



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

The Convention on Cybercrime: state of implementation

Octopus Interface Conference, Council of Europe, Strasbourg, 1-2 April 2008

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

1

Supporting the implementation of the Convention on Cybercrime: the approach

Setting standards:

The Convention on Cybercrime and the Protocol on Xenophobia and Racism

Following implementation:

The Cybercrime Convention Committee (T-CY)

**Technical cooperation:
The Project on Cybercrime**

The Project on Cybercrime

Project objective: To promote broad implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189)

Output 1: Legislation

Output 2: Criminal justice capacities

Output 3: International cooperation

Indicators of success include:

➤ 40 countries will be parties to the Convention (ETS 185), and 12 will be parties to the Protocol (ETS 189)

Start: Sep 06

End: Feb 09

**Funding: CoE,
Microsoft,
Estonia**

**Additional
funding
required**

2 Signatures, ratifications, accessions

Convention on Cybercrime (as at 31 March 2008):

- **Ratifications: 22**
- **Signatures: 21**
- **Invitations to accede: 2**

Protocol on Xenophobia and Racism committed through Computer Systems (as at 31 March 2008):

- **Ratifications: 11**
- **Signatures: 20**
- **Invitations to accede: 0**

Countries that are parties to

the Convention:

- Albania
- Armenia
- Bosnia and Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Hungary
- Iceland
- Latvia
- Lithuania
- Netherlands
- Norway
- Romania
- Slovakia
- Slovenia
- The „former Yugoslav Republic of Macedonia“
- Ukraine
- United States of America

the Protocol:

- Albania
- Armenia
- Bosnia and Herzegovina
- Cyprus
- Denmark
- France
- Latvia
- Lithuania
- Slovenia
- The „former Yugoslav Republic of Macedonia“
- Ukraine

Countries that have signed the Convention:

- Austria
- Belgium
- Canada
- Czech Rep
- Germany
- Greece
- Ireland
- Italy
- Japan
- Luxembourg
- Malta
- Moldova
- Montenegro
- Poland
- Portugal
- Serbia
- South Africa
- Spain
- Sweden
- Switzerland
- United Kingdom

Invited to accede:

- Costa Rica
- Mexico

Trends in ratifications to date:

Year	2002	2003	2004	2005	2006	2007	2008
Ratifications	+2	+2	+4	+3	+7	+3	+1 (Jan-Mar)
Total	2	4	8	11	18	21	22

Factors preventing faster ratification:

- **Countries should have legislation compliant with Convention when depositing the instrument of ratification/accession**
- **Convention has broad range of procedural provisions that take time and parliamentary majorities to adopt**
- **Cybercrime not always a priority of governments/parliaments**

Outlook:

Expect 15+ ratifications/accessions between April 2008 and February 2009

For example:

- **Italy: Parliament ratified in March 2008**
- **Germany: Expected to ratify in April/May 2008**
- **Georgia: Signature in April 2008**
- **South Africa: Signature of Protocol in April 2008**
- **Philippines: Formal invitation to accede in May 2008**

Internet Governance Forum (India, December 2008) as target date?

3 The Convention as a guideline for the development of cybercrime legislation

Major global trend since 2006: countries worldwide are developing legislation on cybercrime

- For example: Argentina, Brazil, Colombia, Egypt, India, Indonesia, Morocco, Nigeria, Pakistan, Philippines, most European countries
- Or adopted new legislation in 2007/8 such as Botswana, Dominican Republic or Sri Lanka

The Convention on Cybercrime serves as a guideline (or model law) globally

Model law function of the Convention

- 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	?

Support by the Project on Cybercrime

- **Country profiles on cybercrime legislation**
- **Detailed analyses of draft laws (so far: Argentina, Brazil, Colombia, Egypt, India, Indonesia, Nigeria, Philippines, Serbia)**
- **Sharing experience (Octopus Interface, regional events)**

4 The Convention as a framework for international cooperation

- **The Convention (Chapter III) is increasingly used as a legal basis for international cooperation**
- **Contributes to the creation of additional 24/7 points of contact**
- **Examples of good practice available**

Issues:

- **Need to enhance the number of countries that are party to the Convention**
- **Need to make 24/7 points of contact more effective**
- **Preliminary measures (e.g. expedited preservation) need to be followed up by efficient MLA process**

5 **Acceding to the Convention**

Article 37: Convention is open for accession by third countries

Accession process:

- 1. Once legislation has been adopted or is in advanced stage, government to send a letter to Secretary General of CoE with a request to initiate consultation with parties to the Convention**
- 2. Secretariat of CoE will carry out consultations and put question before Committee of Ministers**
- 3. If vote is positive, the country will be invited to accede**
- 4. The country is then free to decide when to accede, that is, deposit the instrument of accession**

6 Issues

Convention opened for signature in 2001. Focus on conduct rather than technology. Still up to date.

