



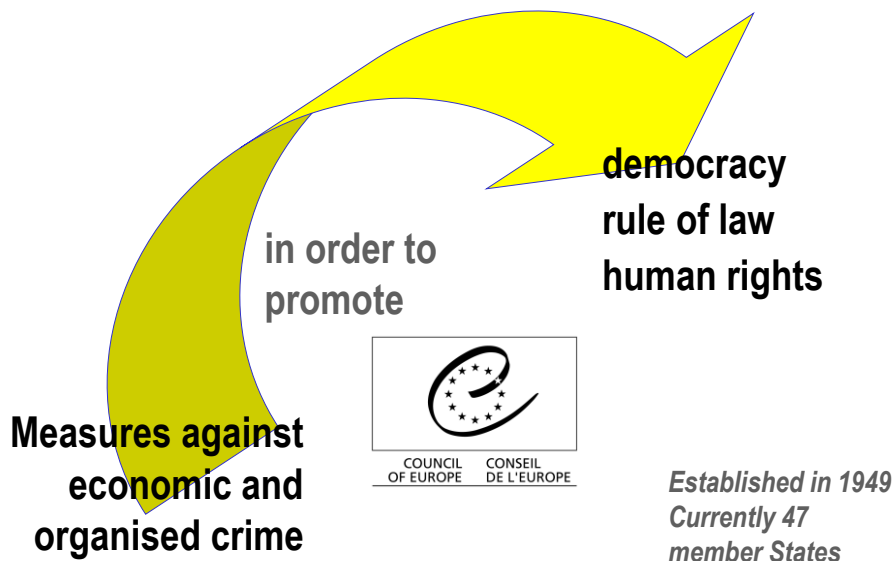
# The Convention on Cybercrime & the question of “cyberterrorism”

*IMPACT Summit, Kuala Lumpur, Malaysia, 20-22 May 2008*

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

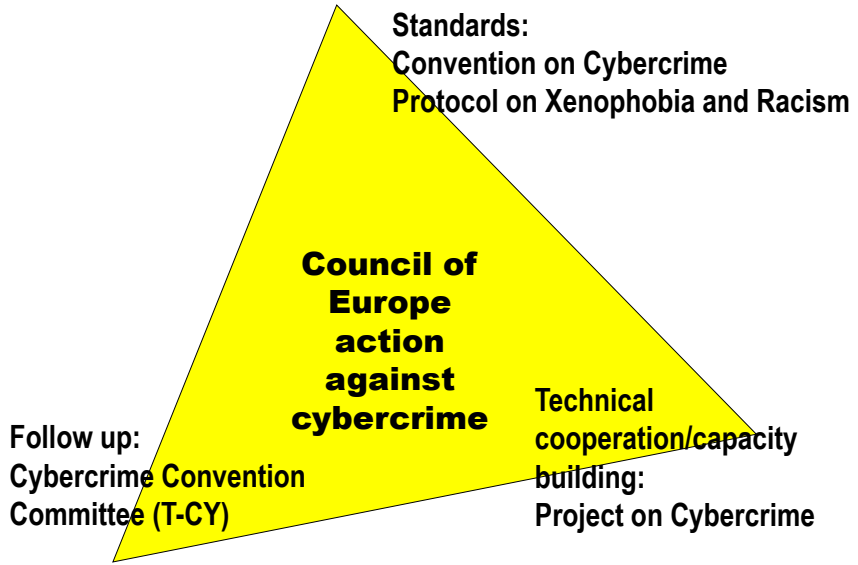
1

**About the Council of Europe ... [www.coe.int](http://www.coe.int)**



2

# The approach against cybercrime



3

## 1 Cybercrime – current challenges

Dependency of societies on information and communication technologies.  
This dependency makes societies highly vulnerable to cybercrimes

Shift in the threat landscape: from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes	Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading	Spam nuisance and carriers of malware
Offenders increasingly organising for crime aimed at generating illicit profits	Offences related to identity theft	Child pornography and sexual exploitation on the internet increasingly commercial
Botnets one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware)	Growing risk of cyber-attacks against critical infrastructure	Use of internet for terrorist purposes (attacks against infrastructure, logistics, recruitment, finances, propaganda)

**But:** Vast majority of people use ICT for legitimate purposes  
Need to balance security and civil rights concerns

4

4

## **Terrorist use of the Internet**

- **Attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interestets, including loss of life**
- **Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism, recruitment or training**
- **Use of ICT by terrorists for logistical purposes such as internal communication, gathering intelligence, target analyses**

5

**2**

## **What criminal law response?**

**Question analysed by the Council of Europe Group of experts on terrorism, CODEXTER (2005 – 2008):**

- **Are existing international instruments sufficient or should additional treaties be developed to deal with the use of the internet for terrorist purposes?**

**Result:**

- **Full and broadest possible implementation of the Convention on Cybercrime and the Convention for the Prevention of Terrorism should be given priority**
- **Additional instruments not necessary at this stage**

