COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Cybercrime and digital evidence: the legal framework

Seminar on prosecuting cybercrime
Yogyakarta, Indonesia, 23 September 2010

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

1

1 Introductory remarks

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

democracy
rule of law
human rights

in order to promote

Measures against economic and organised crime

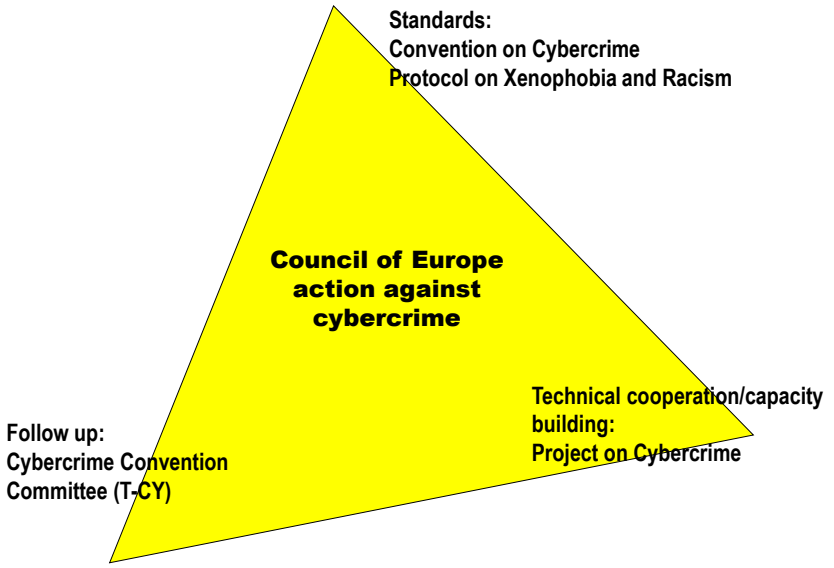
COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Established in 1949
Currently 47 member States

www.coe.int/cybercrime

2

The Council of Europe approach against cybercrime



www.coe.int/cybercrime

3

3

About the Budapest 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

- 30 countries have ratified so far (European + USA)
- 16 have signed e (European + Canada, Japan, South Africa)
- 7 invited to accede (Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines)
- Used as a guideline for legislation by many others
- Any country meeting the requirements of this treaty can accede

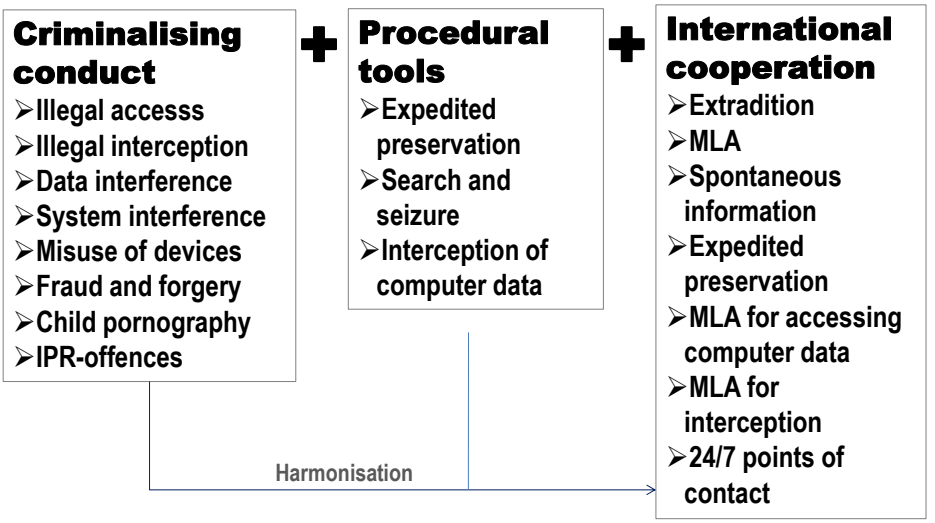
- Complemented by the Protocol on Xenophobia and Racism Committed through Computer Systems