For example:

- Covers DDOS attacks and measures against cyberterrorism**
- Covers most elements related to ID theft and related fraud**

Cybercrime keeps evolving: need continuous review of the adequacy of the international response

Issues

**Investigating cybercrime/
preventing terrorism/
data retention/
authentication etc**

What

Balance?

**Privacy/
protection of
personal data/
freedom of expression**

**Assumption: 99.9% of ICT use is
legitimate**

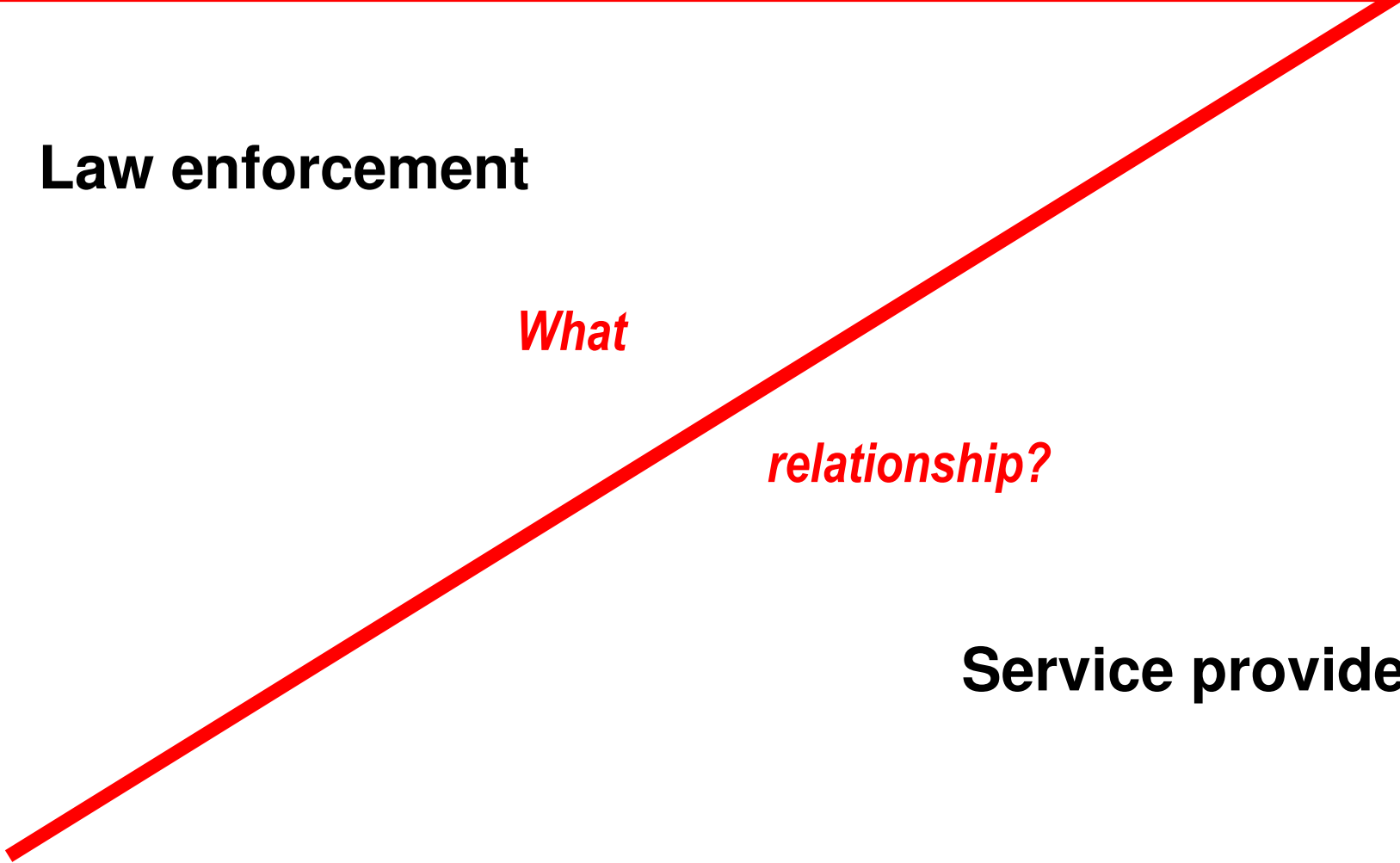
Issues

Law enforcement

What

relationship?

Service providers



Issues

**Efficiency of investigations/
technical possibilities**

What

safeguards?

Due process

Issues

**= importance of Conditions
and Safeguards (Article 15
of the Convention)**

6 **The way ahead**

- **Need to enlarge the number of parties to the Convention**
- **Support strengthening and harmonisation of cybercrime legislation worldwide using the Convention as a guideline**
- **Promote accession to the Convention as a framework for international cooperation**
- **Clear legal basis for public-private partnership**
- **Guidelines for cooperation between ISP and law enforcement**
- **Strengthen law enforcement/criminal justice capacities**
- **Balance security concerns and civil rights**



Thank you.

Alexander.seger@coe.int



www.coe.int/cybercrime