COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

The Convention on Cybercrime

What benefits for Brazil?

Workshop for Prosecutors
Sao Paulo, September 2007

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

1

I Why take measures against cybercrime?

Cybercrime situation analysis and identification of new threats:

1. Dependency of societies on information and communication technologies. This dependency makes societies highly vulnerable to cybercrimes
2. Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading. Used for:
   - Denial of service attacks
   - Identity theft (phishing and other social engineering techniques)
   - Fraud, money laundering and other economic crimes
3. Spam nuisance and carriers of malware

Council of Europe

Sao Paulo September 2007 2

2

4. Child pornography and sexual exploitation on the internet increasingly commercial
5. Offenders increasingly organising for crime aimed at generating illicit profits
6. Botnets one of the central tools of criminal entreprises (DDOS, extortion, placing of adware and spyware). Underground service economy developing (botnets for rent)
7. Shift in the threat landscape: from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes

New challenges

8. Growing risk of cyber-attacks against critical infrastructure
9. Remote storage of data (problem for investigators)
10. Next-generation-networks (NGN), including VoIP (problem for investigators)

Put cybercrime in context:

- In 2007, 1 billion+ Internet users worldwide. Probably 99.9% use ICT for legitimate purposes
- Need to balance concerns for security and fundamental rights and freedoms

II 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

Council of Europe

III 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

Council of Europe

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

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)

Chapter II – Measures at national level

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)

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
- Art 6 Denial, gross minimisation, approval or justification of genocide or crimes against humanity

Implementation – current status

- The Convention entered into force in July 2004
- 21 ratifications + 22 signatures (as of 31 August 2007)
- Signed by Canada, Japan, South Africa, ratified by USA
- Costa Rica and Mexico have been invited to accede
- Legislative amendments and ratification process underway in many other countries

IV Issues (1)

Does the Convention provide a global framework?

Need for a global harmonisation/compatibility of
- substantive criminal law
- procedural law
- Efficient international cooperation

- The Convention on Cybercrime provides such a framework
- Open for accession to third countries
- Currently used as a guideline for legislation around the world

Issues (2)

Does the Convention cover cyberterrorism?

Terrorist may use information and communication technologies for:

- Attacks via the internet aimed at essential electronic communication systems, IT infrastructue and other systems and infrastructure
- Dissemination of illegal contents, including threats, inciting, advertising, fundraising, recruitment, dissemination of racists and xenophobic material
- Logistical purposes, including communication, target analysis, acquisition of information

Issues (2)

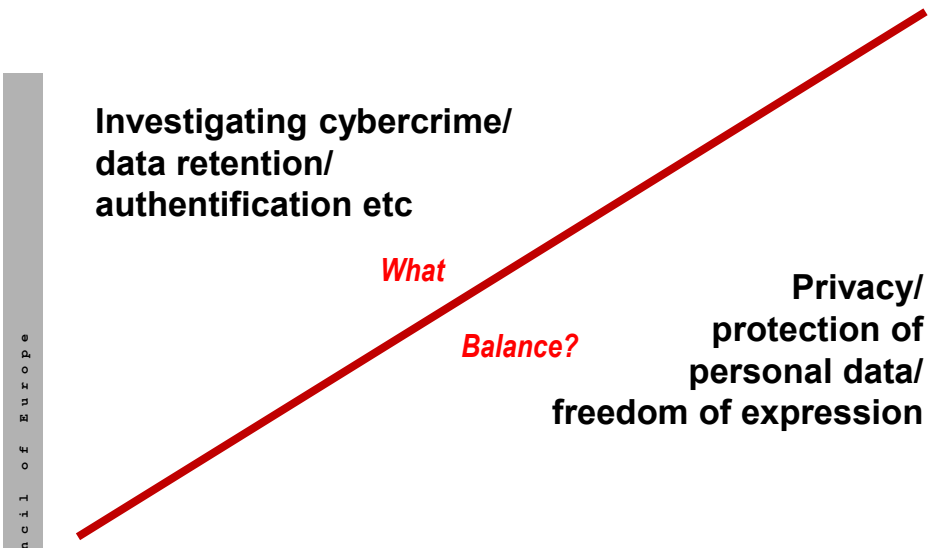
Does the Convention cover cyberterrorism?

Or are new instruments required?

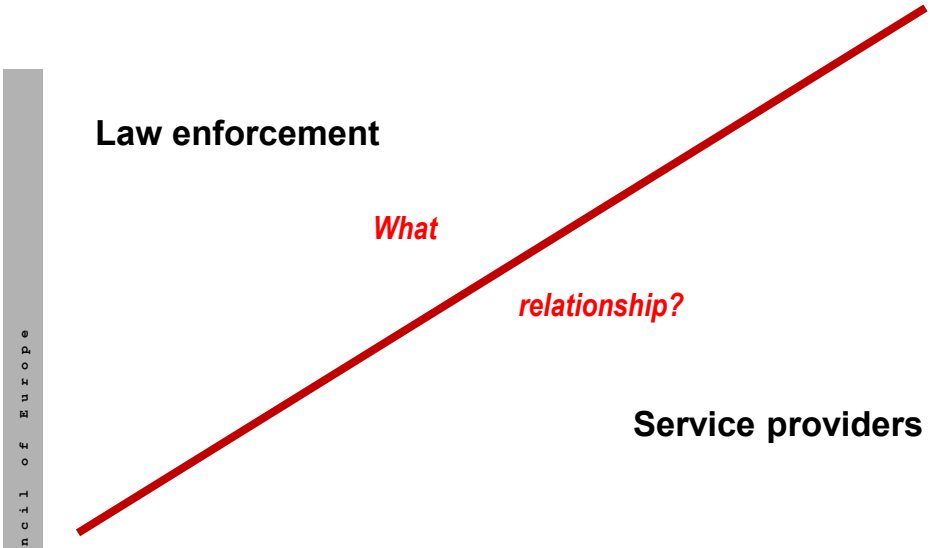
(question under discussion at the CoE's Committee on Terrorism, CODEXTER)

- **Cyberattacks covered by Art 4 (data interference) and Art 5 (system interference) of the Convention on Cybercrime**
- **Investigative tools and international cooperation provisions of the Convention can also be applied against cyberterrorism**
- **Recruitment, incitement etc covered by the Convention for the Prevention of Terrorism (CoE)**
- **Most other issues covered by other existing Conventions.**

Issues (3)



Issues (4)



Council of Europe

Sao Paulo September 2007 19

19

V The Convention and Brazil: what benefits

- The Convention serves as a guideline for the development of national cybercrime legislation
  - Coherent approach to national legislation
  - Harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries
  - Procedural measures for more efficient investigations

- Tools for the gathering of electronic evidence, including tools for the investigation of cyberlaundering, cyberterrorism and other serious crime
  - Through the Convention these tools can also be applied in international cooperation

Council of Europe

Sao Paulo September 2007 20

20

Benefits...

- Chapter 3 of the Convention provides the legal and institutional basis for international law enforcement and judicial cooperation with other parties to the Convention
- Participation in the Consultations of the Parties (Cybercrime Convention Committee, T-CY) = participation in future work on the Convention

VI Conclusion

- Measures against cybercrime require legal basis in substantive and procedural criminal law
- Balance between security concerns and civil liberties to be discussed in each society
- Investigative powers, safeguards and limits to be clearly defined
- Guidelines for relation between law enforcement and service providers to be developed
- Use Convention on Cybercrime as a guideline for the development of national legislation and a framework for international cooperation (consider accession)

Thank you.

Alexander.seger@coe.int

Council of Europe