International Conference on
Cybercrimes and Electronic Evidence
Câmara dos Deputados
Conselho de Altos Estudos e Avaliaçâo Tecnologica
Brasilia, 28 May 2008

The Budapest Convention on Cybercrime

A framework for national action and international cooperation against cybercrime

Jean-Charles de Cordes
Council of Europe
Strasbourg (France)
Tel +33-3-9021-5305
jean-charles.decordes@coe.int
www.coe.int/cybercrime

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

Strategy against economic crime
THE RATIONALE

democracy
rule of law
human rights

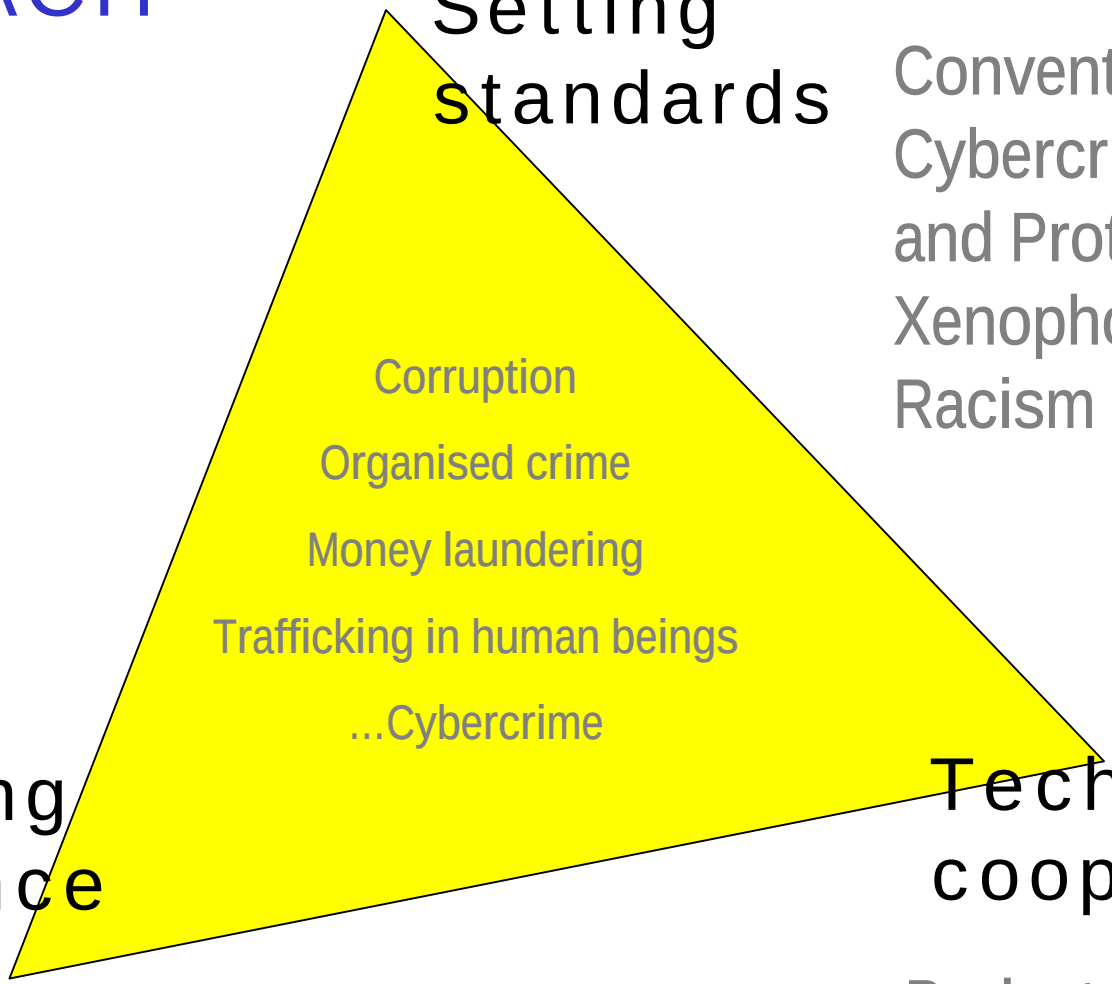
in order to promote

Measures against economic and organised crime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Established in 1949
Currently 47 member States

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, Microsoft, Estonia…

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

Note:

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

(adopted by CM of the Council of Europe on 13 July 2007 - opened to signature since October 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

Council of Europe

Budapest Convention on Cybercrime (ETS 185)

+

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

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 (less than 4 years!)
- Only international instrument containing a full set of provisions re. fight against cybercrime

The Protocol on Xenophobia and Racism Committed through Computer Systems

- Opened for signature in January 2003
- In force since March 2006

Structure and content 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)

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 III - International cooperation...

Article 35 – 24/7 Network

Each Party shall designate a point of contact available on a 24 hour, 7-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;
b the preservation of data pursuant to Articles 29 and 30;
c the collection of evidence, the provision of legal information, and locating of suspects

Chapter III - International cooperation...

Article 35 cont'd

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter III - International cooperation...

Article 35 cont'd

Article 35 is based on the experience of the G8 network of contact points

? Close cooperation between the Council of Europe and the G8 High-Tech Crime Subgroup to maintain a joint directory of contact points

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 (flexibility for governments and parliaments!)

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 Monitoring of the treaty

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

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

Last meeting of the T-CY held on 3-4 April 2008

5 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 crimes
- 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 Convention as a platform facilitating public-private cooperation

6 Implementation – current status

Convention on Cybercrime (ETS185)

- 44 signatures - 22 ratifications (as of 27 May 2008)
- Missing in Europe: Andorra, Azerbaijan, Liechtenstein, Monaco, Russia, San Marino, Turkey
- Legislative amendments and ratification process underway in many countries around the world ? 2008 to be decisive
- The Convention is a global instrument:
  - ✓signed by Canada, Japan, South Africa, ratified by USA
  - ✓accession of non-European countries: Costa Rica, Mexico and The Philippines have been invited / Domenican Republic requested to accede
  - ✓model law for many States such as: Argentina, Mexico, Costa Rica, Russia, India, Indonesia, Pakistan, Egypt, Nigeria, Morocco, …
  - ✓positive talks with Australia and discussions with many others worldwide
  - ? **global trend – keep the momentum!**

6 Implementation – current status

Protocol on Xenophobia and Racism (ETS 189)

- 33 signatures - 12 ratifications (as of 27 May 2008)
- Entered into force on 1 March 2006

***

The Convention as "soft law"

- Apart from legal standards "soft laws" like recommendations can help to harmonise procedures and set standards
- April 2008 (Octopus Conference) = Adoption of Guidelines for the Cooperation between law enforcement and ISP in investigation of cybercrime (working group involved experts/practitioners from ISP, IT-industry, law enforcement)
- Objective: good practices to help structure such cooperation and applicable in any country

7 Conclusions

- Cybercrime Convention serves globally as guideline for national action and as a framework for international cooperation
- Added value for Brazil
- Flexible approach
- Council of Europe ready to assist in the further strengthening of cybercrime legislation and investigations in Brazil to further support its accession to the Convention!

Thank you for
your attention!

jean-charles.decordes@coe.int
+33-3-9021-5305
www.coe.int/cybercrime