Council of Europe

READI Workshop on Cybercrime Legislation in ASEAN Member States, 27-28 November 2008, Kuala Lumpur, Malaysia

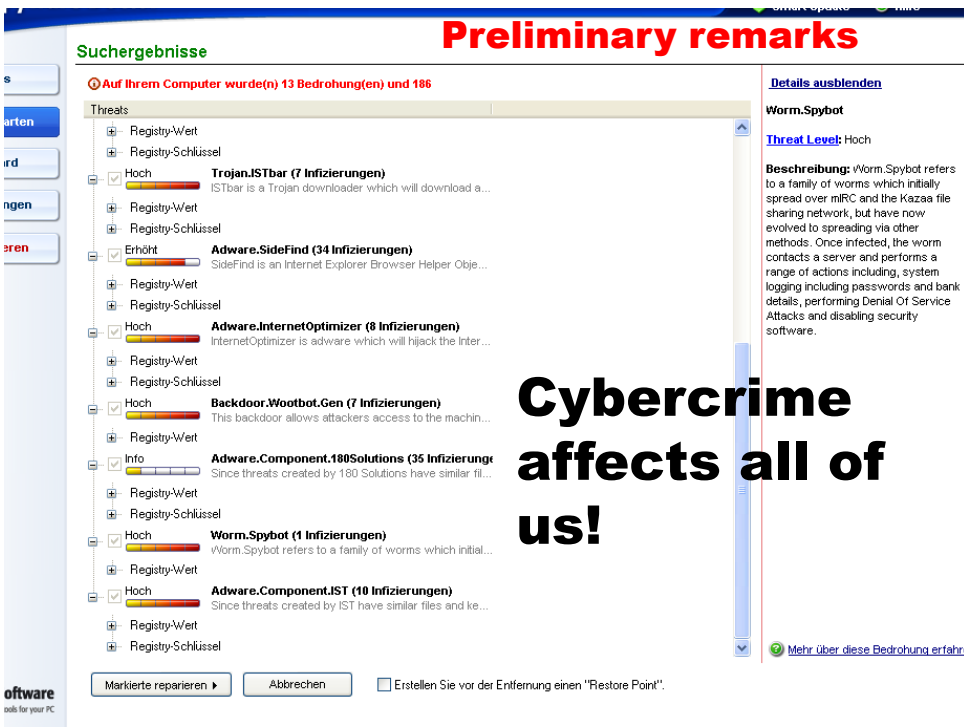
The threat of cybercrime: what legislative responses?

Alexander Seger
Economic Crime Division, Council of Europe
Strasbourg, France
alexander.seger@coe.int

www.coe.int/cybercrime

1

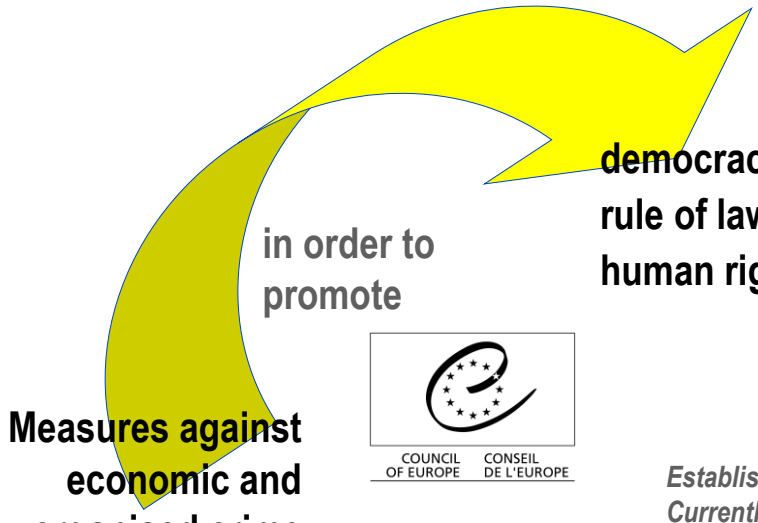
Preliminary remarks



Cybercrime affects all of us!

