Microsoft Symposium
Online Security and the Safety of South Africa's Citizens
Bryanston, Johannesburg, South Africa
20 April 2007

The Convention on Cybercrime of the Council of Europe

A framework for national action and international cooperation against cybercrime

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

1

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

Strategy against economic crime
THE RATIONALE

democracy
rule of law
human rights

in order to promote

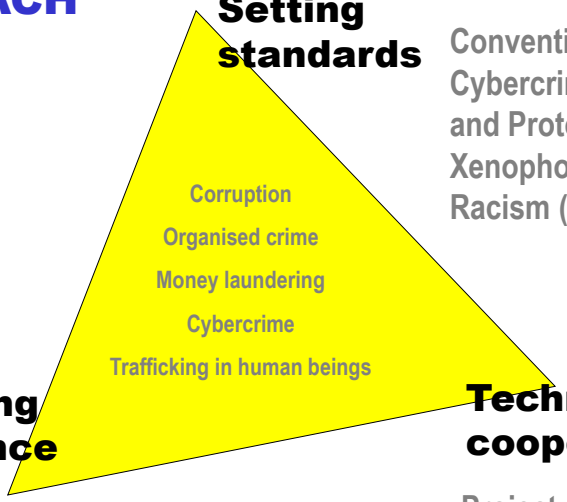
Measures against economic and organised crime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Established in 1949
Currently 46 member States

2

APPROACH



Convention on Cybercrime (ETS 185) and Protocol on Xenophobia and Racism (ETS 189)

Cybercrime Convention Committee (T-CY)

Project on cybercrime
Funded by the Council of Europe and Microsoft

3

2 Why take action against cybercrime?

- Measurable increase in cybercrimes (phishing, botnets etc)
- More cybercrimes for economic gain
- Increase in hate, racism, violence websites
- Software piracy
- Child pornography
- More organising for cybercrime
- Cyberlaundering
- Cyberterrorism
- Cybercrime: low risk and many opportunities

= Societies around the world highly dependent on ICT and thus highly vulnerable

In 2007, 1 billion+ Internet users worldwide. Even if 99.9% were legitimate, this would leave 1 million potential offenders

Need to balance fundamental rights and freedoms and concerns for security

4

Child pornography on the internet

- Increasing reporting on child pornography on the internet
- Increasing number of commercial sites
- Problem: legislative gaps in many countries
- Child porn sites hosted in many different countries (see www.iwf.org.uk)

- Important successes in law enforcement operations
- Law enforcement priority in many European countries
- Public-private cooperation (by ISPs, example CETS)
- Opportunities for enhanced international cooperation (Convention on Cybercrime)

Note:

New Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

(Council of Europe - to be adopted in autumn 2007)

Provisions dealing with:
- Preventive and protective measures
- Substantive criminal law
- Investigation, prosecution and procedural law, including child-friendly procedures
- Treatment of sex offenders
- National data base and exchange of information
- International cooperation

Parties are to criminalise:
- Sexual abuse of a child
- Child prostitution
- Child pornography
- Participation of a child in pornographic performances
- Solicitation of children for sexual purposes

3 The legislative response to cybercrime

- Criminalise certain behaviour → 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

Defining key terms

in legislation:

- "Computer system"
- "Computer data"
- "Service provider"
- "Traffic data"

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 behaviour?

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**

International cooperation

Legislation to provide for:

- **Full international cooperation**
- **Compatibility with legislation of other countries**
- **Authorities for MLA and extradition**
- **National procedural measures to be applied in international cooperation**
- **24/7 points of contact**
- **Ratification of the Convention on Cybercrime and its Protocol on Xenophobia and Racism**

4

Council of Europe

Convention on Cybercrime (ETS 185)

+

Additional Protocol on racism and xenophobia committed through computer systems (ETS 189)

Structure of the Convention

Chapter I: Definitions
(what is a computer system, computer data, service provider, traffic data)

Chapter II: Measures at national level
Section 1 - Substantive criminal law
(behaviour that is to be made a criminal offences)
Section 2 - Procedural law
(measures for more effective investigations of cybercrimes)
Section 3 - Jurisdiction

Chapter III: International cooperation
Section 1 - General principles of cooperation
Section 2 - Specific provisions for more effective cooperation

Chapter IV: Final provisions (including accession by non-member states)

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)

Article 9 of the Convention: child pornography

1 Establish as criminal offences when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

Article 9 of the Convention: child pornography

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

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)

Section 3 – Jurisdiction

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, including South Africa)

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

Protocol on racism and xenophobia committed through computer systems (ETS 189)

Art 3 – Dissemination of racist and xenophobic material through computer systems

Art 4 – Racist and xenophobic motivated threat

Art 5 – Racist and xenophobic motivated insult

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

5 Monitoring of the treaty

Art 46 Consultation of the Parties (Cybercrime Convention Committee, T-CY)

- Facilitate effective implementation of the treaty and identify problems
- Facilitate information exchange
- Consider possible amendments or supplements to the treaty

Next meeting of the T-CY in Strasbourg on 13-14 June 2007

6 Benefits of the Convention:

- 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

7 Implementation – current status

Convention on Cybercrime (ETS185)

- Entered into force in July 2004
- 19 ratifications + 25 signatures (as of March 2007)
- Legislative amendments and ratification process underway in many other countries
- The Convention is becoming a global instrument:
  - signed by Canada, Japan, South Africa, ratified by USA
  - accession of non-European countries: Costa Rica and Mexico have been invited. Discussions with other countries

Protocol on Xenophobia and Racism (ETS 189)

- 6 ratifications + 24 signatures
- Entered into force on 1 March 2006

Coming up

Octopus Interface Conference

Cooperation against Cybercrime

(11-12 June 2007, Strasbourg, France):

- Implementation of the Convention and its Protocol – Update
- Cybercrime: situation analysis and identification of new threats
- Initiatives of other organisations and stakeholders
- Effectiveness of cybercrime legislation
- Public-private partnerships
- International cooperation and the functioning of 24/7 points of contact

(see www.coe.int/economiccrime for further information and registration)

This will be followed by the Cybercrime Convention Committee on 13-14 June

8 Conclusions

- South Africa signed the Convention on Cybercrime in 2001
- Early ratification of the Convention and its Protocol would be beneficial to South Africa and set an example for other African countries
- The Council of Europe is prepared to cooperate with South Africa in cybercrime matters (strengthening of legislation, training, international cooperation) and related matters (judicial cooperation, data protection and privacy, child exploitation)

Thank you for your attention.

alexander.seger@coe.int
+33-3-9021-4506
www.coe.int/economiccrime