National Cybercrime Conference
Pitesti, Romania
27-29 November 2006

The Convention on Cybercrime of the Council of Europe

Implementing the Convention: what are the issues?

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

1

Abstract

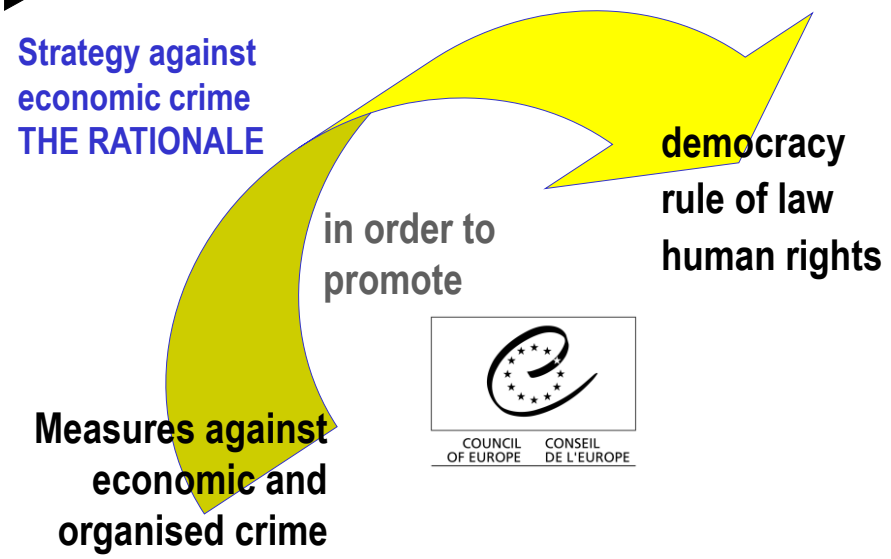
The Convention on Cybercrime provides a framework for national and international action to meet the challenge of cybercrime

The number of countries which are parties to the Convention is increasing

The focus should now shift to the actual implementation of the Convention: What has been the experience of Romania?

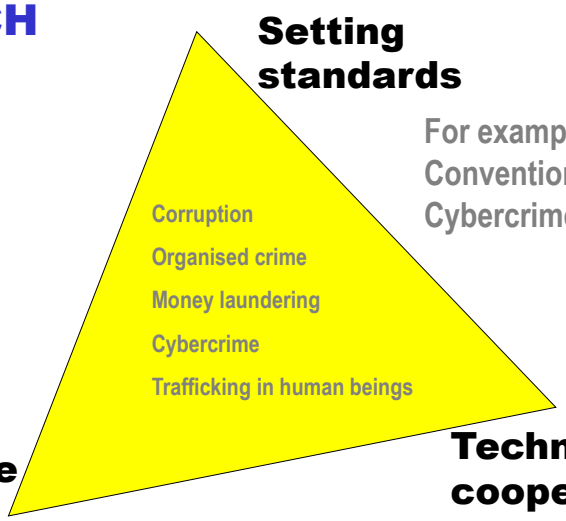
2

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



3

APPROACH



Consultations of the parties to ETS 185 (T-CY)

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

3

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

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

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)

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 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 in June 2007 [TBC]

5 Benefits of the Convention:

- 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

6 Technical cooperation

Council of Europe - Project against cybercrime
(started in September 2006)

Objective:
To promote broad implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189)

Expected results:
1. Draft laws permitting ratification of/accession to ETS 185 and 189 available in at least 10 European and 5 non-European countries
2. Capacities of criminal justice systems strengthened to investigate, prosecute and adjudicate cybercrime
3. Capacities of criminal justice bodies to cooperate internationally re-enforced

Funded by the Council of Europe and Microsoft

7 Implementation – current status

Convention on Cybercrime (ETS185)

- Entered into force in July 2004
- 18 ratifications + 26 signatures (as of 26 November 2006)
- Signed also by Canada, Japan, South Africa and USA
- Legislative amendments and ratification process underway in many other countries

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)

Implementation of the Convention:

- Legislative framework (substantive and procedural law)
- Investigative tools (expedited preservation, gathering of electronic evidence etc.)
- Institution building (capacities of police, prosecutors, judges, creation of specialised units)
- International cooperation
  - expedited preservation of data
  - judicial cooperation
  - 24/7 contact points

Strengths

weaknesses

problems encountered

solutions

good practices

8 Conclusions

- Cybercrime Convention as a global framework for national action and international cooperation
- Need to enlarge number of parties to the Convention (ratifications and accessions)
- Need to ensure implementation and share experience and good practices

T-CY 2007 + Conference: Implementing the Convention on Cybercrime [TBC]

Thank you for your attention.

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