6

### **3 The Convention on Cybercrime**

- **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**

7

7

### **Structure and content of the Convention**

**Chapter I: Definitions**

**Chapter II: Measures at national level**

**Section 1 - Substantive criminal law (offences to be criminalised)**

**Section 2 - Procedural law**

**Section 3 - Jurisdiction**

**Chapter III: International cooperation**

**Section 1 - General principles**

**Section 2 - Specific provisions**

**Chapter IV: Final provisions**

8

8

## Chapter II – Measures at national level

### Section 1 – Substantive criminal law

- Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices)
- Title 2 – Computer-related offences (forgery, fraud)
- Title 3 – Content-related offences (child pornography)
- Title 4 – Infringements of copyright and related rights
- Title 5 – Ancillary liability and sanctions (attempt, aiding, abetting, corporate liability, sanctions and measures)

9

9

### Section 2 – Procedural law

- Title 1 – Common provisions (scope of procedural provisions, conditions and safeguards)
- Title 2 – Expedited preservation of stored computer data (and traffic data and partial disclosure)
- Title 3 – Production order
- Title 4 – Search and seizure of stored computer data
- Title 5 – Real-time collection of computer data (traffic data, interception of content data)

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

10

## **Chapter III - 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**

11

## **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 re 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 re interception of content data**
- **Art 35 - 24/7 network**

12

## Chapter IV – 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**

13

13

## The Convention on Cybercrime and terrorist use of ICT

- **Convention aimed at comprehensive protection of integrity and availability of computer data and systems**
- **Data and system interference (including attacks against critical infrastructure through ICT) covered under Articles 4 and 5**
- **But review level of penalties: fines or 6 months imprisonment in some, up to 12 years imprisonment in other countries**
- **Procedural provisions apply**
- **International cooperation provisions apply**
- **Minimum of harmonisation of substantive and procedural law**
- **Convention on Cybercrime open for accession to third countries**
- **Main problem: More countries need to become Parties to the Convention**

14

14

## Implementation – current status

- The Convention entered into force in July 2004
  - 22 ratifications + 22 signatures (as of 1 April 2008)
  - Signed by Canada, Japan, South Africa, ratified by USA
  - Costa Rica, Mexico, Philippines have been invited to accede
  - Legislative amendments adopted or underway in many other countries (Argentina, Brazil, Caribbean countries, Colombia, Dominican Republic, Egypt, India, Indonesia, Nigeria, Philippines, Sri Lanka etc.) and accession to the Convention under consideration
- = Major global trend towards better cybercrime legislation**
- = Convention provides a global standard**

15

4

## Convention for the Prevention of Terrorism (Council of Europe)

- Opened for signature in Warsaw 2005
- Entered into force in June 2007
- 14 ratifications + 28 signatures by May 2008
- Open for accession by third countries

16

16

## **Convention for the Prevention of Terrorism: contents**

- Article 4 – National prevention policies + Article 5 – international cooperation on prevention of terrorism
- Article 5 – Public provocation to commit a terrorist offence
- Article 6 – Recruitment for terrorism
- Article 7 – Training for terrorism
- Article 8 – Irrelevance of the commission of a terrorist offence
- Article 13 – Protection, compensation and support for victims of terrorism
- Article 15 – Duty to investigate
- Article 17 – International co-operation in criminal matters
- Article 18 – Extradite or prosecute
- Article 20 – Exclusion of the political exception clause
- Article 21 – Discrimination clause
- Article 24 – Accession to the Convention

17

17

## **Convention for the Prevention of Terrorism: offences**

### **Article 5 – Public provocation to commit a terrorist offence**

**1** For the purposes of this Convention, "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed

**2** Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

18

18

## **Convention for the Prevention of Terrorism: offences**

### **Article 6 – Recruitment for terrorism**

1 For the purposes of this Convention, "recruitment for terrorism" means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group.

2 Each Party shall adopt such measures as may be necessary to establish recruitment for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

19

19

## **Convention for the Prevention of Terrorism: offences**

### **Article 7 – Training for terrorism**

1 For the purposes of this Convention, "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence, knowing that the skills provided are intended to be used for this purpose.

2 Each Party shall adopt such measures as may be necessary to establish training for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

20

20

Attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interests, including loss of life

Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism recruitment or training

Use of ICT by terrorists for logistical purposes such as internal communication, gathering intelligence, target analyses

Covered by the

➤ Convention on Cybercrime

in combination with the

➤ Convention for the Prevention of Terrorism

21

21

## Conclusions

### The way ahead:

- Strengthen national legislation using the Convention on Cybercrime and the Convention for the Prevention of Terrorism as a guideline
- Balance security and human rights concerns and establish safeguards
- Consider accession to both treaties as a basis for international cooperation
- Council of Europe is ready to assist

22

22



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

**Thank you.**

**Alexander.seger@coe.int**