The global state of cybercrime legislation

Workshop 1: Cybercrime legislation (Octopus Conference, Strasbourg, 6-8 June 2012)

Cristina SCHULMAN
Cybercrime Unit
Data Protection and Cybercrime Division
Directorate General Human Rights and Rule of Law
Council of Europe
Email: cristina.schulman@coe.int

Project on Cybercrime
www.coe.int/cybercrime

The global state of cybercrime legislation

- Prepared under the Global Project on cybercrime funded by Estonia, Japan, Romania, United Kingdom, Microsoft and Council of Europe
- Use of the Cybercrime Convention *(Budapest Convention)*
  Substantive Law: Articles 2-9
  Procedural Law: Articles 16-21
- Objective: To provide information about cybercrime legislation worldwide

The Budapest Convention

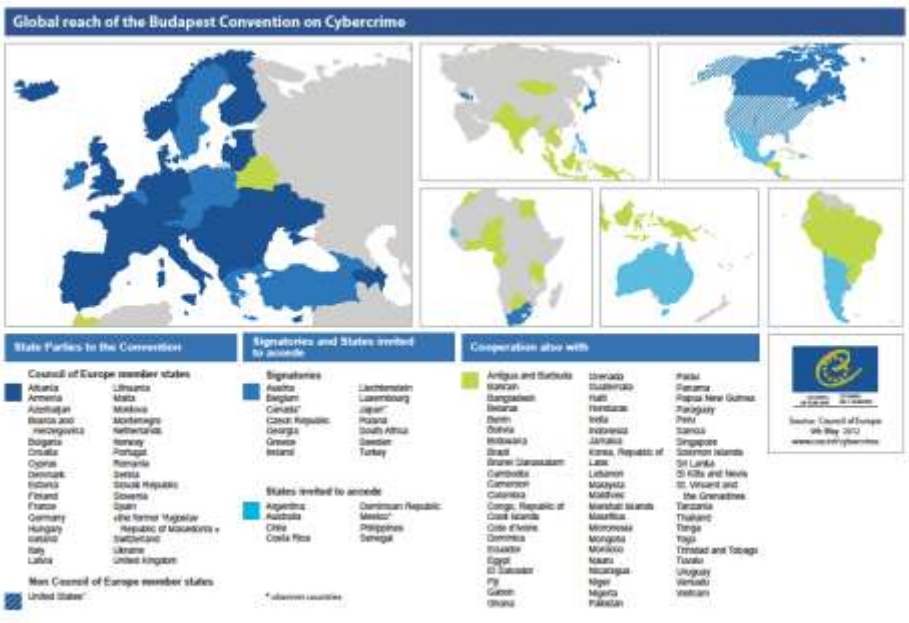
Art 37: Open to any country to become Party

33 Parties:
- European
- USA

soon 36 (Austria,Georgia Dominican Republic)

14 Signatures:
- European
- Canada
- Japan
- South Africa

8 invitations to accede:
- Argentina
- Australia
- Chile
- Costa Rica
- Dominican Republic
- Mexico
- Philippines
- Senegal



About the Budapest Convention

Budapest Convention
- Criminalising conduct
- Efficient investigations through procedural law tools + conditions and safeguards
- International cooperation

Concept of cybercrime:
- Offences against and by means of computers
- Electronic evidence related to any crime

Criminal justice treaty:
- cyberCRIME
- rule of law + human rights principles

- Guideline + treaty
- Generic (conduct) + specific
- Negotiated + accepted
- Scalable
  - Membership
  - Contents (protocols)
  - Link to other standards
- Mature and proven to work:
  - 10 y+ preparation
  - 10 y implementation
- Risk of lower standards and digital divide if a new treaty is prepared

Budapest Convention: Substantive Criminal Law

Legislation to deal with – as a minimum:

- ❑Illegal access to a computer system ("hacking", circumventing password protection, exploiting software loopholes etc.)
- ❑Illegal interception (violating privacy of data communication)
- ❑Data interference (malicious codes, viruses, trojan horses etc.)
- ❑System interference (hindering the lawful use of computer systems)
- ❑Misuse of devices (tools to commit cyber-offences)
- ❑Computer-related forgery (similar to forgery of tangible documents)
- ❑Computer-related fraud (similar to real life fraud)
- ❑Child pornography
- ❑Infringement of copyright and related rights

Criminalising specific conduct and not techniques/technologies

Budapest Convention: Procedural Criminal Law

Legislation to provide for – as a minimum:

- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data
- Procedural safeguards

Budapest Convention: other provisions

Article 15 - Conditions and safeguards

Each Party shall ensure that ... the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties

Chapter III of the Convention - International cooperation

Section 1 – General principles

Section 2 – Specific provisions

Preservation vs. data retention

	Expedited preservation	Data retention (EU Directive)
Aim	Provisional measure to preserve volatile electronic evidence to allow for time for formal measures to obtain evidence	Ensure that data is available for investigation, detection and prosecution of serious crime
Specific/ automated	Specific order for specified data	Automatic retention of data
Type of Data	Any data (including content data)	Traffic and location data and subscriber information (not content data, nor destination IP addresses, URLs, email headers, or list of cc recipients)
Purpose limitation	Any crime involving electronic evidence	Serious crime
Addressee	Any physical or legal person (not limited to service providers)	Service providers
Time period	Flexible: 90 days (renewable)	Specific retention period (6 to 24 months as specified in domestic law)

The global state of cybercrime legislation

Albania, Algeria, Antigua and Barbuda, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahamas, Bangladesh, Barbados, Belarus, Belgium, Benin, Bhutan, Bolivia, Bosnia and Herzegovina, Botswana, Brazil, Brunei Darussalam, Bulgaria, Cambodia, Cameroon, Canada, Chile, China (People's Republic of China), Costa Rica, Croatia, Cyprus, Czech Republic, Dominican Republic, Ecuador, El Salvatore, Estonia, Fiji, Finland, France, Georgia, Germany, Ghana, Guatemala, Honduras, India, Indonesia, Iran, Iraq, Israel, Japan, Jordan, Kenya, Kiribati, Kosovo*, Lao People's Democratic Republic, Lithuania, Malaysia, Mauritius, Mexico, Mongolia, Montenegro, Morocco, Namibia, Nepal, New Zealand, Nicaragua, Nigeria, Pakistan, Panama, Papua Guinea, Paraguay, Peru, Philippines, Portugal, Republic of Moldova, Romania, Russian Federation, Saint Vincent and the Grenadines, Samoa, Saudi Arabia, Senegal, Serbia, Singapore, Slovakia, South Africa, Spain, Sri Lanka, Thailand, "The Former Yugoslav Republic of Macedonia", Tonga, Tunisia, Turkey, Uganda, Ukraine, United Arab Emirates, United Kingdom, United Republic of Tanzania, Unites States of America, Uruguay, Vanuatu, Vietnam and Zambia

** All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo*

The global state of cybercrime legislation

- 30% of the countries have a good level of implementation of substantive law and procedural law provisions
- 60% of the countries have adequate substantive law provisions
- Provisions largely complying with the provisions of the Budapest Convention: illegal access, data interference and system interference
- Major challenge: procedural law
  - ✓ modernisation of existing powers (articles 18, 19, 20 and 21) and the establishment of new powers (articles 16 and 17) are incomplete

Substantive law: illegal access

- Illegal access: 70% of countries have implemented illegal access to computer system in line with the Convention
- Illegal access to computer systems vs. illegal access to computer data
  - ✓ The legal interests protected under Article 2 is broader: integrity, availability and confidentiality of computer systems and computer data

Substantive law: data interference

- 70% of the countries criminalise data interference

- Often countries criminalise data interference and system interference in the same article whereas the legal interests protected are different:
  - ✓ data interference aims at protecting the integrity and the proper functioning or use of stored computer data or computer programs
  - ✓ system interference aims at protecting the interest of operators and users of computer or telecommunication systems being able to have them function properly

- Not all forms of data manipulation are criminalised i.e. damaging, deletion, deterioration, alteration and suppression of computer data that affect information content (integrity) and availability for retrieval or processing.

