Council of Europe

Cybercrime training for prosecutors and judges in South-eastern Europe
Ohrid, 17-18 November 2008

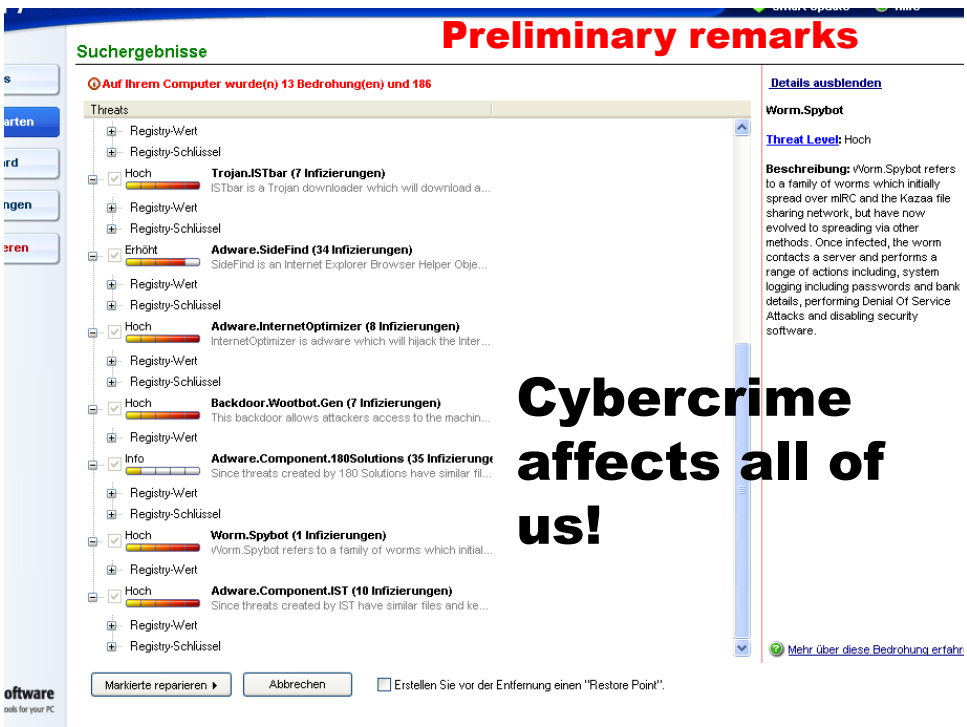
Why should judges and prosecutors worry about cybercrime?

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

www.coe.int/cybercrime

1

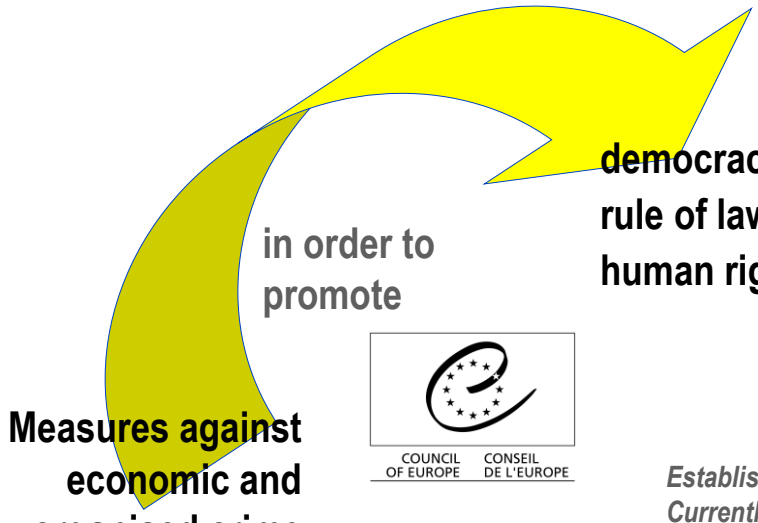
Preliminary remarks



Cybercrime affects all of us!

