www.coe.int/cybercrime

Meeting the challenge of cybercrime: the legal framework

Makati City, Philippines, October 2007

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

1

1 About the Council of Europe ... www.coe.int

Strategy against economic crime
THE RATIONALE

democracy
rule of law
human rights

in order to promote

Measures against economic and organised crime

Established in 1949
Currently 47 member States

2

2

Cybercrime – current challenges

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**

3

3

1. **Dependency of societies on information and communication technologies. This dependency makes societies highly vulnerable to cybercrimes**

WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2007 Est.)	Population % of World	Internet Usage, Latest Data	% Population (Penetration)	Usage % of World	Usage Growth 2000-2007
Africa	933,448,292	14.2 %	**43,995,700**	4.7 %	3.5 %	874.6 %
Asia	3,712,527,624	56.5 %	**459,476,825**	12.4 %	36.9 %	302.0 %
Europe	809,624,686	12.3 %	**337,878,613**	41.7 %	27.2%	221.5 %
Middle East	193,452,727	2.9 %	**33,510,500**	17.3 %	2.7 %	920.2 %
North America	334,538,018	5.1 %	**234,788,864**	70.2 %	18.9%	117.2 %
Latin America/Caribbean	556,606,627	8.5 %	**115,759,709**	20.8 %	9.3 %	540.7 %
Oceania / Australia	34,468,443	0.5 %	**19,039,390**	55.2 %	1.5 %	149.9 %
WORLD TOTAL	6,574,666,417	100.0 %	**1,244,449,601**	18.9 %	100.0 %	244.7 %

4

2. Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading

Software inserted into an information system that causes harm to this or other systems

For example: more than 210,000 new malicious code threats reported Jan-June 2007 (Symantec)

Types:
- Backdoors allowing unauthorised access
- Key loggers
- Rootkits concealing that a computer is compromised
- Spam as a vector for malware
- Spyware capturing and transmitting user data
- Trojan horses to circumvent security measures and carry out attack
- Virus to reduced system performance, destroy data or cause other damage
- Worms (self-replicating)

5

2. Malware ...

Disseminated through:

- Email
- Web
- Instant messengers
- P2P
- Shared-file systems
- Internet Relay Chat
- Removable media

Used for:

- Denying access (distributed denial of service attacks through bots and botnets)
- Extortion
- Stealing information, including identity theft

6

6

2. Malware ...

Bots and Botnets

Covertly installed programmes on a computer to allow unauthorised remote control

Can be used

- for distributed denial of service (DDOS) attacks
- to harvest confidential information (identity theft)
- to distribute spam, spyware, adware
- for phishing attacks

For example:> 52,000 active bot-infected computers per day in 2007, 27% of bot infected computes in China, 13% in USA, 10% in Poland; 43% of command and control servers in USA; 61% of DOS attacks targeted USA (Symantec)

7

7

2. Malware ...

Identity theft

The misuse of the identity (name, date of birth, address, financial information or other personal details) of another person without knowledge or consent
Used to commit a wide variety of crimes
Forms:

- "Theft": Bin raiding, hacking, spyware and other crimeware (e.g. Keyloggers), skimming of credit cards etc.
- Social engineering (deception and psychological manipulation to make people comply with a request):
  - Phishing ("password fishing"), spoofing (fake sites or emails), pharming, vishing, smishing etc

For example: 12.5 million phishing emails per day blocked in 2007 (Symantec); 18% increase in unique phishing messages in 2007 compared to first half of 2006; 59% phishing sites based in USA

Make identity theft a separate offence?

