


Third Annual PILON Cybercrime Workshop
International Cooperation to Share Electronic Evidence and Combat Cybercrime
27 - 31 May 2019, Vanuatu



Co-funded
by the European Union
and the Council of Europe



Co-funded
by the Council of Europe



The importance of international cooperation
on cybercrime and electronic evidence

Alexander Seger, Council of Europe

www.coe.int/cybercrime

1



Council of Europe and cybercrime: WHY?

Hundreds of millions of incidents of theft of personal data every year

Online child sexual abuse

Cyberbullying, harassment and others forms of cyberviolence

Massive fraud generating massive amounts of crime proceeds

Attacks against critical information infrastructure

Ransomware

Interference in computer systems used in elections

Threats to

- ▶ **Human rights**
- ▶ **Democracy**
- ▶ **Rule of law**

2



Challenge: e-evidence on ANY crime

Cybercrime

- ▶ Offences against computer systems and data
- ▶ Offences by means of computer systems and data

+

Electronic evidence

- ▶ Any crime may involve evidence in electronic form on a computer system
- ▶ Needed in criminal proceedings
- ▶ No data, no evidence, no justice

3



Assessment of international cooperation under the Budapest Convention (2014)

International requests for data

Types of data requested:

1. **Subscriber information (80+%)**
2. **Traffic data**
3. **Content data**

Underlying offences

1. **Fraud and other financial crimes**
2. **Violent and serious crime (murder, assault, trafficking, child abuse etc.)**
3. **Offences against computer systems**

4

Rule of law in cyberspace and the 1% problem

Cybercrime and other offences involving evidence on computer systems (e-evidence):

WHO DID IT?

No data, no evidence, no justice

- Billions of users and devices
- Trillions of attacks
- Millions of offences
- Is there any type of crime without e-evidence?
- Investigations % ?
- Convictions % ?

- = Cyberspace basically safe, crime the exception, offenders brought to justice, individuals and their rights protected?
- = Rule of law in cyberspace?
- = Do govs meet obligation to protect individuals against crime (ECtHR, K.U. v. Finland)?

5

Cybercrime and e-evidence: the problem of territory 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?



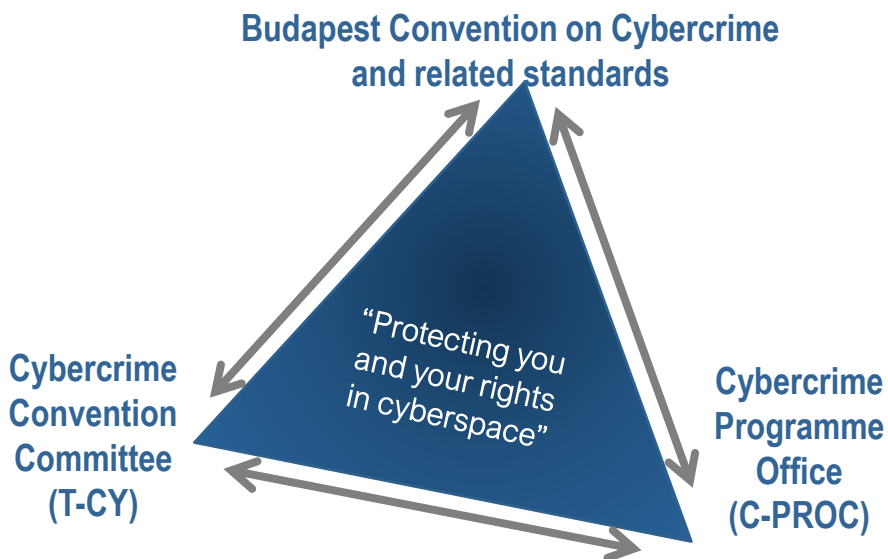
6

The Budapest Convention on Cybercrime as a response

- Budapest Convention on Cybercrime
- Opened for signature in Budapest, Hungary, on 23 November 2001
- Negotiated by Council of Europe (47 members), Canada, Japan, South Africa and USA
- Currently 63 Parties
- Protocol on Xenophobia and Racism via computer systems (2003)
- Guidance Notes
- 2nd Additional under negotiation

7

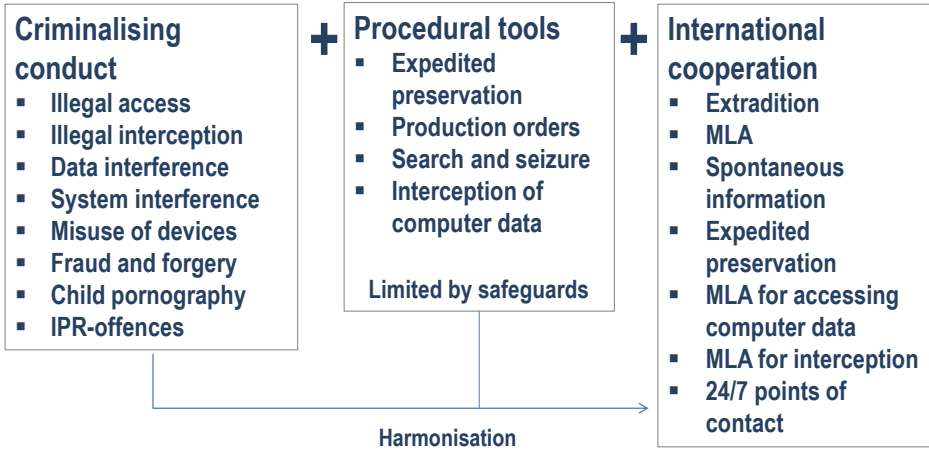
The “mechanism” of the Budapest Convention



