1

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

2

1 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)

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

Article 35 – 24/7 Network

Each Party shall designate a point of contact available on a twenty-four hour, seven-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.

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.

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

- **Close cooperation between the Council of Europe and the G8**

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

2 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

3 Monitoring and support

- The Convention is followed by the Cybercrime Convention Committee (T-CY)
- The Council of Europe – through the Project on Cybercrime – provides support to countries around the world in the strengthening of legislation
- The Council of Europe is closing cooperating with other international organisations, national authorities and the private sector

4 The Convention as a framework for international cooperation

The Convention serves as a guideline for the development of national cybercrime legislation

- Harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries

Tools for the gathering of electronic evidence

Tools for the investigation of cyberlaundering, cyberterrorism and other serious crime

- Through the Convention these tools can also be applied in international cooperation

The Convention as a framework for international cooperation cont'd

- Chapter 3 of the Convention provides the legal basis for international law enforcement and judicial cooperation with other parties to the Convention
- Requires Parties to establish 24/7 points of contact
- The Convention is open for accession to any country
- Participation in the Consultations of the Parties (Cybercrime Convention Committee, T-CY) = participation in future work on the Convention

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Conclusion:
There are many good arguments for implementing the Convention!

Thank you for your attention.

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