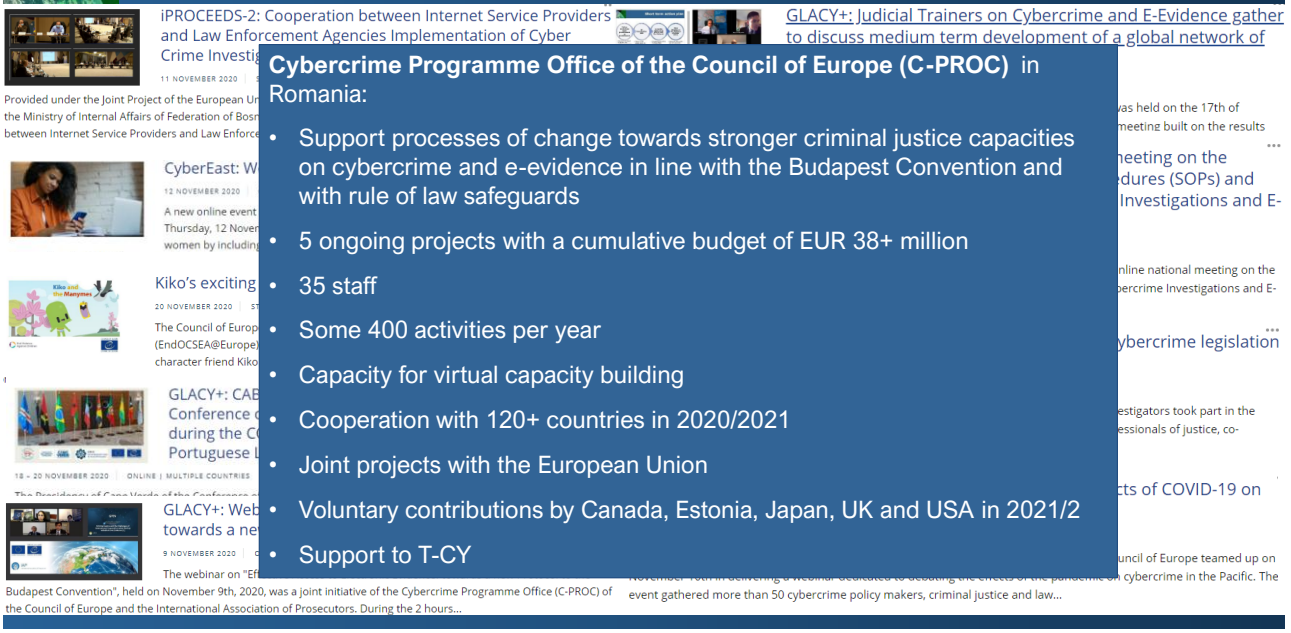
How to accede to the Budapest Convention

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

The Budapest Convention: 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
- 5 ongoing projects with a cumulative budget of EUR 38+ million
- 35 staff
- Some 400 activities per year
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2020/2021
- Joint projects with the European Union
- Voluntary contributions by Canada, Estonia, Japan, UK and USA in 2021/2
- Support to T-CY

11

COVID-19, cybercrime and e-evidence

COVID-19 related crime in cyberspace

- Phishing campaigns and malware distribution through seemingly genuine information or advice on COVID-19 .
- Ransomware shutting down medical, scientific or other health-related facilities testing for COVID-19 or developing vaccines
- Ransomware targeting individuals through apps claiming to provide genuine information on COVID-19
- Attacks against critical infrastructures or international organizations
- Offenders targeting employees who are teleworking
- Fraud schemes offering personal protective equipment or fake medicines claiming to prevent or cure SARS-CoV-2
- Misinformation or fake news to create panic, social instability, xenophobia, racism or distrust in measures taken health authorities

What crime?

Who did it?

What evidence?

12

COVID-19 and the Budapest Convention

COVID-19 related crime in cyberspace

- Phishing campaigns and malware distribution through seemingly genuine information or advice on COVID-19 .
- Ransomware shutting down medical, scientific or other health-related facilities testing for COVID-19 or developing vaccines
- Ransomware targeting individuals through apps claiming to provide genuine information on COVID-19
- Attacks against critical infrastructures or international organizations
- Offenders targeting employees who are teleworking
- Fraud schemes offering personal protective equipment or fake medicines claiming to prevent or cure SARS-CoV-2
- Misinformation or fake news to create panic, social instability, xenophobia, racism or distrust in measures taken health authorities

Budapest Convention – Articles

- 2 – Illegal access
- 3 – Illegal interception
- 4 – Data interference
- 5 – System interference
- 6 – Misuse of devices
- 7 – Forgery
- 8 – Fraud
- 10 – IPR offences

Protocol on Xenophobia and Racism

Guidance Notes on

- Botnets
- DDOS attacks
- Critical information infrastructure attacks
- Malware
- Spam
- ID theft

Procedural powers to secure evidence and identify offenders

- 16+17 – Expedited preservation
- 18 – Production orders
- 19 – Search and seizure
- 20+21 – Interception

With safeguards

- Article 15

Guidance Note on

- Article 18 – Production orders

Framework for international cooperation

- Articles 23 - 35

13

COVID-19 and the Budapest Convention

The tools of the Budapest Convention (criminalization, procedural powers, international cooperation)

Backed up capacity building programmes

Are available to address COVID-19 related cybercrime … and similar future crises.

14

COVID-19 and **more tools**

Coming soon (12 May 2022):

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

- Direct requests to registrars for disclosure of WHOIS information
- Direct orders to service providers for subscriber information (“direct disclosure”)
- Effective means to obtain subscriber information and traffic data (“giving effect”)
- Cooperation in emergencies (“expedited disclosure” + “emergency MLA”)
- Mutual assistance tools (“video-conferencing”, “JITs”)
- Data protection safeguards to permit the flow of personal data under the Protocol

(Details will follow in another session of this workshop)

15