



[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

## Budapest Convention

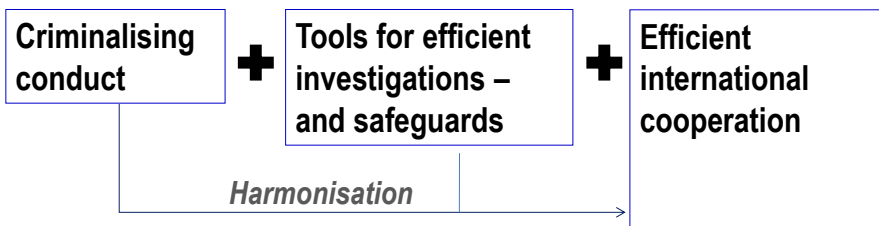
- **guideline for harmonised legislation**
- **framework for international cooperation**
- **vector for capacity building**

**UN Expert Group on Cybercrime – Vienna, January 2011**

Alexander Seger  
 Council of Europe,  
 Strasbourg, France  
 Tel +33-3-9021-4506  
[alexander.seger@coe.int](mailto:alexander.seger@coe.int)

1

## Legislative responses to cybercrime: What is required?



**= The Budapest Convention on Cybercrime as a solution**

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

2

2

## The Convention on Cybercrime

### **The Budapest Convention**

- Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA
- Opened for signature in Budapest in November 2001
- In force since July 2004

### **The Protocol on Xenophobia and Racism Committed through Computer Systems**

- Opened for signature in January 2003
- In force since March 2006

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

3

3

## Budapest Convention: Scope

### **Definitions/use of terms (Art 1)**

- Computer system
- Computer data
- Service provider
- Traffic data

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

4

4

## Budapest Convention: Scope

### Criminalise conduct

Offences against computers - Offences by means of computers

1. Offences against the confidentiality, integrity and availability of computer data and systems
  - Illegal access to a computer system (Art 2)
  - Illegal interception (Art 3)
  - Data interference (Art 4)
  - System interference (Art 5)
  - Misuse of devices (Art 6)
2. Computer-related forgery (Art 7) and fraud (Art 8)
3. Content-related offences (child pornography (Art 9), xenophobia & racism [protocol])
4. Offences related to intellectual property rights and similar rights (Art 10)

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

5

5

## Budapest Convention: Scope

### Procedural law tools

- Common provisions (Art 14 scope of procedural provisions, Art 15 conditions and safeguards)
- Expedited preservation of stored computer data (Art 16) and partial disclosure of traffic data (Art 17)
- Production order (Art 18)
- Search and seizure of stored computer data (Art 19)
- Real-time collection/interception of computer data (Art 20 traffic data, Art 21 interception of content data)

*These apply to all criminal offences involving a computer system!*

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

6

6

## Budapest Convention: Scope

### International cooperation

#### 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

#### Specific provisions

- Art 29 - Expedited preservation of stored computer data
- Art 30 - Expedited disclosure of preserved computer data
- Art 31 - Mutual assistance re accessing stored computer data
- Art 32 - Trans-border access to stored computer data
- Art 33 – MLA in real-time collection of traffic data
- Art 34 – MLA interception in content data
- Art 35 - 24/7 network

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

7

7

## Budapest Convention: Scope

### Final provisions

- Art 36 Signature and entry into force (open to member States and non-members which have participated in its elaboration)
- Art 37 Accession (any State may accede following majority vote in Committee of Ministers and unanimous vote by the parties entitled to sit on the Committee of Ministers)
- Art 40 – 43 Declarations, reservations
- Art 46 – Consultations of the parties

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

8

8

## The Convention on Cybercrime – State of implementation

- Signatures (47): European countries, Canada, Japan and South Africa, USA
- Ratifications (30): European countries and USA
- Invited to accede (7): Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines
- Used as a guideline, reference standard or model law in a large number of countries
- Consideration of additions to Convention, e.g. jurisdiction and trans-border access

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

9

9

## Budapest Convention as a guideline/model law

- Use as a checklist
- Compare provisions
- Use wording

Provision of Convention	Provision in national law
Art 4 System interference	?
Art 6 Misuse of devices	?
Art 9 Child pornography	?
Art 16 Expedited preservation	?
Art 18 Production order	?

