THE CONVENTION ON CYBERCRIME

Margaret KILLERBY

Head of Department of Crime of Problems

DGI

Council of Europe, Strasbourg

THE CONVENTION ON CYBERCRIME

- Dangers of Cybercrime
- Nature of Cybercrime
- Fighting cybercrime
- Need for a Convention
- Convention on Cybercrime
- Crimes covered by the Convention
- Effective procedural measures under the Convention
- Promoting international co-operation by the Convention
- Developments concerning the Convention on cybercrime

THE CONVENTION ON CYBERCRIME

WHAT ARE THE DANGERS OF CYBERCRIME?

Information and communication technologies (ICT)
= indispensable

BUT

VERY dangerous as it is an unsafe environment

WHY?

THE CONVENTION ON CYBERCRIME

- Cybercrime is the fastest growing category of crime in many countries (especially child pornography)
- Cybercrime attacks individuals, the private sector, States, cultural and legal traditions and the global economy
- Cybercrime threatens your computer system, your finances, your identity, your personal information and your security
- Cybercrime facilitates the commission of both computer related and traditional crimes
- Cybercrime is easy to carry out but difficult to detect, to identify the criminals, to obtain evidence and to prosecute
- The technical and legal complexity of cybercrime is increased as most cybercrime crosses international frontiers

THE CONVENTION ON CYBERCRIME

- Should we be worried?
- YES – VERY WORRIED

THE CONVENTION ON CYBERCRIME

WHAT IS CYBERCRIME ?

Crimes committed against computer systems:

- gaming illegal access (for example by hacking, cracking)
- illegally intercepting information (for example by monitoring or recording)
- interfering with information or the computer system (viruses, Trojan horses, denial of services attacks, misuse of devices such as hacker tools)

THE CONVENTION OF CYBERCRIME

Crimes committed through computer systems such as:

- computer related forgery or fraud
- child pornography
- cyberhate texts
- infringement of copyright
- cyberlaundering
- cyberterrorism

THE CONVENTION ON CYBERCRIME

HOW CAN WE FIGHT CYBERCRIME?

- Prevention: promoting awareness, security, reporting, training
- Working closer together: victims, internet service providers (ISPs), law enforcement, public and private sectors
- Ensuring common minimum technical and legal standards which are compatible and workable at a national and international level
- Providing a global binding solution available to all States to enable them to raise their standards and avoid becoming safehavens by:

THE CONVENTION ON CYBERCRIME

- harmonising common types of cybercrime offences (to ensure compability concerning conduct which is criminal, to avoid gaps in legislation and problems of dual criminality)

- strengthening procedural law (to ensure rapid and effective procedures and common types of investigative powers to assist international investigations and to obtain eletronic evidence before all traces disappear)

- promoting international co-operation (to increase co-operation between law enforcement authorities)

THE CONVENTION ON CYBERCRIME

WHY DO WE NEED A CONVENTION?

- Guidelines not sufficient (definitions, co-operation)
- Role of bilateral agreements (numerous, too complicated)
- Need for a Convention (binding, effective)
- Specific role of the Convention on cybercrime (practical, existing, widely accepted).

THE CONVENTION ON CYBERCRIME

WHAT IS THE CONVENTION ON CYBERCRIME?

- The only binding instrument that prevents and combats worldwide cybercrime

  - in force (2004)
  - widespread international support and has been used as a model law
  - open to all States (fight against cybercrime can only be won at an international level)
  - fair: balances the needs of law enforcement (for example speed, secrecy and sufficient powers) with the respect for individual rights.

THE CONVENTION ON CYBERCRIME

– flexible:

enables States to adapt provisions to their own legal systems (by means of interpretation of certain general requirements for example «intentionally» or « without right », the extent that insignificant conduct may be excluded; by means of declarations (Article 40) or reservations (Article 42)

maintains the application of existing agreements (Article 39)

contains provisions to enable the Convention to be amended (Article 44)

describes conduct rather than technology to ensure that it will remain effective even when technology evolves

THE CONVENTION OF CYBERCRIME

The Convention deals with:

. substantive criminal law (i.e. what is generally agreed to be unacceptable)

. procedural law (i.e. to assist law enforcement) deal with the new technological environment)

. international co-operation (i.e. to ensure that frontiers do not hinder the fight against cybercrime).

