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
Legislative responses to cybercrime: What is required?

- Criminalising conduct
- Tools for efficient investigations – and safeguards
- Efficient international cooperation

= The Budapest Convention on Cybercrime as a solution
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
Budapest Convention: Scope

Definitions/use of terms (Art 1)

- Computer system
- Computer data
- Service provider
- Traffic data
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)
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!
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
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
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
Budapest Convention as a guideline/model law

- Use as a checklist
- Compare provisions
- Use wording

<table>
<thead>
<tr>
<th>Provision of Convention</th>
<th>Provision in national law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art 4 System interference</td>
<td>?</td>
</tr>
<tr>
<td>Art 6 Misuse of devices</td>
<td>?</td>
</tr>
<tr>
<td>Art 9 Child pornography</td>
<td>?</td>
</tr>
<tr>
<td>Art 16 Expedited preservation</td>
<td>?</td>
</tr>
<tr>
<td>Art 18 Production order</td>
<td>?</td>
</tr>
</tbody>
</table>
# Budapest Convention as a guideline/model law – useful tools

## Country profiles

<table>
<thead>
<tr>
<th>Provision of Convention</th>
<th>Country A</th>
<th>Country B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art 4 System interference</td>
<td>§</td>
<td>§</td>
</tr>
<tr>
<td>Art 6 Misuse of devices</td>
<td>§</td>
<td>§</td>
</tr>
<tr>
<td>Art 9 Child pornography</td>
<td>§</td>
<td>§</td>
</tr>
<tr>
<td>Art 16 Expedited preservation</td>
<td>§</td>
<td>§</td>
</tr>
</tbody>
</table>
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?
Guideline for 100+ countries

LEA-ISP cooperation (guidelines 2008)

Criminal money flows

24/7 points of contact

Efficient MLA

Protecting children

CERT/CSIRTs, registries, registrars, ICANN

Public/private cooperation

High-tech crime units

LEA training

Judicial training

Guideline for 100+ countries

Budapest Convention

- Criminalising conduct
- Investigative tools (procedural law)
- Legal framework for international cooperation

Shared responsibility: Networks + initiatives

Multi-stakeholder action (IGF, EuroDIG, Octopus)

Other treaties, laws and instruments

Human rights, data protection, rule of law principles

Prevention of terrorism

Cloud computing?
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.
The way ahead: launch a global capacity building effort

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

1. Review needs

2. Provide support

3. Assess progress

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

www.coe.int/cybercrime
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
Thank you

Alexander.seger@coe.int