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

10

10

## Budapest Convention as a guideline/model law – useful tools

### Country profiles

Provision of Convention	Country A	Country B	
Art 4 System interference	§	§	
Art 6 Misuse of devices	§	§	
Art 9 Child pornography	§	§	
Art 16 Expedited preservation	§	§	

### Article profiles

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

1  
1

11

## Budapest Convention: legislative analyses and reviews

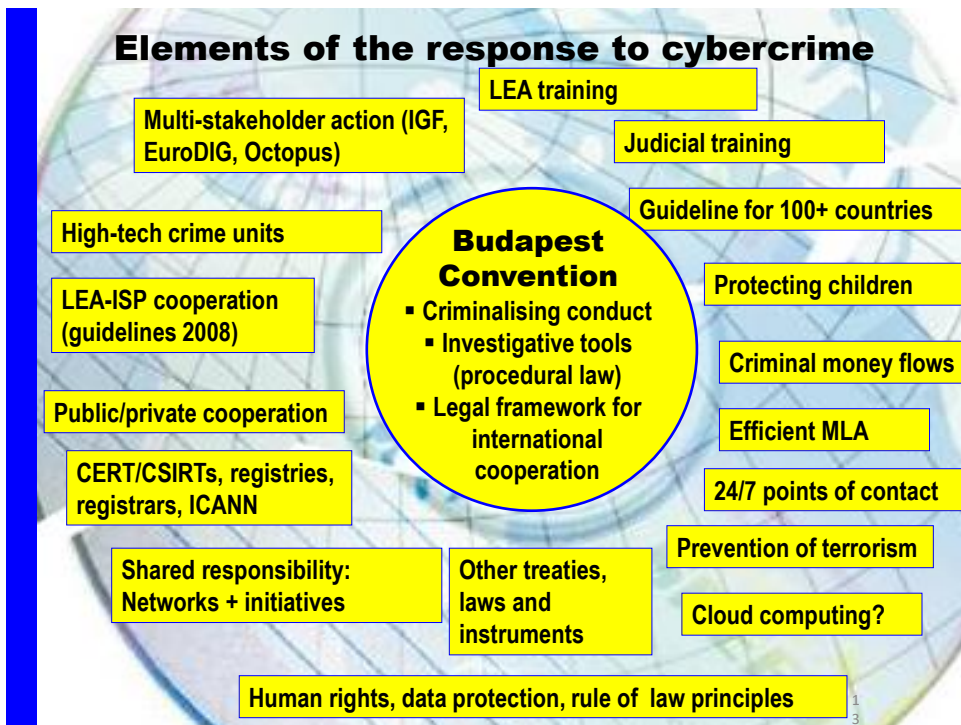
Legislative review workshops and/or written analysis by CoE (with partners):

- 12 countries of Asia (including 2 workshops for ASEAN countries)
  - 16 countries of Latin America
  - 13 countries of the Caribbean
  - 18 countries of Africa
  - European countries
  - Coming up: legislative review workshop for 15 Pacific Island States
- = Much progress already made since 2006 in the strengthening and harmonising of legislation globally
- = Reforms underway in many countries at this moment
- = UN Expert Group: what message?

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

1  
2

12



13

## Core problem

Many tools and instruments against cybercrime are already available. Others are being developed.

But they are not necessarily implemented for lack of resources, capacities, commitment.

14

## **The way ahead: launch a global capacity building effort**

**Greatest impact by common effort to support implementation of existing tools and instruments against cybercrime**



### **Support**

- Strengthening of legislation
- Judicial training
- LEA training
- High-tech crime units
- LEA-ISP cooperation
- International cooperation
- Protection of children
- Rule of law and human rights
- Political commitment

1. Review needs
2. Provide support
3. Assess progress

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

1  
5

15

## **Examples of capacity building projects**

- CoE global Project on Cybercrime (since 2006)
  - Cybercrime@IPA regional project of the EU and COE
  - Cybercrime@EAP regional project of the EU and COE
- = Support provided to some 80 countries since 2006
- But much more comprehensive support required
- Action plan for global capacity building effort

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

1  
6

16



**Thank you**

**Alexander.seger@coe.int**