8

8

3. Spam nuisance and carriers of malware

- More than 60% of email traffic considered spam
- 47% of spam detected worldwide originated from USA
- 1 / 233 spam contained malicious codes

(Symantec data for Jan-June 2007)

9

9

4. Child pornography and sexual exploitation on the internet increasingly commercial

- Increasing reporting on child pornography on the internet
- Problem: legislative gaps in many countries
- Child porn sites hosted in many different countries (see www.iwf.org.uk)
- Increasing number of commercial sites
- Convention on Cybercrime: opportunity for broad criminalisation and international cooperation against child porn on the internet

10

10

5. Offenders increasingly organising for crime aimed at generating illicit profits

- ICT facilitate offences by OC groups and networks, in particular economic crime
- ICT creates vulnerabilities -> exploited by OC
- ICT facilitate logistics, anonymity and reduce risks of OC
- ICT facilitate global outreach of OC
- ICT shape OC -> networks

Emergence of underground economy servers to sell stolen information

Breakdown of goods in 2007:

1 Credit cards 22%
2 Bank accounts 21%
3 Email passwords 8%
4 Mailers 8%

11

11

6. Botnets one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware)

Underground service economy developing: botnets for rent

Division of labour in criminal projects:

- Coder = writer of malicious code
- Launcher = runs the code
- Miner = extracts data
- Washer = launders proceeds

(Europol)

12

12

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

For example:

- **data breaches with possible identity theft: 30% in education sector, 26% government, 15% health, 14% financial sector in 2007 (Symantec)**
- **72% of spoofed websites were sites of financial service organisation**

13

13

8. Growing risk of cyber-attacks against critical infrastructure

The question of cyberterrorism

Terrorist may use information and communication technologies for:

- **Attacks via the internet aimed at essential electronic communication systems, IT infrastructure 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**

14

14

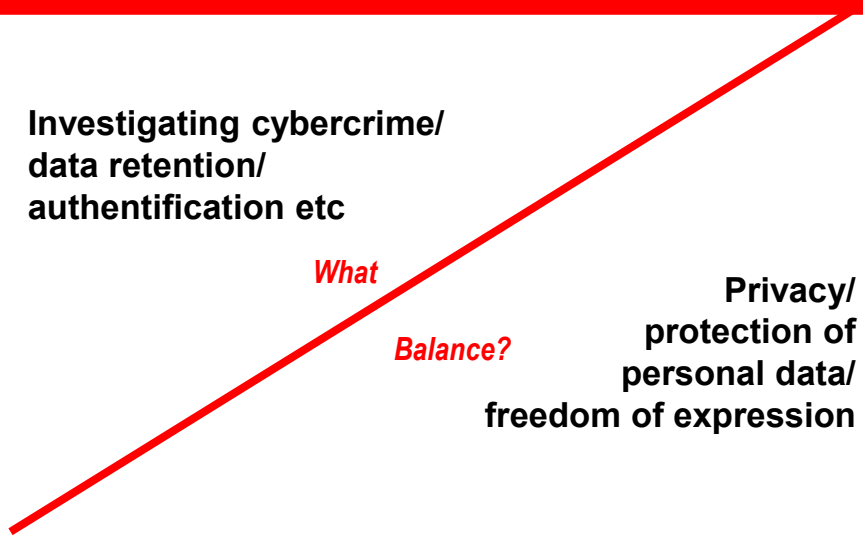
9. Remote storage of data (problem for investigators)

10. Next-generation-networks (NGN), including VoIP (problem for investigators)

15

15

Issues (1)



16

16

Issues (2)

Law enforcement

What

relationship?

Service providers

17

17

Issues (3)

Efficiency of investigations/ technical possibilities

What

safeguards?

Due process

18

18

3 The legislative response to cybercrime

- Criminalise certain conduct ▶ 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

19

19

Substantive law

Legislation to deal with – as a minimum:

- **Illegal access to a computer system** ("hacking", circumventing password protection, key-logging, 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**
- **Child pornography**
- **Hate speech, xenophobia and racism**
- **Infringement of copyright and related rights**

Criminalising specific techniques/technologies or a certain conduct?

20

Procedural 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

21

21

4 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

22

22

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)

25

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

26

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

29

29

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

30

30

Conclusions

The Convention serves as a framework for international cooperation against cybercrime

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

By becoming a party to this treaty, the Philippines can make use of this framework

31

31

Conclusions

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

32

32

Conclusions

"Model law" function of the Convention

- Use as a checklist
- Compare provisions

Provision of Convention	Provision in national law
Art 4 System interference	?
Art 6 Misuse of devices	?
Art 9 Child pornography	?
Art 16 Expedited preservation	?
Art 18 Production order	?

33

33

Thank you.

Alexander.seger@coe.int

34

34