www.coe.int/cybercrime

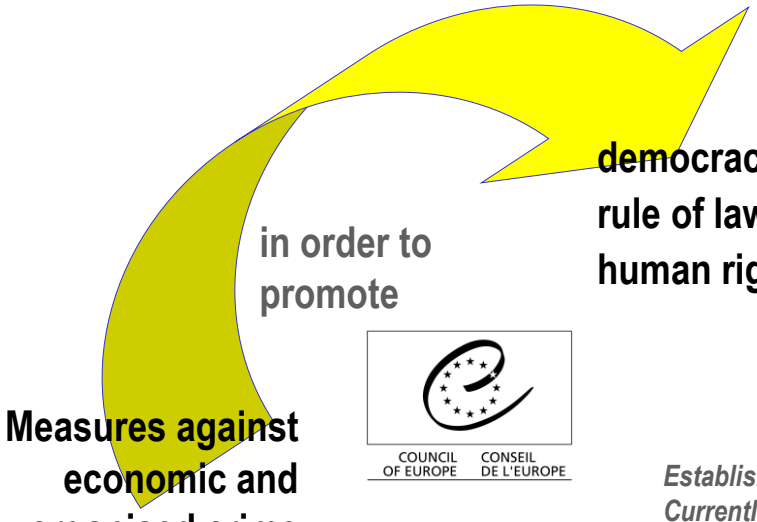
Electronic Law – National and International Rules: The Convention on Cybercrime as a framework

73rd ILA Conference (Rio de Janeiro, Brazil, 17-21 August 2008)

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

1

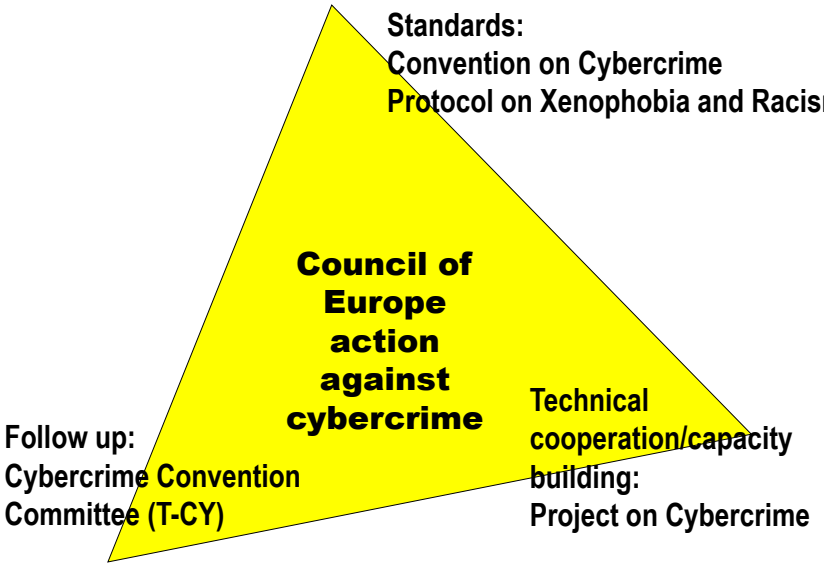
1 About the Council of Europe ... www.coe.int



Established in 1949
Currently 47
member States

2

The approach against cybercrime



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

The Protocol on Xenophobia and Racism Committed through Computer Systems

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

4

4

Structure and content of the Convention

Chapter I: Definitions

Chapter II: Measures at national level
- **Section 1 - Substantive criminal law (conduct to be criminalised)**
- **Section 2 - Procedural law**
- **Section 3 - Jurisdiction**

