Taming the World Wild Web

Council of Europe's Convention on Cybercrime : a pioneering attempt towards a global response to the challenge posed by cybercriminality

WSIS, 2nd PREPCON, Round Table 6
Geneva, 19 February 2003

Manuel LEZERTUA
Head of Economic Crime Division
Directorate General of Legal Affairs
Council of Europe, Strasbourg

Challenges : global networks and global crimes

- A world increasingly dependent on computer networks : higher vulnerability to criminal misuse
- Computer networks deserve and need protection :

  - global information society : virtually no frontiers neither for lawful use or criminal misuse of computer networks

  - information virtually accessible anywhere at any time : remote access, legal or illegal, to vast quantities of data stored by computer systems is unhindered

  - promise of a new era of online e-commerce, offering services and goods for hundreds of bilions €

Difficulties to combat computer crime

- Internet borderless for ciminals, but law enforcement confined by national sovereignety
- Discrepancies in legal systems : a major obstacle for mutual legal assistance f.i. failure to criminalise computer-related offences

Law enforcement tools

- Harmonisation of the laws defining criminal behaviour is essential, but not enough
- Enforcement requires appropriate tools for detecting and investigating
- New mutual assistance regimes for investigating and prosecuting cybercrime
- New avenues and methods for co-operation between multiple countries and intergovernmental emergency networks

Reaction by Governments

- No reaction or late and limited reaction
- Too slow to adapt legal categories to the virtual world
- Lack of harmonisation as regards the definition of the offences and procedural means to combat them
- Insufficient lack of international co-operation against a criminal fenomenon which is international in nature

Council of Europe's Convention on Cybercrime

- A pioneering attempt towards a global response to the challenge posed by cybercriminality

Council of Europe's Convention on Cybercrime

Aims

- It sets the basis for a harmonised criminalisation of dangerous criminal acts committed against or through computer networks.
- It determines the criminal law consequences that should derive from those acts.

- It regulates the means of detection, investigation and gathering of evidence that could be legitimately used in criminal cases occurring in the cyber-espace, ensuring full respect for human rights and constitutional standards.
- It provides for enhanced means for international co-operation against cyber-offenders, in particular by setting up a network of 24/7 –24h a day, 7 days a week- able to provide assistance to the authorities of any contracting party in charge of investigating a case of cibercriminality.

Convention on Cybercrime
Structure

- Chapter I – Use of terms
- Chapter II – Measures to be taken at domestic level
  - *i)* ***substantive law***: common definition of offences in the area of computer-related crime
  - *ii)* ***procedural law***: defines means of investigation and sets conditions and safeguards for the use of procedural powers
- Chapter III – International co-operation

  Chapter IV – Final clauses

Convention on Cybercrime
Criminal Offences

These offences fall into four categories :

- offences against the confidentiality and availability of data or computer systems
- computer-related offences
- content-related offences
- offences involving the infringement of intellectual property and related rights

Convention on Cybercrime

Offences against the confidentiality and availability of data or computer systems

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices

Convention on Cybercrime
Computer-related offences

Computer-versions of two old offences :

- **computer-related forgery**
- **computer-related fraud**

two specific kinds of manipulation of computer systems or computer data

Convention on Cybercrime

Content-related offences

Offences related to child pornography

- Strengthen children protection measures by modernising criminal law to more effectively circumscribe the use of computer systems in the commission of sexual offences against children
- Convention criminalises :

  - the production of child pornography for the purpose of distribution through a computer system.

  - the ‘offering’ of child pornography through a computer system

  - the distribution or transmission of child pornography through a computer system

  - obtaining child pornography, e.g. by downloading it

  - the possession of child pornography in a computer system or on a data carrier

Convention on Cybercrime

Offences related to infringements of copyright and related rights

- Infringements of intellectual property rights most commonly committed on the Internet : concern of copyright holders and computer networks professionals
- Convention criminalises wilful infringements of copyright and related rights when committed by means of a computer system on a commercial scale

  - the precise manner in which such infringements are defined under domestic law may vary from State to State

New protocol : new offences
Combating racism on the Net

- Aim : to complement the Convention, bringing new offences into its scope
- Definition of racist and xenophobic material : any written material, image or other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion
- Protocol criminalises dissemination through computer networks of :

  - racist and xenophobic material
  - racist and xenophobic motivated threats or insult
  - denial of, gross understatement of, approval or justification of genocide and crimes against humanity
- Opened for signature on 28 January 2003 : 12 signatures

Convention on Cybercrime
Procedural powers

- Procedural measures to be taken at the national level for the purpose of criminal investigation of the criminal offences committed by means of a computer system and the collection of evidence in electronic form
- New measures to ensure that traditional measures of collection of evidence (search and seizure), remain effective in volatile technological environment

Convention on Cybercrime
Procedural powers

- Traditional procedural measures adapted to new technological environment f.i. search and seizure
- Collection procedures relevant to telecommunications adapted f.i. real-time collection of traffic data, interception of content data
- Collection of data for the purpose of any specific criminal investigation
- Application of these powers subject to conditions and safeguards under domestic law

Convention on Cybercrime

Procedural powers

The Convention deals with the following powers :

1. **Expedited preservation of stored computer data**
   - expedited preservation of stored computer data
   - expedited preservation and partial disclosure of traffic data
2. **Production order**
3. **Search and seizure of stored computer data**
   - search of computer systems
   - seizure of stored computer data
4. **Real-time collection of computer data**
   - real-time collection of traffic data
   - interception of content data

Convention on Cybercrime

International co-operation

- Parties should provide “to the widest extent possible” : co-operation to each other, minimising impediments to the smooth and rapid flow of information and evidence internationally.
- In respect of all criminal offences related to computer systems and data, as well as to the collection of evidence in electronic form of a criminal offence
- In accordance with relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws
- An international computer-crime assistance network > **24/7 network** : a network of national contact points available on a permanent basis.

Convention on Cybercrime

Benefits

- Unique platform for common action against cyber-criminals
- Global deterrent effect of criminal law for potential cyber-criminals
- Re-assuring effect on users about the safety of the Net => wider use of e-commerce
- Reduce level of damage caused to society, business and individual users
- Reducing the level of impunity = promoting the rule of law in the Net

Convention on Cybercrime

Conclusions

- Computer crime will not stop at the borders of future contracting states : this is why the CoE Convention is intended as a global instrument, reaching all nations that are willing and capable of joining the original group of Contracting States.
- Criminality deriving from new technologies (computers, Internet, wireless communications) provides daunting challenges for law enforcement around the world. The CoE Convention is just one important step forward taken by the international community to meet this challenge.