Workshop for Iraq on
Digital Evidence Collected from Terrorist Bomb Scenes
UNODC, Vienna, 25-28 March 2019

Legislative reforms and structural requirements under the Budapest Convention on Cybercrime

Alexander Seger, Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
1949.2019

www.coe.int/cybercrime

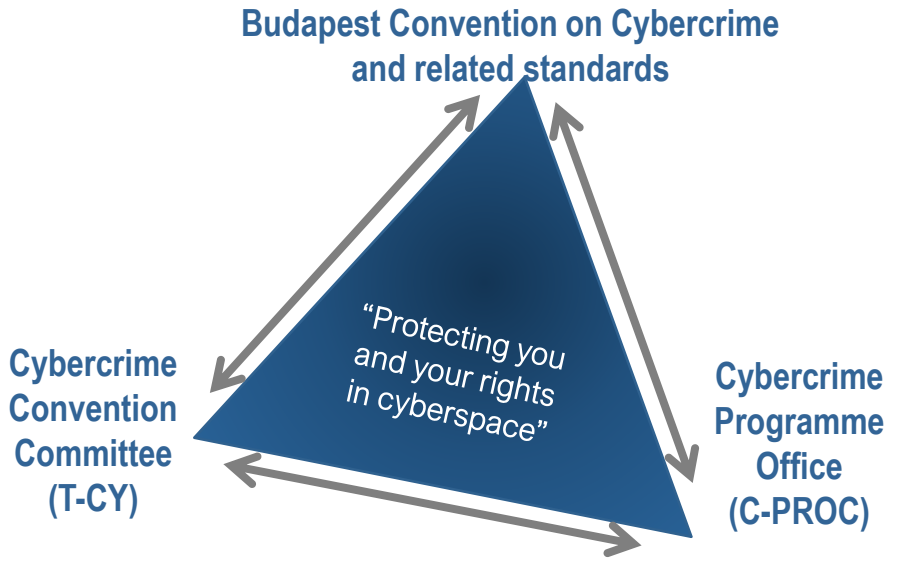
1

About the Budapest Convention on Cybercrime

- 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

2

The "mechanism" of the Budapest Covnention



3

Scope 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

Harmonisation

4

Scope of the Budapest Convention

Cybercrime

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

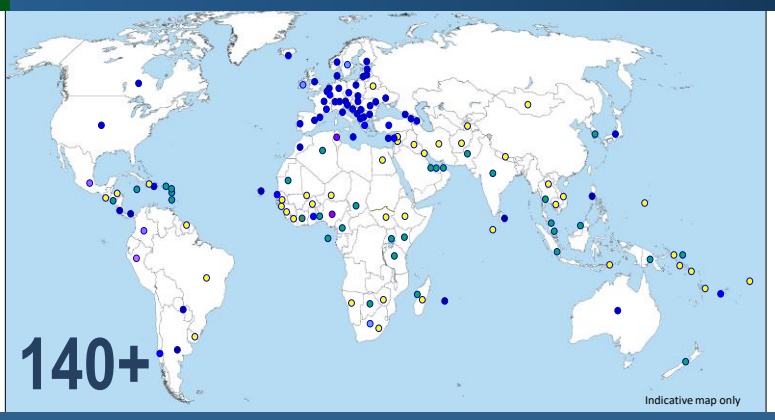
+

Electronic evidence

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

5

REACH of the Budapest Convention



Ratified/acceded: 63

Signed: 3

Invited to accede: 5

= 71

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

Further States drawing on Budapest Convention for legislation = 50+

6

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

7

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

8

8

Requirements in terms of legislation: substantive law

Article	Budapest Convention	Domestic Law
Art. 1	Definitions	
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. 9	Child pornography	
Art. 10	IPR offences	
Art. 11	Attempt, aiding, abetting	
Art. 12	Corporate liability	

9

Requirements in terms of legislation: substantive law

Concern: Laws on cybercrime used to prosecute speech

- The protection of national security and public order is a legitimate ground for restricting freedom of expression where that restriction is
  - prescribed by law
  - necessary in a democratic society
  - proportionate
- Broad, vaguely defined provisions do not meet these requirements
  - "use of computers with intent to compromise the independence of the state or its unity, integrity, safety or any of its high economic, political, social, military or security interests or subscribe, participate, negotiate, promote, contract or deal with an enemy in any way in order to destabilise security and public order or expose the country to danger …"
  - "use of computers to create chaos in order to weaken the trust of the electronic system of the state or provoke or promote armed disobedience, provoke religious or sectarian strife, disturb public order, or harm the reputation of the country … "
  - "creation of sites with a view to disseminating ideas contrary to public order or morality"
  - "broadcasting information to mislead security forces"
- Problematic trend ► Discredits legitimate action on cybercrime ► violates fundamental rights

10

Requirements in terms of legislation: procedural powers

Article	Budapest Convention	Domestic law
Art. 15	Conditions and safeguards	
Art. 16	Expedited preservation	
Art. 17	Expedited preservation and partial disclosure of traffic data	
Art. 18	Production order	
Art. 19	Search and seizure	
Art. 20	Real-time collection traffic data	
Art. 21	Interception of content data	
Art. 22	Jurisdiction	

11

Requirements in terms of legislation: procedural powers

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties

12

Requirements in terms of legislation: International cooperation

Chapter III of the Convention - International cooperation

Section 1 – General principles

- Art 23 General principles on international cooperation
- Art 24 Principles related to extradition
- Art 25 Principles related to mutual legal assistance
- Art 26 Spontaneous information
- Art 27 MLA in the absence of applicable international instruments
- Art 28 Confidentiality and limitation on use

13

Requirements in terms of legislation: International cooperation

Chapter III - International cooperation

Section 2 – Specific provisions

- Art 29 - Expedited preservation of stored computer data
- Art 30 - Expedited disclosure of preserved computer data
- Art 31 - Mutual assistance regarding accessing stored computer data
- Art 32 - Trans-border access to stored computer data (public/with consent)
- Art 33 - Mutual assistance in real-time collection of traffic data
- Art 34 - Mutual assistance regarding interception of content data
- Art 35 - 24/7 network

14

Requirements in terms of institutions

Declare:

- **Authority for extradition (Article 24)**
- **Authority for mutual legal assistance (Article 27)**
- **24/7 point of contact (Article 35)**

15

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"

16