



Regional workshop 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



www.coe.int/cybercrime

1



Reminder: the problem of cybercrime ...

Cybercrime To Cost The World \$10.5 Trillion Annually By 2025

Every U.S. business is under cyberattack

Online child abuse racket: CBI raids 77 spots,

40% Increase in Ransomware Attacks in Q3 2020

40% increase in Ransomware Attacks in Q3 2020

soft target of cyberbullying and media

Fifteen times more child sexual abuse material found online than 10 years ago

Experts from Internet Watch Foundation demand UK uses online safety bill to protect children

Child protection

Covid-19 lockdowns drive spike in online child abuse

Offences against and by means of computers

Cybercrime

Cybersecurity Ventures predicts global cybercrime costs will grow more than eight-fold again, reaching \$10.5 trillion annually by 2025, up from \$1.2 trillion in 2015. That's a 780% increase.

Artificial intelligence

Warning: rise in 20

This year has been rocky, yet as businesses attempt to re-build for 2

external to the nation

Post Covid, corporates see huge increase in cyb

crimes

Sarah Marsh

Sat 13 Nov 2021 07:00 GMT

ENQUÊTE | En plein essor, très lucrative, la criminalité sur Internet est passée de la petite délinquance au crime organisé. L'agili

Par Sophie Caulier

Publié le 10 novembre 2020 à 18h00 - Mis à jour le 10 novembre 2020 à 19h00

Reservez à nos abonnés

Partagez

by TIM SANDLE NOV 25, 2020 IN BUSINESS

Published December 3, 2020, 6:39 AM

by Agence France-Presse

Updated Dec 02, 2020, 05:00 PM IST

2

... and e-evidence re all types of crime

Cybercrime To Cost The World \$10.5 Trillion Annually

Warning: Domestic cyber terrorism on the rise in 2021

40% Increase in Ransomware Attacks in Q3 2020

Evidence on a computer system

- Online sexual violence against children
- COVID-19 related crime
- Violence against women
- Election interference
- Terrorism
- Money laundering
- Drug trafficking
- Corruption
- Fraud
- Murder
- Kidnapping
- Hate crime
- Medicrime
- ANY 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

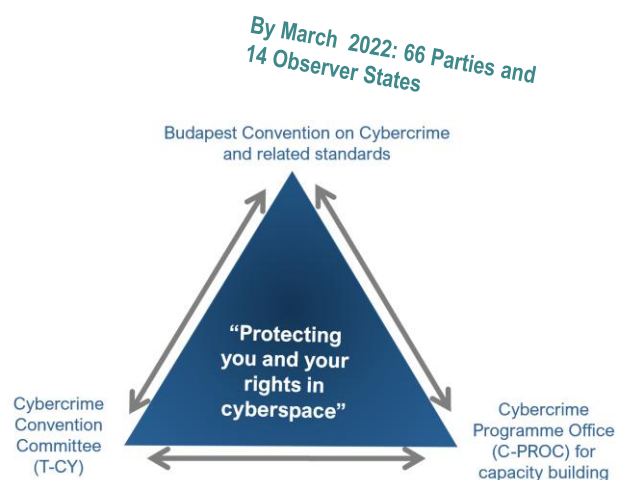
Budapest Convention on Cybercrime (2001):