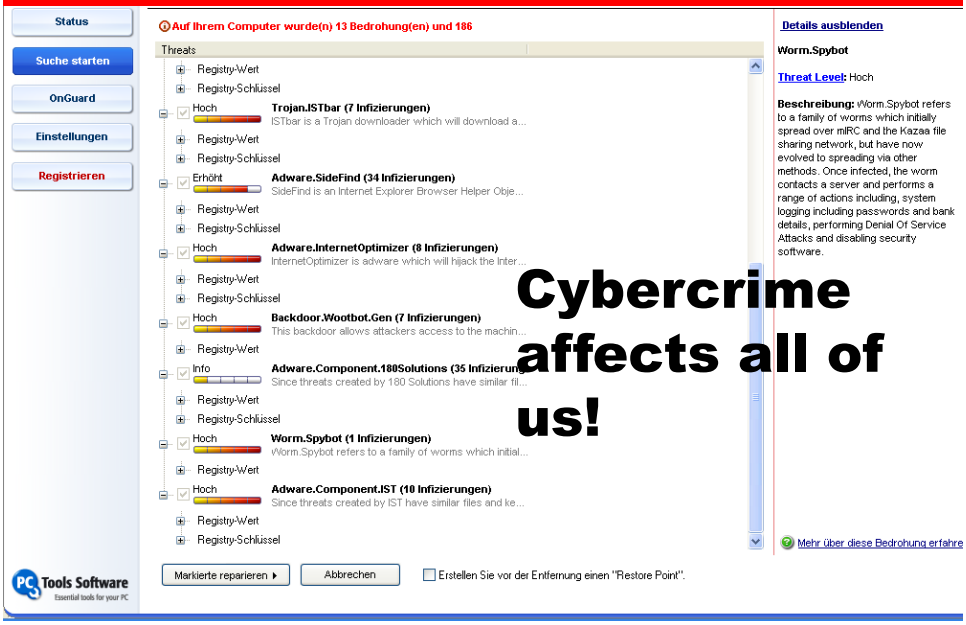
Chapter III: International cooperation
- **Section 1 - General principles**
- **Section 2 - Specific provisions**

Chapter IV: Final provisions

5

5

2 Cybercrime: why take action?



6

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
- Child pornography and sexual exploitation on the internet increasingly commercial
- Offenders increasingly organising for crime aimed at generating illicit profits
- Offences related to identity theft
- Use of internet for terrorist purposes (attacks against infrastructure, logistics, recruitment, finances, propaganda)
- Botnets one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware)
- Growing risk of cyber-attacks against critical infrastructure

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

7

7

3 The criminal law response

- Criminalise certain conduct ▶ substantive criminal law
- Give law enforcement/criminal justice the means to investigate, prosecute and adjudicate cybercrimes (immediate actions, electronic evidence) ▶ criminal procedure law
- Allow for efficient international cooperation ▶ harmonise legislation, make provisions and establish institutions for police and judicial cooperation, conclude or join agreements

8

8

A. Criminalising conduct

Legislation to deal with – as a minimum:

- **Illegal access to a computer system** (“hacking”, circumventing password protection, key-logging, exploiting software loopholes etc)
- **Illegal interception** (violating privacy of data communication)
- **Data interference** (malicious codes, viruses, trojan horses etc)
- **System interference** (hindering the lawful use of computer systems)
- **Misuse of devices** (tools to commit cyber-offences)
- **Computer-related forgery** (similar to forgery of tangible documents)
- **Computer-related fraud** (similar to real life fraud)
- **Child pornography**
- **Infringement of copyright and related rights**

Criminalising specific techniques/technologies or conduct?

9

9

How to criminalise conduct? See Convention on Cybercrime …

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)**

10

B. Legal conditions for efficient investigations

Procedural law to provide for – as a minimum:

- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data
- Procedural safeguards

11

11

How to provide for procedural law provisions? See Convention on Cybercrime …

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!

12

C. Conditions for efficient international cooperation

- Harmonise legislation between countries
- Create legal basis for judicial cooperation
- Direct, immediate police cooperation
- Immediate measures based on requests from other countries
- Join international agreements

13

Harmonising legislation: use Convention on Cybercrime as a guideline

Guideline or 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	?