2

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

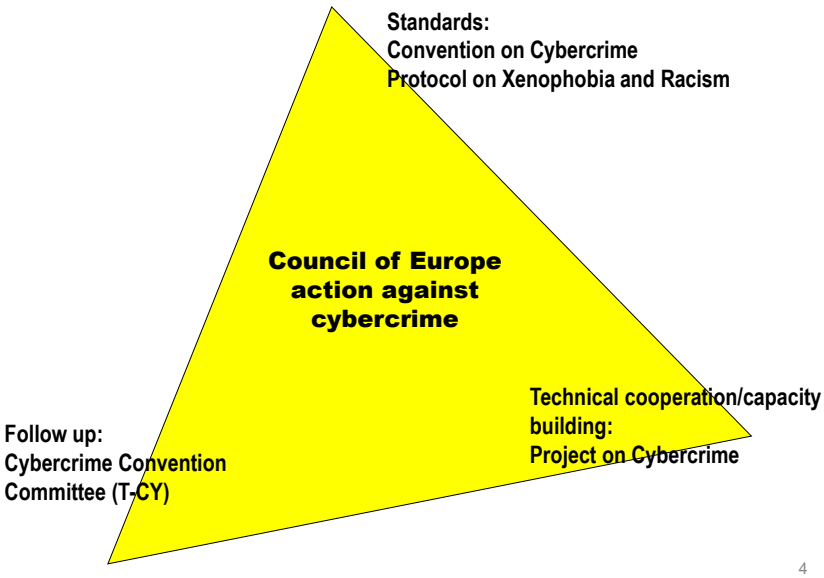


Established in 1949
Currently 47
member States

3

3

The approach against cybercrime



4

4

1 Why worry about cybercrime?

- Opportunities provided by information and communication technologies
- Information society: where is your private life taking place?
- Confidentiality, integrity, and availability of your computer data
- Reliance of public infrastructure on ICT
- Reliance of business on ICT
- Dependency of societies on ICT = vulnerability to cybercrime
- Need for secure and accessible ICT

But:

- Vast majority of people use ICT for legitimate purposes
- Safeguards and guarantees to ensure security and protect fundamental rights

5

5

2 What is cybercrime?

1. Offences against the confidentiality, integrity and availability of computer data and systems
2. Computer-related forgery and fraud
3. Content-related offences (child pornography, xenophobia, racism)
4. Offences related to intellectual property rights and similar rights

6

6

What is cybercrime?

1. Offences against the confidentiality, integrity and availability of computer data and systems (CIA offences)

- Illegal access to a computer system
- Illegal interception
- Data interference
- System interference
- Misuse of devices

7

7

What is cybercrime?

2. Computer-related forgery and fraud

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

- Security breaches and financial losses in companies
- Credit card fraud and other financial crime
- Advance fee fraud
- Extortion
- Internet marketing and retail fraud
- Auction fraud and stock market manipulation
- Phishing and other forms of identity theft
- Etc.

8

8

What is cybercrime?

3. Content-related offences

- Child pornography
- Xenophobia, racism, hate speech

Issue:

- Security and protection versus freedom of expression

9

9

What is cybercrime?

4. Offences related to intellectual property rights and similar rights

- IPR protected by national and international regulations
- Counterfeit products
- Health and safety risks
- Economic loss to companies and unfair competition
- Feeds organised crime

10

10

What is cybercrime?

Malware

Cross-cutting issues

- Software inserted into an information system that causes harm to this or other systems
- Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading

11

11

What is cybercrime?

SPAM

Cross-cutting issues

- Accounts for a large amount of internet traffic (70%+)
- Vector for malware

12

12

What is cybercrime?