www.coe.int/cybercrime

4

4

Scope of the Budapest Convention



www.coe.int/cybercrime

5

2 What is cybercrime?

Crime against computers	Crime by means of computers
1. Offences against the confidentiality, integrity and availability of computer data and systems	2. Computer-related forgery and fraud
➢ Illegal access to a computer system	3. Content-related offences (child pornography, xenophobia, racism)
➢ Illegal interception	4. Offences related to intellectual property rights and similar rights
➢ Data interference	
➢ System interference	
➢ Misuse of devices	

www.coe.int/cybercrime

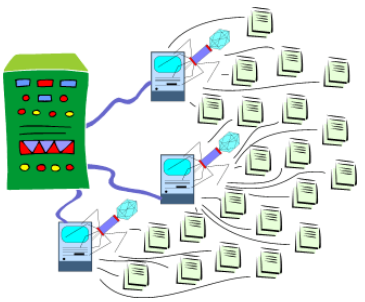
6

6

What is cybercrime?

Situation, trends and infrastructure

- Malware
- Botnets
- Underground economy
- Criminal domains
- Social networking platforms
- Cyberwarfare, „hacktivism“, espionage, terrorism
- Organised crime
- Cybercrime aimed at proceeds (fraud)



What is cybercrime?

Case study: Targeting online banking customers (Source: M86 Security)

1. Criminals infect legitimate website/malicious adverts
2. Users accessing sites are redirected to a site from where an exploit kit is downloaded
3. Trojan horse is downloaded to the user`s computer
4. User computer is an externally controlled bot (robot, zombie)
5. User access bank account online; Trojan transfers login and other credentials to command and control (CC) server
6. Data of bank transaction form is sent to CC server, instead of bank
7. System of CC servers decrypts information and selects a mule account
8. Trojan receives instructions to send an updated transaction form to bank to transfer money to a mule account

= £ 675,000 stolen in July/August 2010

- Illegal access, illegal interception, data and system interference, forgery and fraud
- Organised criminals and use of money mules

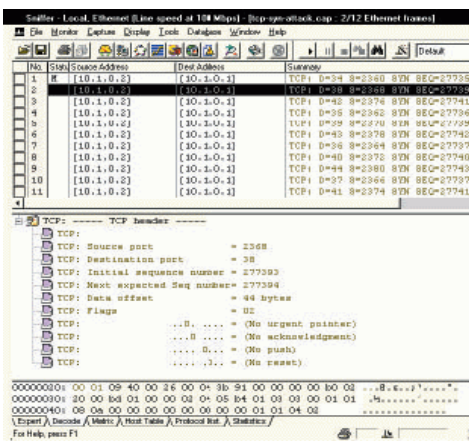
Legal response to cybercrime 1: Need to criminalise conduct

Budapest Convention	Conduct	Indonesia
Art 2	Illegal access to computer system	✓Art 30 (Act 11/2008 IET)
Art 3	Illegal interception	✓Art 31 (Act 11/2008 IET)
Art 4	Data interference	✓Art 32 (Act 11/2008 IET)
Art 5	System interference	✓Art 33 (Act 11/2008 IET)
Art 6	Misuse of devices	✓Art 34 (Act 11/2008 IET)
Art 7	Computer-related forgery	✓Art 35 (Act 11/2008 IET)
Art 8	Computer-related fraud	✓Art 36 (Act 11/2008 IET)
Art 9	Child pornography	Art 27 + 52 (Act 11/2008 IET)
Art 10	Infringement of copyright and related rights	Art 4 (draft Cybercrime Law)

3 Investigating, prosecuting, adjudicating cybercrime: challenges

Evidence 

Electronic evidence



Electronic evidence is volatile evidence ►need for efficient, urgent measures

Legal response to cybercrime 2:
Procedural law tools for efficient investigations and securing electronic evidence

Budapest Convention	Procedural law measure	Indonesia
Art 16	Expedited preservation of stored computer data	Art 8 + 9 + 10 (draft Cybercrime Law) = retention
Art 17	Expedited preservation and partial disclosure of traffic data	
Art 18	Production order	Art 5 + 12 (draft Law)
Art 19	Search and seizure of stored computer data	Art 13 (draft Law) + Art 24 (Act 11/2008 IET)
Art 20	Real-time collection of traffic data	Art 14 (draft Law)
Art 21	Interception of content data	Art 11 + 14 (draft Law)
Art 15	Safeguards and conditions	Art 42 + 43 (Act 11/2008)

