COUNCIL OF EUROPE CONSEIL DE L'EUROPE

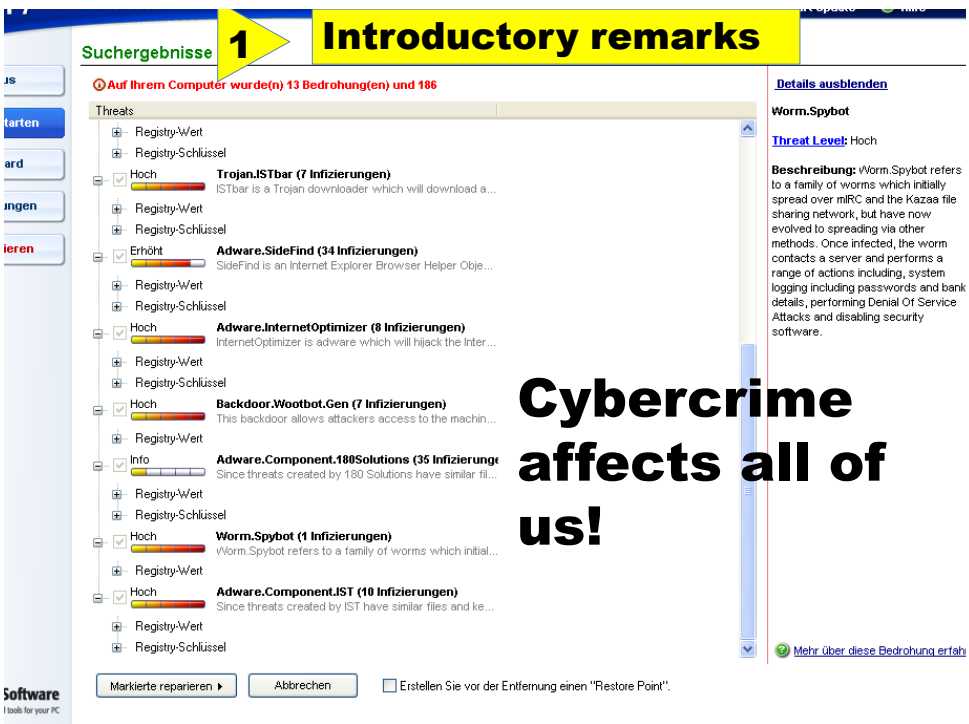
www.coe.int/cybercrime

The threat of cybercrime – challenges for Cambodia

Workshop on cybercrime – Phnom Penh, July 2010

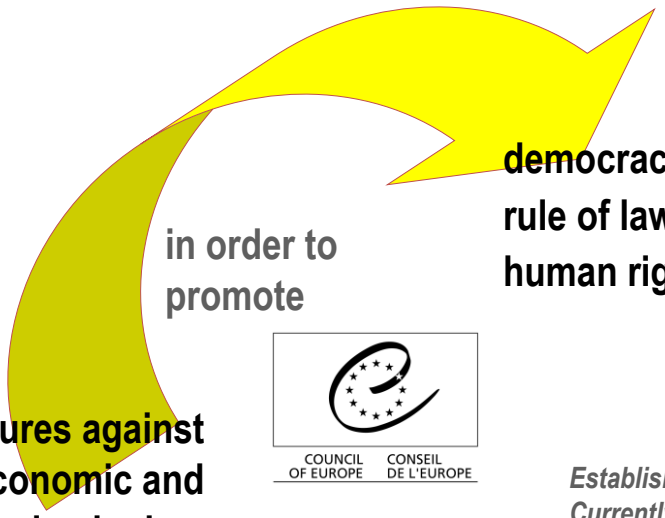
Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

1



2

About the Council of Europe … www.coe.int



Established in 1949
Currently 47
member States

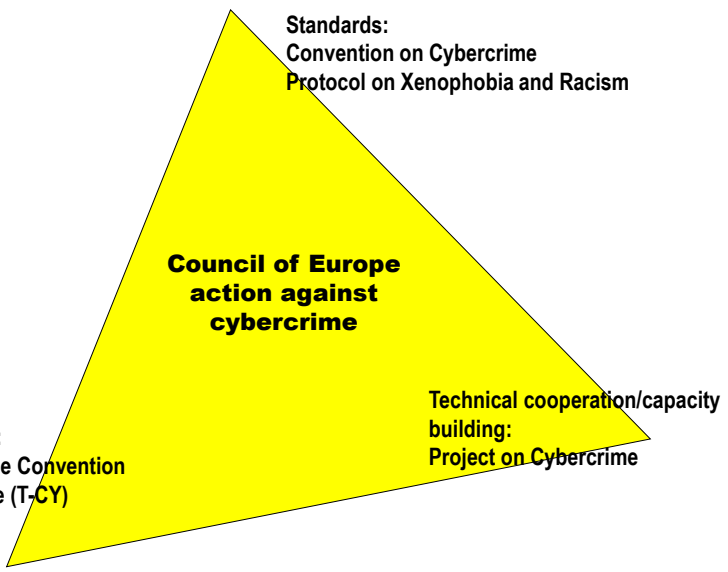
3

www.coe.int/cybercrime

3

3

The Council of Europe approach against cybercrime



www.coe.int/cybercrime

4

4

2 Why worry about cybercrime?

- Opportunities provided by information and communication technologies
- ICT for development, democracy, rule of law, human rights
- 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

Important considerations:

Enhancing trust and security/measures against cybercrime -> build into development cooperation

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

3 What is cybercrime?

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

What is cybercrime?