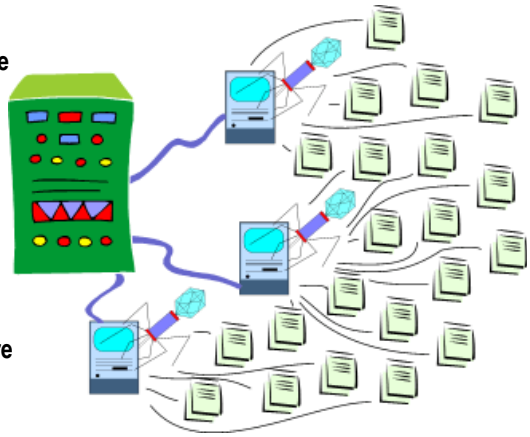
Bots and botnets

Cross-cutting issues

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



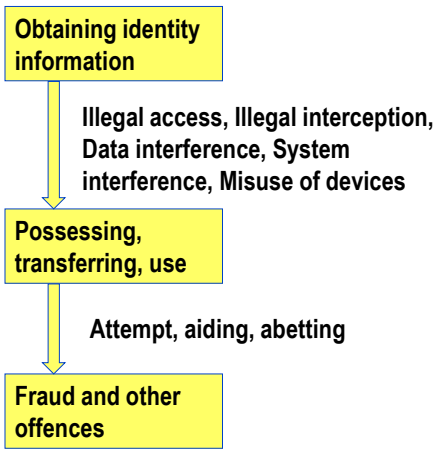
13

13

What is cybercrime?

Cross-cutting issues

Phishing and other forms of identity theft



14

14

What is cybercrime?

Cross-cutting issues

Cybercrime and organised crime

- Offenders increasingly organising for cybercrime
- Botnets an important tool
- 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

15

15

What is cybercrime?

Cross-cutting issues

Terrorist use of the internet/ICT

- Possible attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interests, including loss of life
- Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism, recruitment or training
- Use of ICT by terrorists for logistical purposes such as internal communication, gathering intelligence, target analyses

16

16

The legislative response 1: Substantive Criminal Law

Legislation to deal with – as a minimum:

- Illegal access to a computer system
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Computer-related forgery and fraud
- Child pornography, xenophobia, racism
- Infringement of copyright and related rights

Criminalising specific techniques/technologies or conduct?

