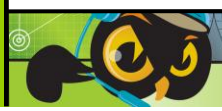
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Efficient cooperation against cybercrime

Alexander Seger
Council of Europe

alexander.seger@coe.int



CeCOS II 東京
TOKYO May 26 & 27, 2008

APWG ANTIPHISHING JAPAN フィッシング対策協議会

1

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

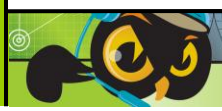
democracy
rule of law
human rights

in order to promote

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Measures against economic and organised crime

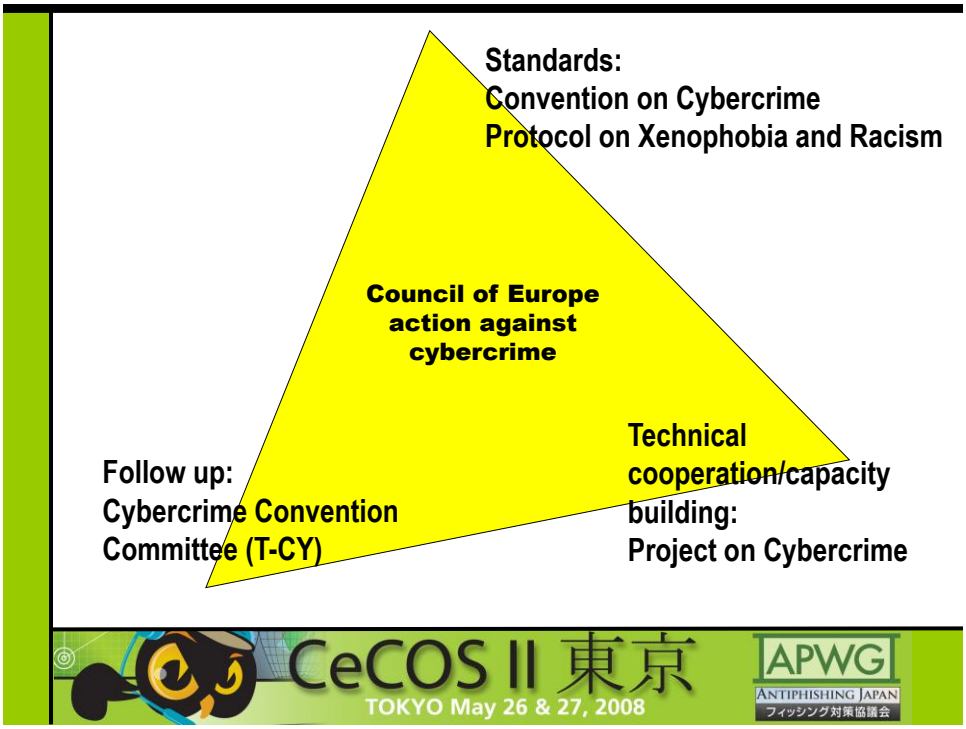
Established in 1949
Currently 47 member States



CeCOS II 東京
TOKYO May 26 & 27, 2008

APWG ANTIPHISHING JAPAN フィッシング対策協議会

2



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

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

2 Building a consistent legal basis against cybercrime

Measures against cybercrime must be based on law:

- 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

6

3 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**
- **Child pornography**
- **Hate speech, xenophobia and racism**
- **Infringement of copyright and related rights**

Criminalising specific techniques/technologies or a certain conduct?

7

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)**

8

Does the Convention cover phishing / identity theft?

Substantive criminal law provisions

+ procedural provisions (expedited preservation, search and seizure, production order, real time interception etc.)

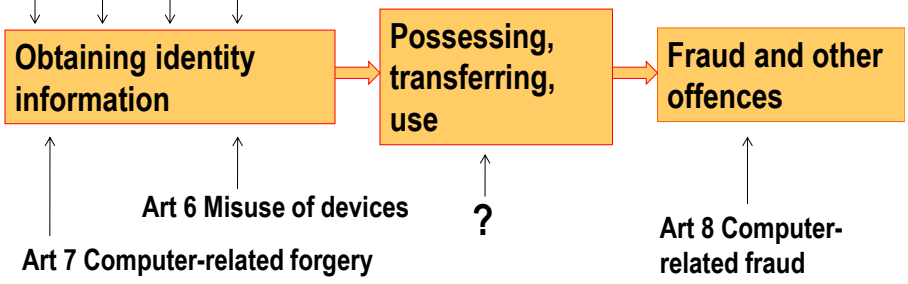
+ international cooperation provisions

Art 2 Illegal access

Art 3 Illegal interception

Art 4 Data interference

Art 5 System interference



Art 6 Misuse of devices

?

Art 7 Computer-related forgery

Art 8 Computer-related fraud

9

4 Legal conditions for efficient investigations

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 (privacy, protection of personal data, freedom of expression, due process etc.)

10

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!

11

5 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

12

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	?

13

The Convention on Cybercrime as a legal basis for international cooperation:

Parties to the Convention agree to cooperate with each other to the widest extent possible

14

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

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

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. 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

17

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

= Need more parties to make international cooperation work

18

6 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**

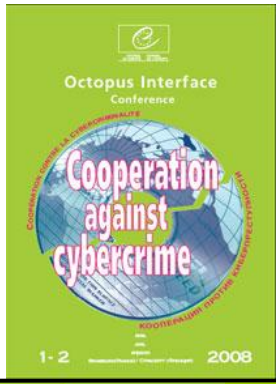
19

7 Follow the money

20

8 Conclusion: Interface!

Pragmatic, responsive, pro-active cooperation at all levels!



CeCOS II 東京
TOKYO May 26 & 27, 2008
APWG
ANTIPHISHING JAPAN
フィッシング対策協議会

21

Thank you.

Alexander.seger@coe.int

CeCOS II 東京
TOKYO May 26 & 27, 2008
APWG
ANTIPHISHING JAPAN
フィッシング対策協議会

22