Substantive law: system interference

60% of the countries criminalise system interference

- A number of legislations provides vague and unclear provisions to criminalise system interference

- Provisions seem to refer also to physical destruction of computer system

- A form of system interference is denial of service attacks. Such DDOS attacks can be used to hinder or disable critical infrastructure. Thus criminalisation of ''blocking of a computer system'' is not sufficient to consider such attacks.

- A lower implementation of Article 4 and 5 cannot guarantee the protection of critical infrastructure

Substantive law: Articles 3 and 6

Implementation of illegal interception, misuse of devices

- Illegal interception
  - ✓ Partial implementation and missing important elements e.g. non-public transmissions of computer data, electromagnetic emissions or the means of interception
  - ✓ Some countries would need to apply traditional offences related to violation of secrets of correspondence for illegal interception of computer which is different from illegal interception that can be compared to a surveillance or spying.
- Misuse of devices
  - ✓ 30% of the countries studied do not have any legislation in place for this provision
  - ✓ Partial implementation : dual use of devices is not considered; focus on the production of some specific devices; misuse of devices is criminalised only in relation with illegal access or system interference

Substantive law: Articles 7-9

- 30% of countries have implementation of computer related offences (forgery and fraud) in line with the Convention
- Traditional offences of fraud and forgery are applicable
- Need to consider:
  - ✓for forgery: the offence should apply to an electronic document
  - ✓for fraud, it is important to take into consideration any kind of manipulation of data as well as any interference with the functioning of a computer system
- Child pornography : A study has been completed and will be presented in workshop 3

Procedural law: Articles 16, 17 and 20

Expedited preservation of stored computer data (Article 16)
Preservation and disclosure of traffic data (Article 17)
Real-time collection of traffic data (Article 20)

- Only about 20% of the countries seem to have such powers
  - ✓ partial implementation or no implementation
  - ✓ time for preservation is not determined
  - ✓ implementation of the data retention, which is not provided under the Budapest Convention

Procedural law: Search and seizure

- About 20% of the countries have implemented Article 19
- It requires adaptation of the traditional power of search and seizure for cybercrime investigations:
  - ✓ search and similarly access a computer system or a computer storage medium;
  - ✓ search and similarly secure computer data accessed: seize or similarly secure a computer system, make and retain copy of those computer data, maintain the integrity of the relevant stored computer data, render inaccessible or remove those computer data in the accessed computer system.
- Many countries do not expressly provide specific provisions for these powers
- Ensuring adequate safeguards when establishing such powers in the connection with computer systems and computer data is crucial.

The global state of cybercrime legislation

Preliminary findings

- **Budapest Convention on Cybercrime has served as a model law for many countries in the world regardless the region or if it is or not Party**
- **Substantive law:** 90% took inspiration from the Budapest Convention or the Commonwealth Model Law on computer and computer related crime
  - ✓ Some offences, in particular illegal access, illegal interception and data interference are often implemented using the same wording of the Budapest Convention
  - ✓ Some legislations seem to be inspired by some European countries that implemented Convention e.g. Senegal, Morocco, Algeria, Cambodia considered the French legislation; similarly many countries were inspired by United Kingdom
- **Procedural law: among 20% of those who have implemented the powers, 90% used the Convention as a guideline and 10% the commonwealth model law.**
- **The way ahead: need for stronger implementation Budapest Convention and harmonisation of cybercrime legislation**

Contact:

Cristina SCHULMAN

Email: cristina.schulman@coe.int

Marie AGHA-WEVELSIEP
Project Officer
Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe
F-67075 Strasbourg Cedex
Tel +33-3-9021-5666
Fax +33-3-9021-5650
Email marie.agha-wevelsiep@coe.int
www.coe.int/cybercrime