~~Beyond~~ WITH Budapest:

Global cooperation on cybercrime, including DNS abuse

Alexander Seger
Head of Cybercrime Division
Council of Europe
www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

1

Cybercrime, including DNS abuse, as a matter of criminal justice:

- Governments have an obligation to protect, including through criminal law (ECtHR 2008: K.U. v Finland)
- Cybercrime and e-evidence require an effective criminal justice response
- Budapest Convention is a criminal justice treaty (specified data in specific investigations)
- Criminal justice response is protective:
  - powers to investigate and prosecute
  - but limited by rule of law conditions and safeguards to protect rights of individuals, including suspects, and prevent abuse
- The criminal justice response is complementing other measures to prevent and respond to security threats and DNS abuse

2

Budapest Convention: a global framework for cooperation on cybercrime

Cybercrime and freedom on the net

Budapest Convention:

- Starting assumption: free flow of and access to information.
- Obligation to protect.
- But restrictions to be narrowly defined in criminal law in line with rule of law requirements (prescribed by law, legitimate aim, necessary, proportionate, effective remedies, guarantees against abuse).
- Expand to global level.

Counter-proposal:

- "Information crime" based on doctrine of information security.
- Sovereign governmental control of information space.
- Governments controlling what information individuals should be exposed to.
- Vague concepts of "crime".
- Limited safeguards.
- Create spheres of influence.

3

Budapest Convention: a global framework for cooperation on cybercrime

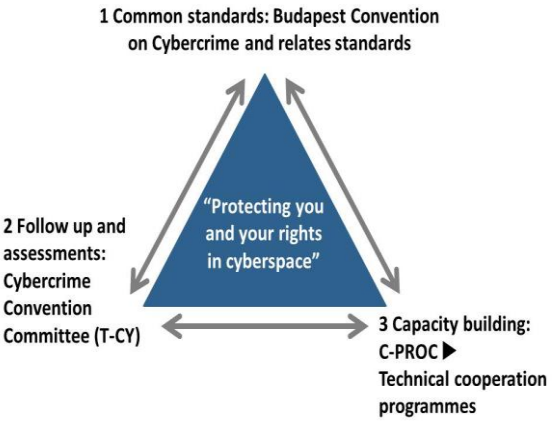
Budapest Convention on Cybercrime:

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

+ Guidance Notes

+ Protocol on enhanced cooperation on cybercrime and electronic evidence under negotiation

By October 2020: 65 Parties and 12 Observer States



www.coe.int/cybercrime

4

Budapest Convention: a global framework for cooperation on cybercrime

DNS (including COVID-19) related crime

- Phishing
- Malware
- Ransomware
- Botnets and DDOS
- Spam
- Fraud

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

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

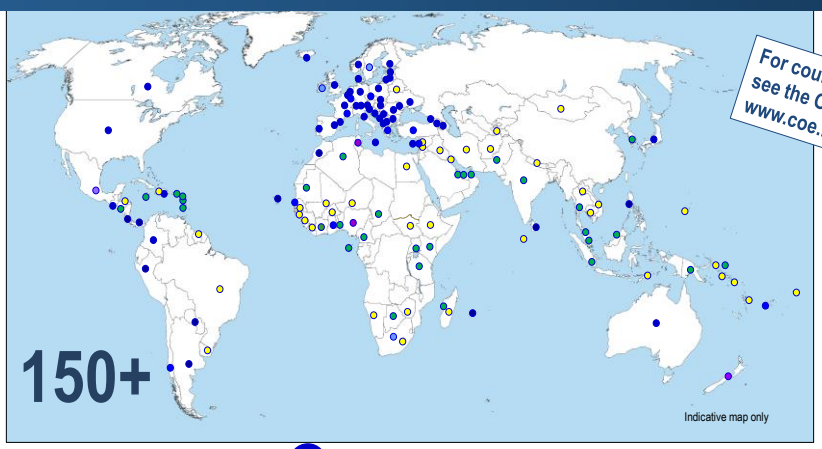
Framework for international cooperation

- Articles 23 - 35

www.coe.int/cybercrime

5

Budapest Convention: a global framework for cooperation on cybercrime



For country-specific information see the Octopus Community at www.coe.int/cybercrime

Parties:	65
Signed:	3
Invited to accede:	9
=	77

Other States with laws largely in line with Budapest Convention = 20+

Further States drawing on Budapest Convention for legislation = 50+

www.coe.int/cybercrime

6

The Budapest Convention tomorrow: towards a new Protocol

Why a new Protocol?

- The scale and quantity of cybercrime, devices, users and victims
- Cloud computing, territoriality and jurisdiction
  - Where is the crime?
  - Where is the data, where is the evidence?
  - Who has the evidence?
  - What legal regime applies to order / disclose data?
- The challenge of mutual legal assistance

Protocol prepared by the Cybercrime Convention Committee

(= Parties to the Budapest Convention)

2017 – 2020

To be opened for signature in 2021?

The Budapest Convention tomorrow: towards a new Protocol

Elements of the Protocol

- Provisions for more efficient MLA
- Expedited cooperation in emergencies
- Direct cooperation with providers in other jurisdictions
  - Subscriber information
  - [WHOIS]
- Data protection safeguards

Conclusion

- The Budapest Convention – with its future Protocol – is likely to remain the most relevant international standard on cybercrime as a matter of criminal justice
- Offences involving DNS abuse are covered by the Convention
- The procedural and international cooperation provisions are available to investigate and prosecute DNS abuse
- Discussions are underway on including a legal basis for requests for and the disclosure of domain name registration information (WHOIS) across Parties to this Protocol.