

The Convention on Cybercrime: A framework for legislation and international cooperation for countries in Asia and Pacific

ASEAN POL - Singapore (April 2008)

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

1

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

2

2 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

3

3

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 (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

5

5

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)

6

6

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!

7

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

8

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**

9

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**

10

10

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 underway in many other countries (Argentina, Brazil, Colombia, Egypt, India, Nigeria, Philippines etc.) and accession to the Convention under consideration

= Convention provides a global standard

11

4

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

12

12

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	?

13

13

5

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

14

14

- Coherent national approach to legislation on cybercrime
- Facilitates the gathering of electronic evidence
- Facilitates the investigation of cyberlaundering, cyberterrorism and other serious crime
- Harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries
- Legal and institutional basis for international law enforcement and judicial cooperation with other parties to the Convention
- Participation in the Consultations of the Parties
- The treaty as a platform facilitating public-private cooperation

15

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

16

7 Issues (1)

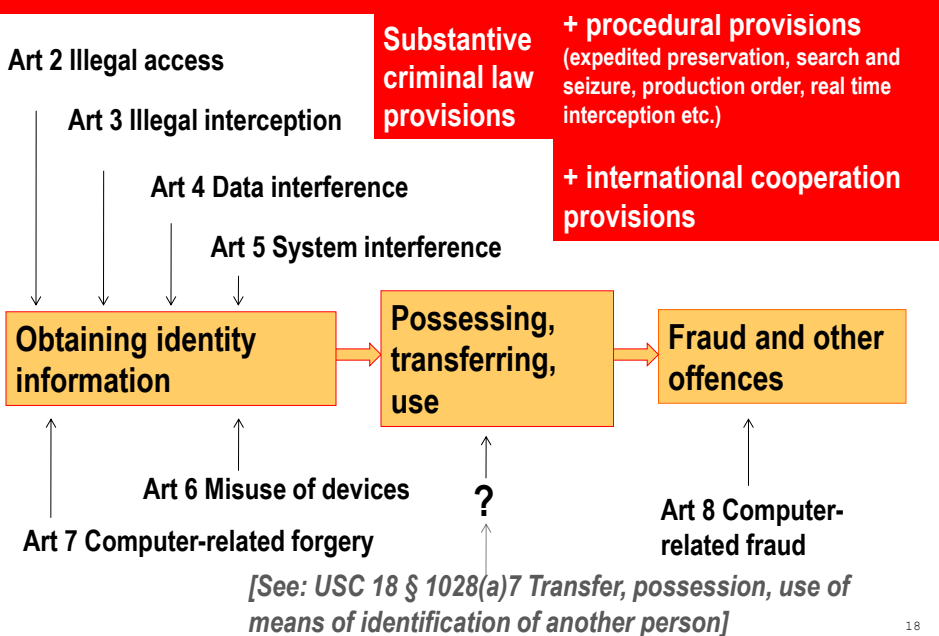
How does the Convention cover attacks against critical information infrastructure or cyber-terrorism?

- 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

17

17

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



18

18

Issues (3)

Efficiency of investigating cybercrime/
data retention/
authentication etc

What

Balance?

Privacy/
protection of
personal data/
freedom of expression

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

19

19

Issues (4)

Law enforcement

What

relationship?

Service providers

20

20

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**

21

21

8 The way ahead

- **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**

22

22



www.coe.int/cybercrime

Thank you.

Alexander.seger@coe.int