Microsoft ILEA
LE and Prosecutor
Cybercrime Training
Bangkok, June 2006

A global response to a global challenge:

the Convention on Cybercrime of the Council of Europe

... and why countries of Asia and the Pacific should accede to it

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

1

Purpose of this presentation

To encourage countries of Asia and the Pacific to enact legislation in line with the Convention on Cybercrime and consider accession of their countries to this treaty

2

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

3

APPROACH

Setting standards

For example:
Convention on Cybercrime (ETS 185)

- Corruption
- Organised crime
- Money laundering
- Cybercrime
- Trafficking in human beings

Monitoring compliance

Consultations of the parties to ETS 185

Technical cooperation

Provide support through a global project on cybercrime?

4

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 organised cybercrime
- Cyberlaundering
- Cyberterrorism
- Cybercrime: low risk and many opportunities

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

In 2006, 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

5

3

Council of Europe

Convention on Cybercrime (ETS 185)

+

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

6

Structure 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

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)

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

9

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

10

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

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

4 Implementation – current status

Convention on Cybercrime (ETS185)

- Entered into force in July 2004
- 14 ratifications + 28 signatures (as of 15 June 2006)
- Signed also by Canada, Japan, South Africa and USA

Protocol on Xenophobia and Racism (ETS 189)

- 6 ratifications + 24 signatures (including Canada)
- Entered into force on 1 March 2006

Example Romania

- Signed Convention in 2001
- Analysed the existing legislation
- Drafted law 161/2003 on transparency and the prevention and control of corruption, including Title III on preventing and fighting cybercrime
- Substantive, procedural and international cooperation provisions
- Text of the Convention as basis
- Additional laws on pornography, and copyright and related rights.
- Reviewed by Council of Europe in March 2004
- Ratified Convention in May 2004
- Competent Romanian authority: Service for Combating Cybercrime established at the Prosecutor's Office of the High Court of Cassation

Problems encountered:

- Many investigations, prosecutions but few verdicts
- Reasons: summoning of foreign witnesses, lack of training of police, prosecutors, judges (in particular those of first instance)

Example France

- Signed 2001
- Ratified 2006
- Law 2004-575 of 21 June 2004 on confidence in the digital economy
- Title III on Security in the digital economy with Chapter II on the Fight against cybercrime
- Amends Criminal and Criminal Procedure Codes

Lessons re drafting of legislation

- Stick to treaty, Convention as model

Effectiveness of Convention so far

- To be reviewed by the Cybercrime Convention Committee (T-CY)

5 Monitoring of the treaty

The Cybercrime Convention Committee (T-CY)
– First Consultation of the Parties (to Art 46)
in Strasbourg, France, 20-21 March 2006:

- Effectiveness of Convention
- Role of law enforcement officials
- Cooperation of law enforcement and private sector
- Operation of the 24/7 network
- Extension or amendment of the Convention

www.coe.int/economiccrime

6 Accession to the Convention – Benefits for Asia/Pacific countries

- Coherent national approach to legislation on cybercrime
- Tools for the gathering of electronic evidence
- Tools for 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

APEC recommended that its 21 members take into account the Cybercrime convention when enacting legislation

The Organisation of American States

- Recommended that its member States consider the possibility of acceding to the Convention on Cybercrime (at the 5th Conference of Ministers of Justice and Attorneys General of the OAS, Washington DC, April 2004)
- Confirmed this position again in Madrid, December 2005, at a conference co-organised by the Council of Europe, the OAS and the Ministry of Justice of Spain
- And again at Meeting of OAS Group of Governmental Experts on Cyberbrime, Washington, 27-28 Feb 2006

Canada and the USA

- Signed the Convention in November 2001

Support has been expressed.

Need to move towards implementation

- Draft, review and adopt legislation to implement the principles and provisions of the Convention into national law
- Take practical steps towards accession to the Convention

7 Technical cooperation

- Reviewing/drafting of legislation
- Training of all institutions of the criminal justice chain
- Partnerships, networking and exchange of experience

Lessons learned:

- 12 from 14 countries that ratified the Convention so far had received prior Council of Europe support
- PPP also in technical cooperation
- Need for consistent assistance (coordination/consultations)

The Council of Europe is prepared to assist countries of Asia and the Pacific through a TC project and work with a consortium of partners

Conclusions

- Cybercrime Convention recognised as global framework for national action and international cooperation
- Convention as basis for PPP
- Support has been expressed
- Need to move towards implementation (accession)
- Council of Europe and other partners are ready to provide support

There are many good arguments for implementing the Convention and its Protocol!

Thank you for your attention.

alexander.seger@coe.int
www.coe.int/economiccrime