THE CONVENTION OF CYBERCRIME

WHICH CRIMES ARE COVERED BY THE CONVENTION ON CYBERCRIME?

- The Convention applies to:
- ✓ criminal offences committed by means of a computer system
- ✓ the collection of evidence in electronic form of a criminal offence

- Certain types of crime are specifically mentioned:

a) new types of computer crime

- ✓ illegal access to a computer (confidentiality) - Article 2
- ✓ illegal interception of computer data (integrity) - Article 3
- ✓ data interference (availability) - Article 4

THE CONVENTION OF CYBERCRIME

- ✓ system interference – Article 5
- ✓ misuse of devices (to commit offences under Articles 2 to 5) Article 6

b) traditional crimes by new technologies

- ✓ computer related forgery (public or private documents) Article 7
- ✓ computer related fraud (for example credit card fraud, electronic frauds) - Article 8
- ✓ child pornography (criminalises from production to possession) - Article 9
- ✓ infringement of copyright and related rights - Article 10

THE CONVENTION OF CYBERCRIME

- ✓ cyberhate (racist and xenophobia material , threats or insults, denial etc of genocide or crimes against humanity) - Additional Protocol concerning the criminalisation of acts of racist and xenophobia nature committed through computer systems

The above crimes must be committed « intentionally » and « without right » (slightly different wording for Article 10)

- ❑ Additional provisions concern: attempts, aiding and abetting (Article 11), corporate liability (Article 12) and sanctions and measures which must be effective, proportionate and dissuasive (Article 13)

- ❑ The Parties must assume jurisdiction over the above offences when committed in their territory (or on board one of them registered aircraft) or by nationals (unless extradited) Article 22

THE CONVENTION OF CYBERCRIME

HOW DOES THE CONVENTION ON CYBERCRIME ENSURE THAT PROCEDURAL MEASURES ARE EFFECTIVE?

- Parties are required to have powers to investigate cases (Article 14), subject to the usual domestic and international safeguards for example proportionality (Article 15) and in particular powers to order:
- ✓ the expedited preservation of computer data (i.e. keeping and protected from change) - Article 16 and the expedited preservation and partial disclosure of traffic data (for example the identify other ISPs) Article 17
- ✓ the production of specified computer data (or data concerning subscriber information) - Article 18 and the search and seizure of computer data (used if the person is not trustworthy enough for Article 18 to be used) - Article 19
- ✓ Real time collection of traffic data – Article 20 and interception, in serious cases, of content data – Article 21

THE CONVENTION OF CYBERCRIME

HOW DOES THE CONVENTION ON CYBERCRIME PROMOTE INTERNATIONAL CO-OPERATION?

- The Convention requires Parties:

- ✓ to co-operate « to the widest extent possible » (Article 23)
- ✓ to provide for the possibility for extradition for serious offences under Articles 2 to 11 (Article 24)
- ✓ to provide mutual assistance « to the widest extent possible » (Article 25) including:

THE CONVENTION OF CYBERCRIME

- the sending of spontaneous information were there are no applicable agreements to help another Party (Article 26)
- the designation of a central authority to deal with mutual assistance (Article 27) subject to confidentiality and limitation on use (Article 28)
- mutual assistance regarding provisional measures (expedited preservation of stored computer data – Article 29; expedited disclosure of preserved traffic data – Article 30)
- mutual assistance regarding investigative powers (mutual assistance regarding accessing of stored computer data - Article 31; transborder access to stored computer data with consent or where publicly available Article 32;
- mutual assistance in the real time collection of traffic data Article 33;
mutual assistance in the interception of content data -Article 34)

THE CONVENTION OF CYBERCRIME

. to set up a 24/7 Network which is an important means of co-operation (Article 35)

THE CONVENTION OF CYBERCRIME

HAVE THERE BEEN ANY RECENT DEVELOPMENTS CONCERNING THE CONVENTION ON CYBERCRIME?

- Present state of signatures, ratifications and accessions (Articles 36 & 37)
- Consultations of the Parties (Article 46)
- Further steps which we can take to prevent cybercrime:
  - promote awareness of dangers of cybercrime
  - promote Convention on cybercrime
  - promote training of persons dealing with cybercrime
  - promote international co-operation to combat cybercrime

Thank you for your attention.

For further information:

margaret.killerby@coe.int

www.coe.int/economiccrime