2

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

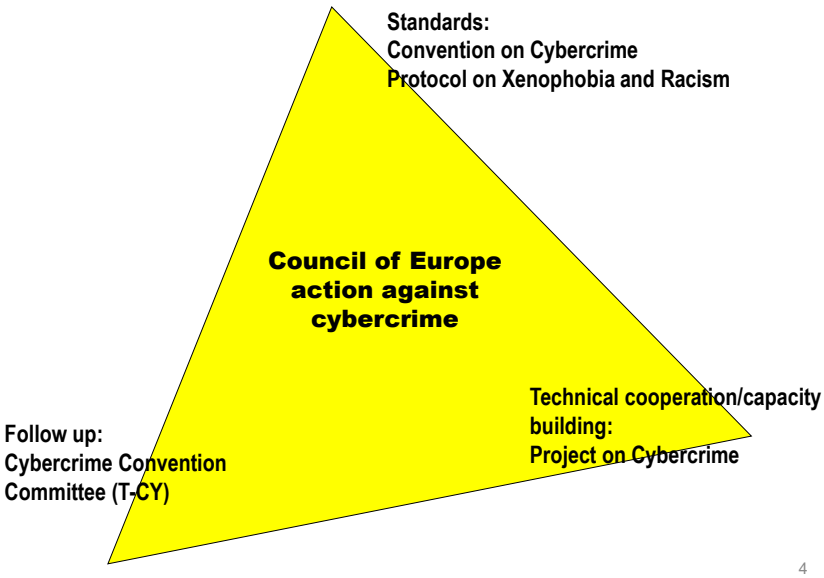


Established in 1949
Currently 47
member States

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?