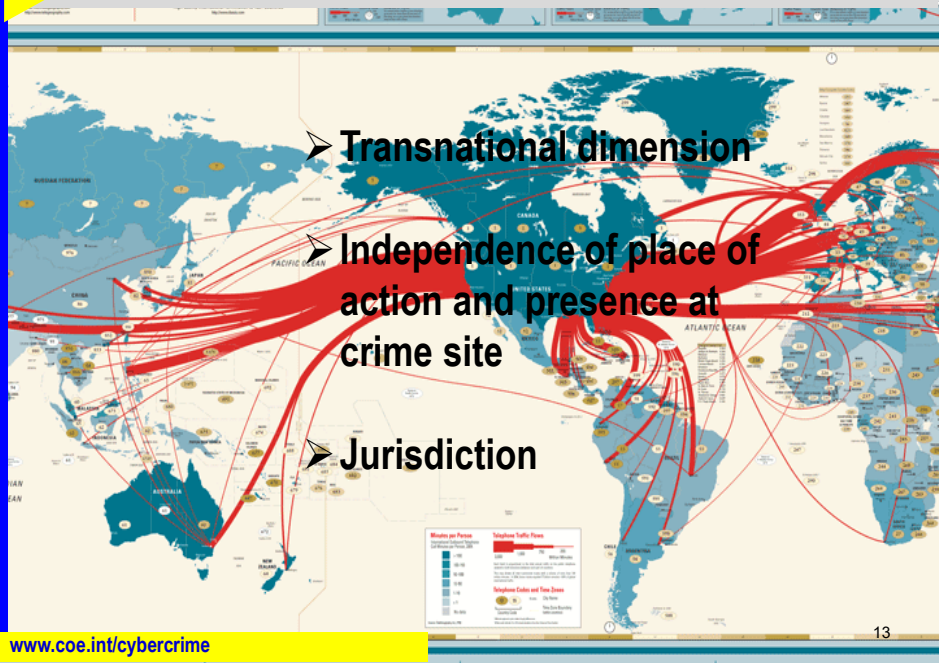
Data preservation ≠ Data retention!

11

4 More challenges: cybercrime as transnational crime

12

More challenges: cybercrime as transnational crime



www.coe.int/cybercrime 13

13

Legal response to cybercrime 3:
Securing electronic evidence through international cooperation + accession to Budapest Convention

Budapest Convention	International cooperation provisions	Indonesia
Art 23 - 28	General principles (extradition, MLA etc.)	Art 20 + 19 (draft Law)
Art 29	Expedited preservation of stored computer data	Art 27 (draft Cybercrime Law)
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	
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	Art 22 (draft Law)

www.coe.int/cybercrime 14

14

International cooperation: Acceding to the Budapest Convention on Cybercrime

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

The Convention on Cybercrime: how to accede

Article 37: Convention is open for accession by third countries

Accession process:

1. Indonesia has adopted and has draft law before Parliament ►Government to send a letter to Secretary General of CoE with a request to initiate consultation with parties to the Convention
2. Secretariat of CoE will carry out informal consultations and put question before Committee of Ministers
3. Once vote is positive, the country will be invited to accede
4. The country is then free to decide when to accede, that is, deposit the instrument of accession

5 Training

Provide for sustainable training for law enforcement, prosecutors and judges

Global Project on Cybercrime/Octopus 2009:

- **Concept for training of judges and prosecutors in cybercrime and electronic evidence (www.coe.int/cybercrime ►resources): "to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training"**
- **Draft training manual**

6 Conclusion

With the Act 11/2008 on Information and Electronic Transaction and adoption of the (draft) Law on Cybercrime Indonesia will:

- **Have the legislation and tools to prosecute cybercrime**
- **Be in line with international standards (the Budapest Convention)**

Through accession to the Budapest Convention, Indonesia could also prosecute cybercrime also at the international level

Thank you!

Alexander.seger@coe.int