14

The Convention on Cybercrime as a legal basis for international cooperation

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

15

The Convention on Cybercrime as a legal basis for 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

16

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. After positive vote, the country will be invited to accede
4. The country is then free to decide when to accede, that is, when to deposit the instrument of accession

17

4 Implementation – current status

- The Convention entered into force in July 2004
- 23 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, 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

18

5 Issues (1)

How does the Convention cover attacks against critical information infrastructure or "cyber-terrrorism"?

- **Cyberattacks covered by Art 4 (data interference) and Art 5 (system interference) of the Convention on Cybercrime**
- **Investigative tools and international cooperation provisions of the Convention can also be applied against cyberterrorism**

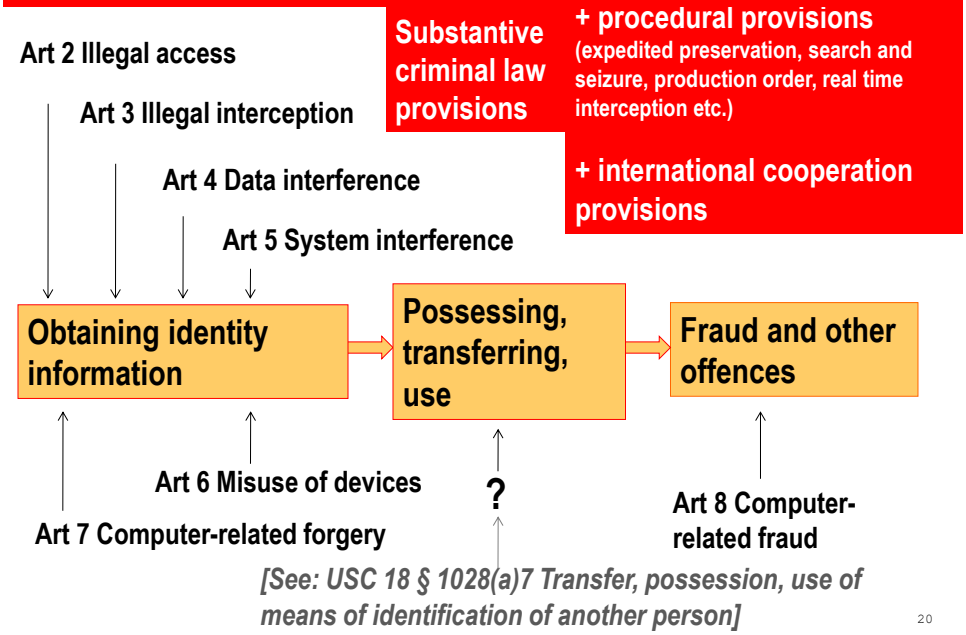
Convention for the Prevention of Terrorism for:

- 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

19

19

Issues (2): does the Convention cover phishing / identity theft?



20

20

Issues (3)

Efficiency of investigating cybercrime/ data retention/ authentification etc

What

Balance?

Privacy/ protection of personal data/ freedom of expression

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

21

Issues (4)

Law enforcement

What

relationship?

Service providers

22

Issues (4): Law enforcement – ISP cooperation

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime

Adopted at the global Conference on Cooperation against Cybercrime (Council of Europe, Strasbourg, 1-2 April 2008:

- **Common measures (including protection of rights and freedoms)**
- **Measures to be taken by law enforcement**
- **Measures to be taken by service providers**

23

23

6 The way ahead

- **Countries should review their legislation against the provisions of the Convention**
- **If necessary take steps to strengthen legislation**
- **Consider accession to the Convention as a framework for international cooperation**
- **Council of Europe ready to provide support: legislative analysis, workshops on cybercrime legislation**
- **OAS/CoE Cybercrime legislation workshop for Latin American countries, Bogota, 3-5 September 2008**
- **Global Conference on Cooperation against Cybercrime, Strasbourg, 10-11 March 2009**

24

24

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Thank you.

Alexander.seger@coe.int

25