



The Convention on Cybercrime

Workshop on cybercrime legislation and training of judges (Plovdiv, Bulgaria, 17-18 December 2007)

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

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

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

2

The legislative response to cybercrime

- 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

3

Substantive law

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**
- **Child pornography**
- **Hate speech, xenophobia and racism**
- **Infringement of copyright and related rights**

Criminalising specific techniques/technologies or a certain conduct?

Procedural law

Legislation 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

5

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

6

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

7

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)**

8

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!

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

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

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

Implementation – current status

- The Convention entered into force in July 2004
- 21 ratifications + 22 signatures (as of 31 October 2007)
- Signed by Canada, Japan, South Africa, ratified by USA
- Costa Rica and Mexico have been invited to accede
- Legislative amendments and ratification process underway in many other countries

4

The Convention as a guideline for national legislation (“model law”)

The Convention serves as a guideline for the development of national cybercrime legislation

- Coherent approach to national legislation that helps protect society from cybercrime challenges
- Helps create a basis for public-private cooperation
- Harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries
- Procedural measures for more efficient investigations
- Tools for the gathering of electronic evidence, including tools for the investigation of cyberlaundering, cyberterrorism and other serious crime

The Convention as a guideline for legislation

“Model law” function of the Convention

- Use as a checklist
- Compare provisions
- Use wording
- Basis for analysis

See country profiles on
cybercrime legislation

- [Romania](#)
- [Bulgaria](#)
- [Macedonia](#)
- [Serbia](#)

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	?
-------------------------	---

15

Thank you.

Alexander.seger@coe.int