



Workshop on effective cybercrime legislation in Eastern Africa
Dar es Salaam, Tanzania, 22 -24 August 2013

Session 2: International perspectives

The Budapest Convention on Cybercrime

Alexander Seger
Secretary Cybercrime Convention Committee
Council of Europe

www.coe.int/cybercrime

1

About the Budapest Convention

Opened for signature November 2001 in Budapest

Followed by Cybercrime Convention Committee (T-CY) = Committee of the Parties

As at August 2013:

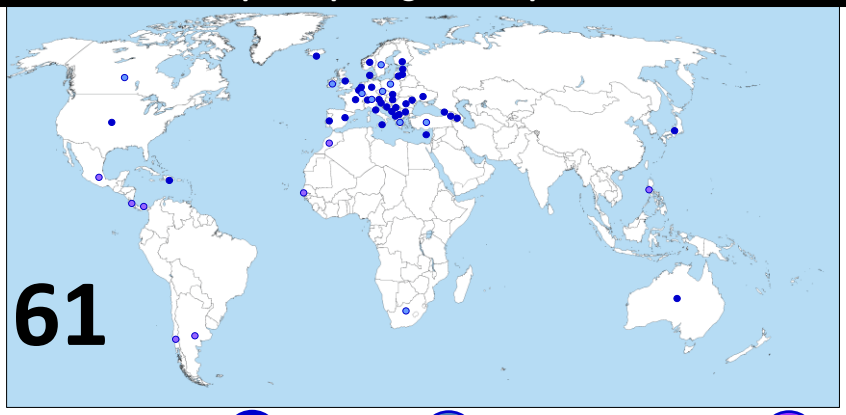
- **40 parties (36 European, Australia, Dominican Republic, Japan and USA)**
- **11 signatories (European, Canada, South Africa)**
- **10 states invited to accede (Argentina, Chile, Costa Rica, Israel, Mauritius, Mexico, Morocco, Panama, Philippines, Senegal)**

= 61 states are parties/are committed to become parties

- **Additional invitations to accede are in process**
- **Many more have used Budapest Convention as a guideline for domestic legislation**

2

About States participating in Budapest Convention



Ratified/acceded: 40

European
- Australia
- Dominican Republic
- Japan
- USA

Signed: 11
- 9 European
- Canada
- South Africa

Invited to accede: 10
- Argentina
- Chile
- Costa Rica
- Israel
- Mauritius
- Mexico
- Morocco
- Panama
- Philippines
- Senegal

3

About joining the Budapest Convention

Treaty open for accession by any State (article 37)

Phase 1:
- If a country has 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

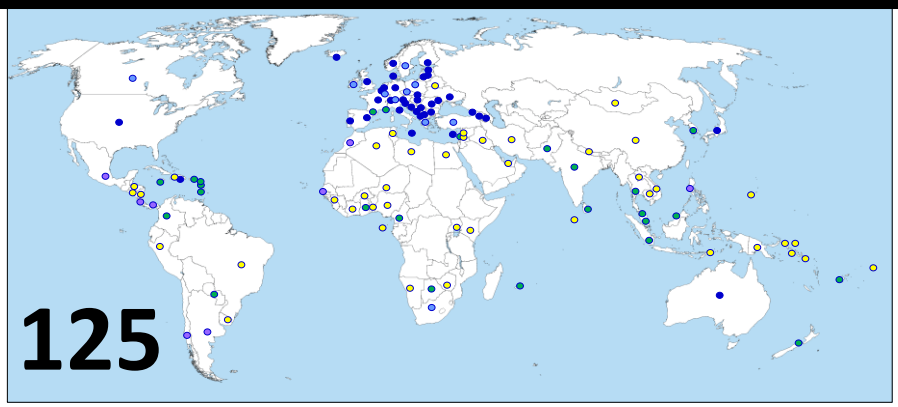
Phase 2:
- Domestic procedure (e.g. decision by national Parliament)
- Deposit the instrument of accession at the Council of Europe

▶ Acceded: Australia, Dominican Republic

▶ Invited: Argentina, Chile, Costa Rica, Israel, Mauritius, Mexico, Morocco, Panama, Philippines, Senegal

4

States using Budapest Convention



Indicative map only

Ratified/acceded: 40

Signed: 11

Invited to accede: 10

= 61

Other States with laws/draft laws largely in line with Budapest Convention = 19

Further States drawing on Budapest Convention for legislation = 45

5

About the scope of 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
- Search and seizure
- Interception of computer data