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

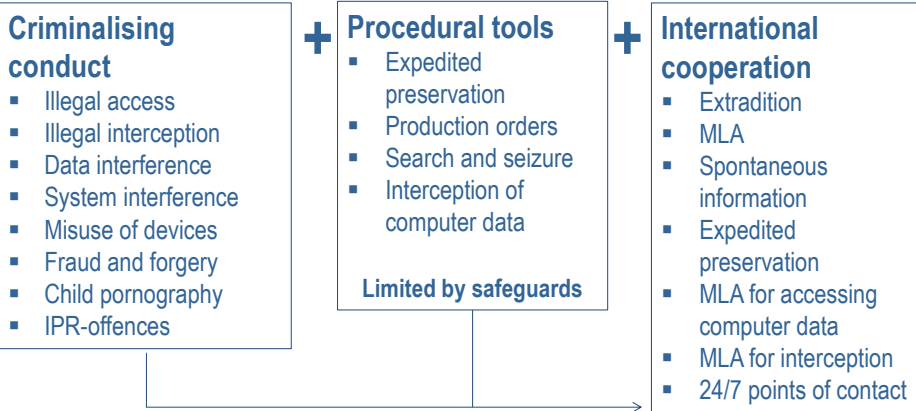
+ Guidance Notes

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



6

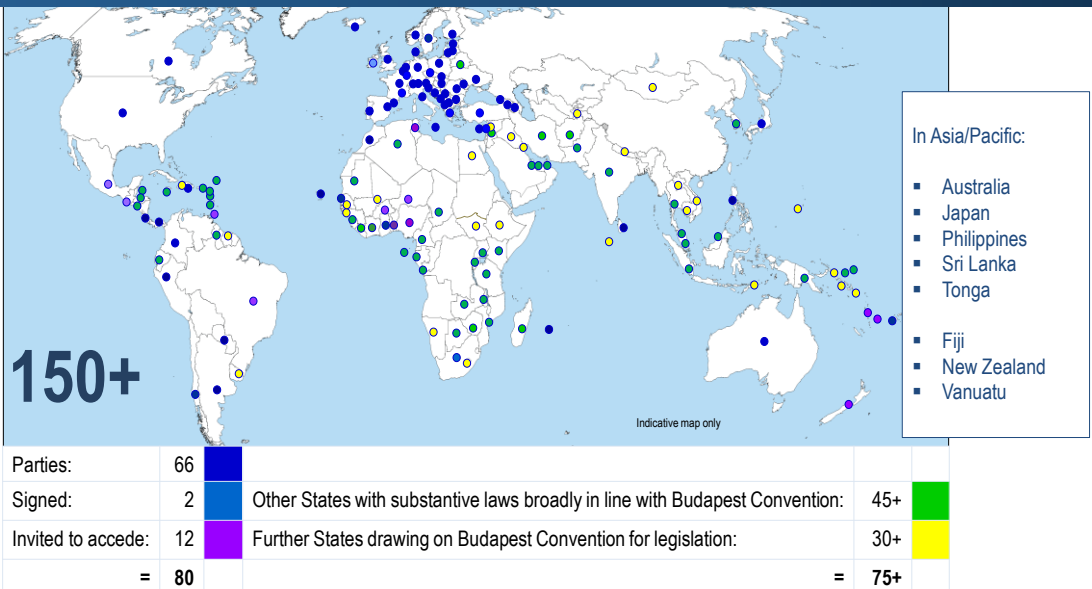
Content of the Budapest Convention



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

7

Reach of the Budapest Convention



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

www.coe.int/cybercrime

9



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

10

The Budapest Convention: backed up by capacity building



iPROCEEDS-2: Cooperation between Internet Service Providers and Law Enforcement Agencies Implementation of Cyber Crime Investig...



GLACY+: Judicial Trainers on Cybercrime and E-Evidence gather to discuss medium term development of a global network of

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

Provided under the Joint Project of the European Union and the Ministry of Internal Affairs of Federation of Bosnia and Herzegovina between Internet Service Providers and Law Enforcement Agencies



CyberEast: Workshop on Cybercrime and E-Evidence Investigation Procedures (SOPs) and E-Evidence Investigation and E-Evidence Investigation



Kiko's exciting journey: The Council of Europe (EndOCSEA@Europe) character friend Kiko



GLACY+: CAB Conference during the Conference of the Portuguese Law Enforcement Agencies



GLACY+: Webinar towards a new era of cybercrime

Budapest Convention", held on November 9th, 2020, was a joint initiative of the Cybercrime Programme Office (C-PROC) of the Council of Europe and the International Association of Prosecutors. During the 2 hours...

event gathered more than 50 cybercrime policy makers, criminal justice and law...

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



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)