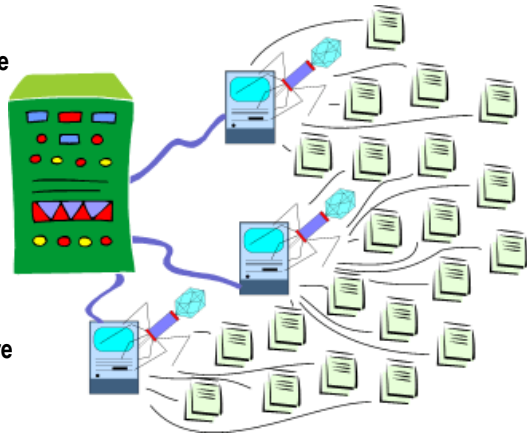
Bots and botnets

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



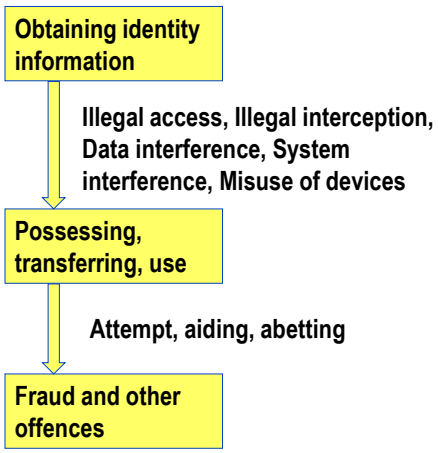
13

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

3 Investigating, prosecuting, adjudicating cybercrime: challenges for judges & prosecutors

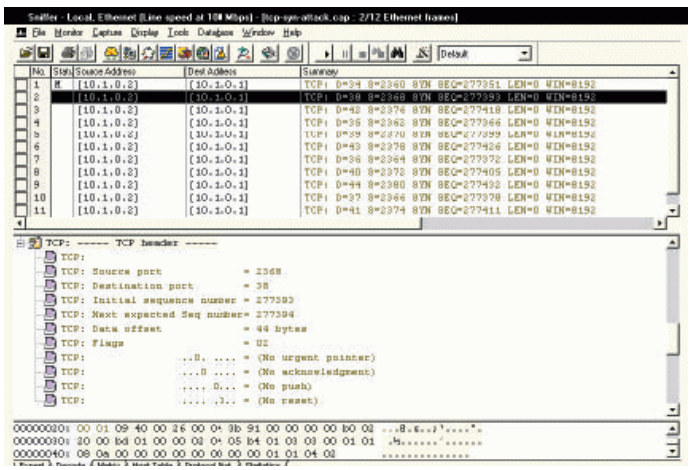
Evidence

17

17

Challenges for judges & prosecutors

Electronic evidence



18

Challenges for judges & prosecutors

Many different kind of devices

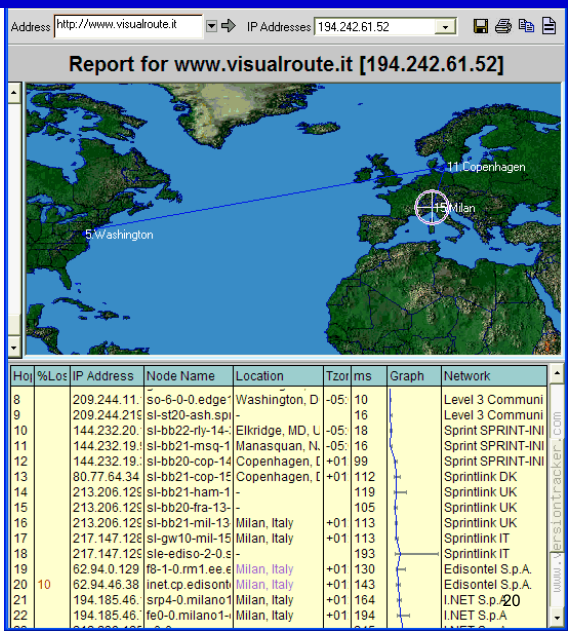
19

19

Challenges for judges & prosecutors

Electronic evidence is volatile evidence

- need for efficient, urgent measures



20

20

Challenges for judges & prosecutors

Electronic evidence

- Any data obtained from an electronic device or digital mean that serves to establish the existence of a matter of fact (01000110)
- Many different types of devices
- Large amounts of data on small storage devices
- Intangible evidence
- Integrity and preservation of evidence
- Specialised knowledge needed for analysis and interpretation
- Volatile evidence

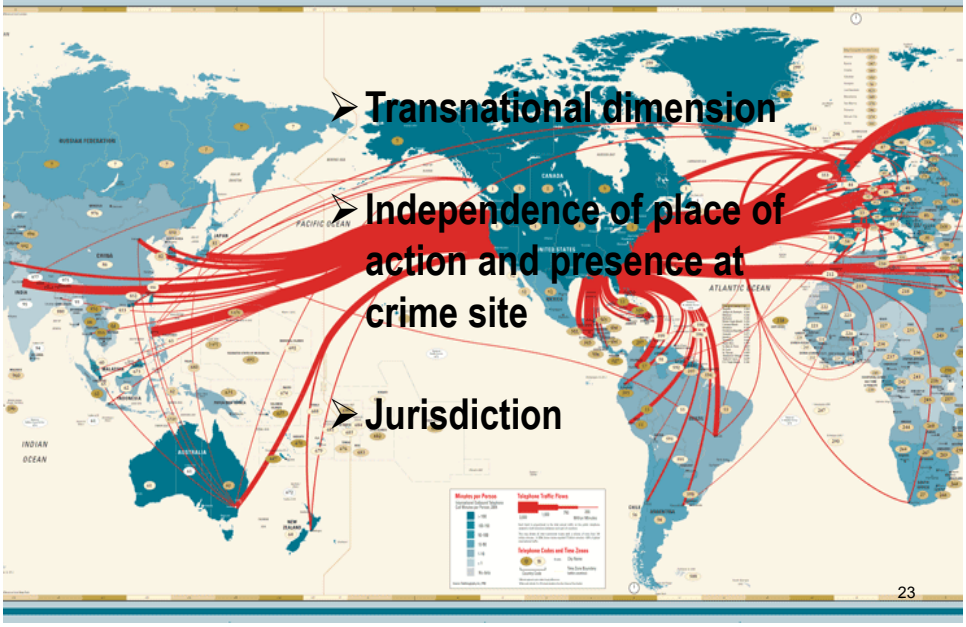
➢"traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service

21

Challenges for judges & prosecutors

22

Challenges for judges & prosecutors



23

Follow the money

24

Challenges for judges & prosecutors

Law enforcement – private sector cooperation

Why law enforcement authorities (LEA) / Internet service provider (ISP) cooperation is necessary:

- Information society dependend on ICT - vulnerable to cybercrime - Need to enhance security of ICT
- LEA and ISP play crucial role in a secure Internet
- LEA investigations often not possible without ISP cooperation
- Ensure efficient work of LEA
- Protect ability of ISP to provide services
- Ensure due process
- Protect rights of users
- How to enhance, how to structure cooperation?
- Guidelines for cooperation (Strasbourg, April 2008)

25

25

Challenges for judges & prosecutors

Security concerns and freedom rights:

- a question of balance?

German Constitutional Court February 2008: Confidentiality and integrity of computer data and systems a basic right

26

26

Challenges for judges & prosecutors

Resources, skills, training, specialisation

27

27

Challenges for judges & prosecutors

How will judges and prosecutors deal with these challenges?

28

28

Global Octopus Conference

Strasbourg, 10-11 March 2009

Legislation: Criminalising child pornography

Effectiveness of international cooperation against cybercrime

Training resources for law enforcement, prosecutors, judges and industry

Follow the money on the internet

29

29

Thank you

Alexander.seger@coe.int

30

30