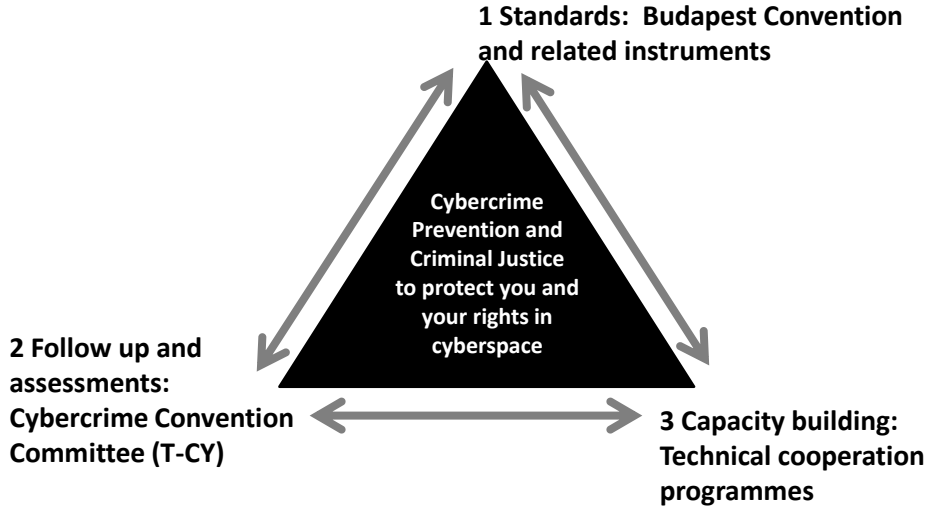
+

International cooperation
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

6

Functioning of the Budapest Convention



www.coe.int/cybercrime

7

Budapest Convention as a guideline

- Use as "checklist"
- Compare articles

See country profiles at

www.coe.int/cybercrime

Articles of the Convention	Provisions in domestic law
Art 4 System interference	?
Art 6 Misue of devices	?
Art 9 Child pornography	?
Art 16 Expedited preservation	?

www.coe.int/cybercrime

8

Budapest Convention as a guideline

Example: Uganda Computer Misuse Act 2011

Article	Budapest Convention	Law of Uganda
Art. 1	Definitions	Article 2 CMA
Art. 2	Illegal access	Article 12(1) etc.
Art. 3	Illegal interception	Articles 15, 12(1)
Art. 4	Data interference	Article 12(2)
Art. 5	System interference	Article 16
Art. 6	Misuse of devices	Article 12 (3), (4)

www.coe.int/cybercrime

9

Budapest Convention as a guideline

Example: Uganda Computer Misuse Act 2011

Article 5 of the Convention: system interference

- Establish as criminal offences under domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

16 CMA. Unauthorised obstruction of use of computer.

A person who, knowingly and without authority or lawful excuse—

(a) interferes with or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer, commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

10

Budapest Convention as a guideline

Article	Budapest Convention	Law of Uganda
Art. 7	Computer-related forgery	
Art. 8	Computer-related fraud	Article 19
Art. 9	Child pornography	Article 23
Art. 10	IPR offences	
Art. 11	Attempt, aiding, abetting	
Art. 12	Corporate liability	

www.coe.int/cybercrime

11

Budapest Convention as a guideline

Article	Budapest Convention	Law of Uganda
Art. 15	Conditions and safeguards	
Art. 16	Expedited preservation	Article 9
Art. 17	Expedited preservation and partial disclosure of traffic data	Article 10
Art. 18	Production order	
Art. 19	Search and seizure	Article 28
Art. 20	Real-time collection traffic data	
Art. 21	Interception of content data	
Art. 22	Jurisdiction	

12

Budapest Convention as a guideline

Example: Uganda Computer Misuse Act 2011

Article 16 of the Convention – Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

9 CMA. Preservation Order.

(1) An investigative officer may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

(2) For the purpose of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) shall remain in force—

(a) until such time as may reasonably be required for the investigation of an offence; or

(b) where prosecution is instituted, until the final determination of the case or until such time as the court deems fit.

13

Capacity building

Capacity building: Technical cooperation programmes

Focus on:

- Cybercrime strategies
- Legislation and safeguards
- Cybercrime units
- Law enforcement training
- Judicial training
- Financial investigations
- Protecting children
- Public/private cooperation
- International cooperation

Council of Europe global and regional projects:

- 500+ activities with 125+ countries & 130+ organisations and private sector since 2006
- New joint EU/COE project on Global Action on Cybercrime (GLACY) in 2013
- Encouraging other donors to provide assistance to countries in implementing Budapest Convention

14

Capacity building

Capacity building: Tools - examples

- Electronic evidence guide
- 1st responders training pack
- Judicial training – introductory course
- Judicial training – advanced course

- LEA/ISP cooperation guidelines
- Cybercrime strategies
- Criminal money flows – typology study
- Etc.

15

Effectiveness/Impact of the Budapest Convention

- 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"

The Budapest Convention is in place and functioning.

Obstacles:

1. Limited criminal justice capacities
2. Political disagreements

www.coe.int/cybercrime

16

Benefits for Africa

Benefits

- ✓ Trusted and efficient cooperation with other Parties
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- ✓ Enhanced trust by private sector
- ✓ Technical assistance and capacity building

"Cost": Commitment to cooperate

Disadvantages?

17

Contact for follow up

Alexander.seger@coe.int

Secretary of the Cybercrime Convention Committee (T-CY)
Council of Europe
Strasbourg, France

www.coe.int/cybercrime

18