8



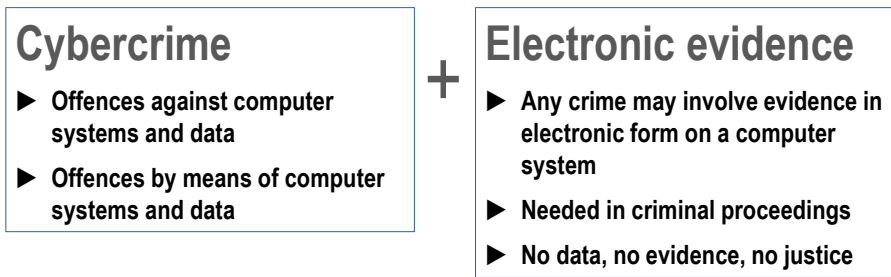
Scope of the Budapest Convention



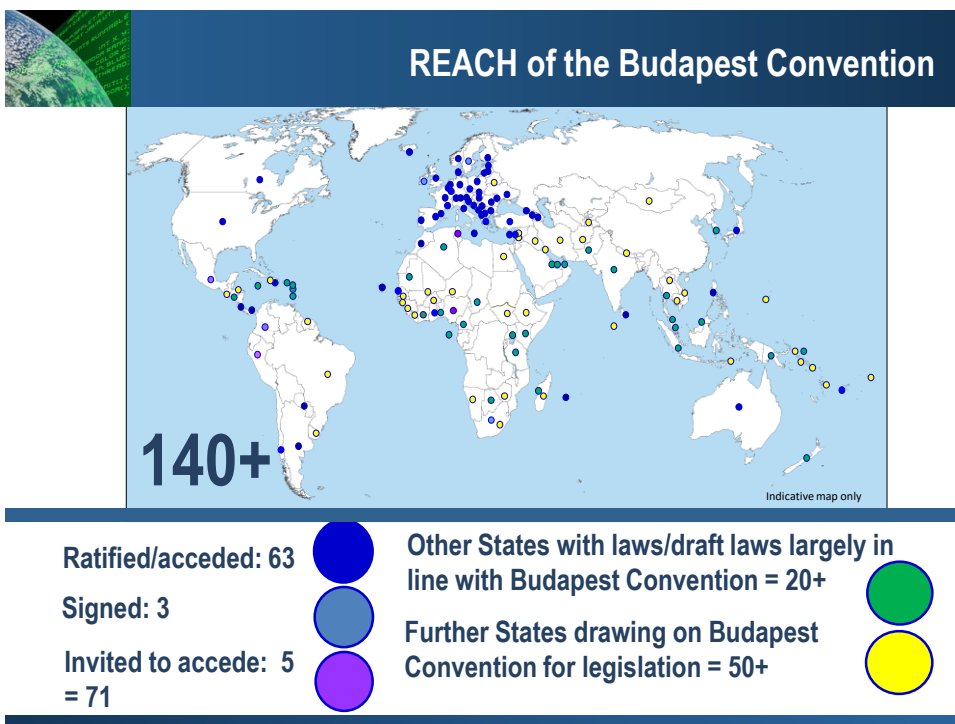
9



Scope of the Budapest Convention



10



11

Keeping the Budapest Convention up to date

- ▶ **Protocol on Xenophobia and Racisms via Computer Systems (31 Parties + 13 Signatories)**
- ▶ **Guidance Notes on**
 - Notion of computer systems
 - Botnets
 - Malware
 - Spam
 - Terrorism
 - Transborder access to data (Article 32)
 - Production Orders for Subscriber Information (Article 18)
 - Election interference [in preparation]
- ▶ **Protocol on enhanced international cooperation under negotiation**

= Budapest Convention remains up-to-date and relevant

12



Acceding to the Budapest Convention

Treaty open for accession by any State (article 37)

Phase 1:

- If a country has legislation in place: 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 the instrument of accession at the Council of Europe

13

13



Impact to date

- Stronger and more harmonised legislation
 - More efficient international cooperation between Parties
 - Better cybersecurity performance
 - More investigation, prosecution and adjudication of cybercrime and e-evidence cases
 - Trusted partnerships and public/private cooperation
 - Catalyst for capacity building
 - Contribution to human rights/rule of law in cyberspace
- = “Protecting you and your rights in cyberspace”

14