17

17

3 Investigating, prosecuting, adjudicating cybercrime: challenges

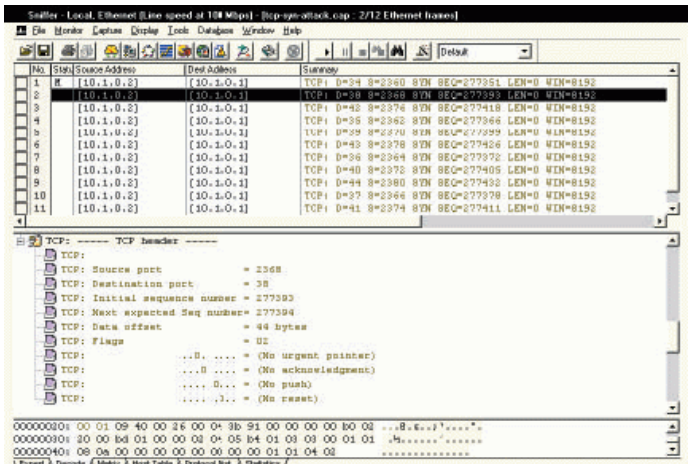
Evidence

18

18

Challenges

Electronic evidence



19

Challenges

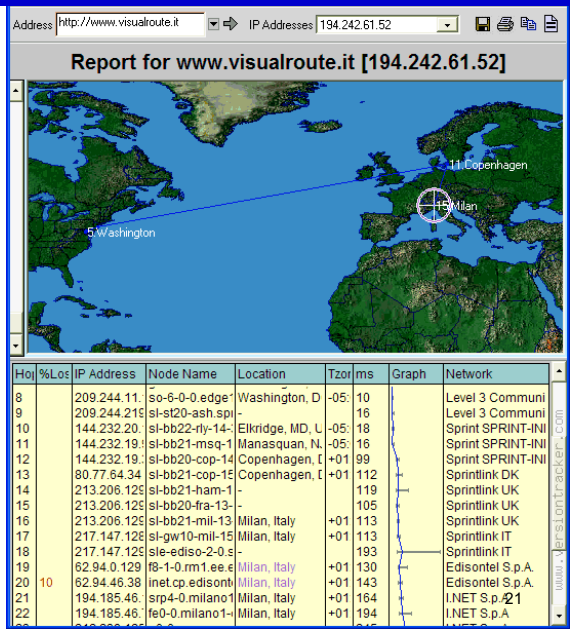
Many different kind of devices

20

Challenges

Electronic evidence is volatile evidence

- need for efficient, urgent measures



The legislative response 2: Procedural Law

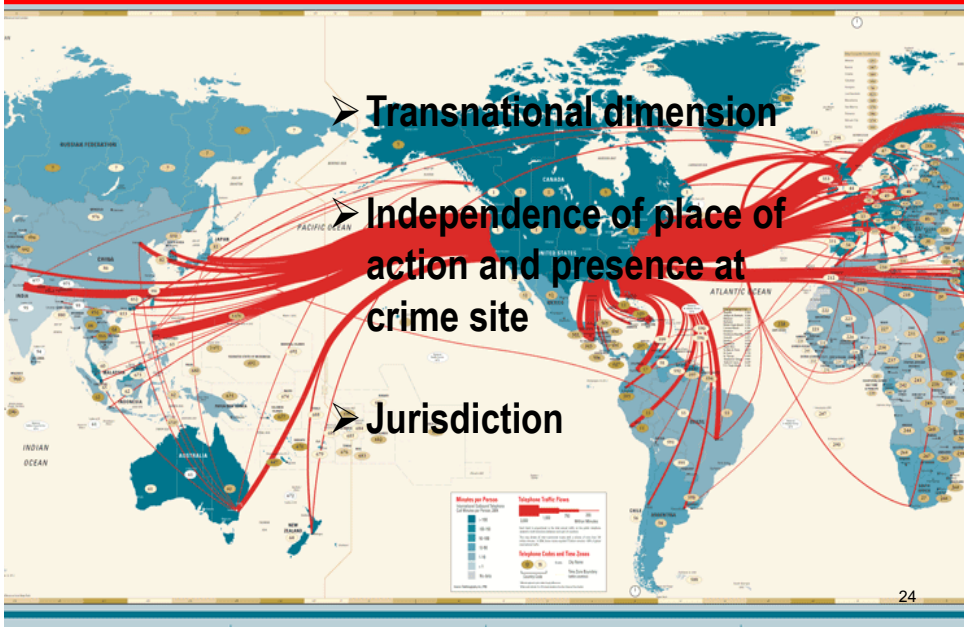
Legislation to provide for – as a minimum:

- 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

4 More challenges: cybercrime as transnatiohal crime

23

Challenges



24

The legislative response 3: International cooperation

- Harmonise legislation with other countries
- Join international agreements
- Provide for mutual legal assistance and other provisions for international cooperation
- Introduce specific provisions for:
  - Expedited preservation of stored computer data
  - Expedited disclosure of preserved computer data
  - Mutual assistance regarding accessing stored computer data
  - Trans-border access to stored computer data (public/with consent)
  - Mutual assistance in real-time collection of traffic data
  - Mutual assistance regarding interception of content data
  - 24/7 network

25

= The Convention on Cybercrime

The Budapest Convention on Cybercrime as a response:

- A guideline for consistent substantive and procedural legislation
- A framework for efficient international cooperation

26

26

Thank you

Alexander.seger@coe.int

27