Malware

- 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

Phishing and other forms of identity theft

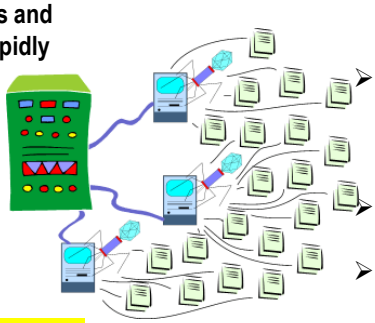
SPAM

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



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

What is cybercrime?

Terrorist use of the internet/ICT

Cross-cutting issues

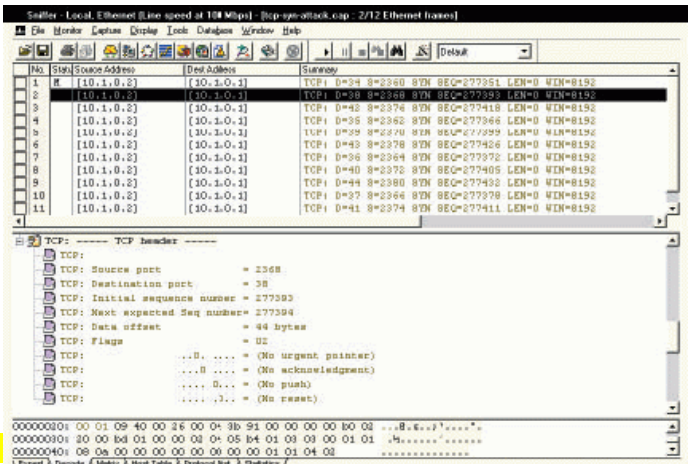
- Possible attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interests, including loss of life
- Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism, recruitment or training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

4 Investigating, prosecuting, adjudicating cybercrime: challenges

Evidence

Investigating, prosecuting, adjudicating cybercrime: challenges

Electronic evidence



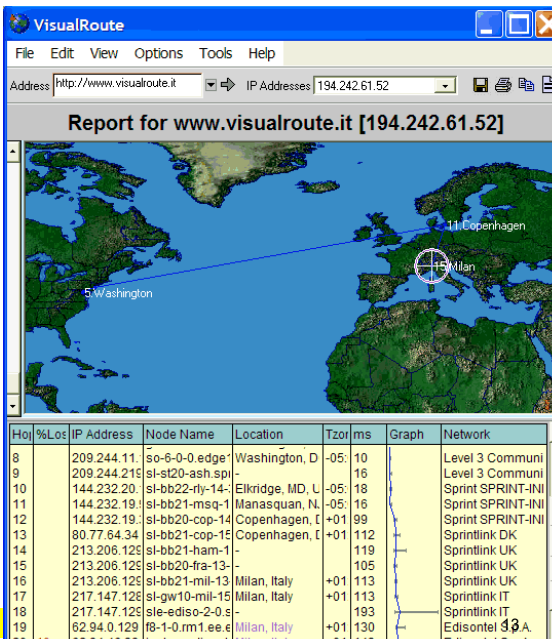
Investigating, prosecuting, adjudicating cybercrime: challenges

Many different kind of devices

Investigating, prosecuting, adjudicating cybercrime: challenges

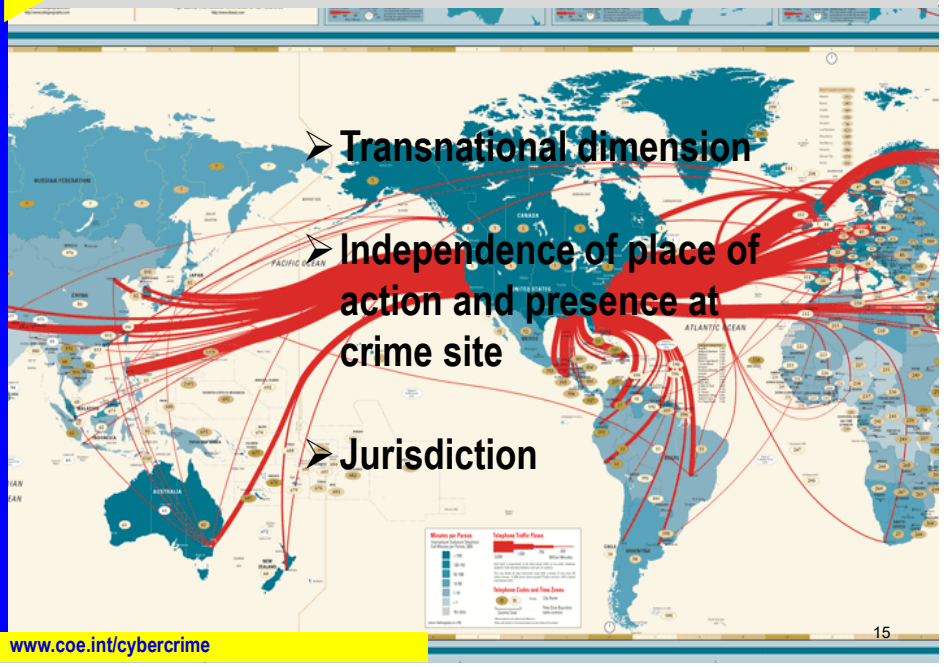
Electronic evidence is volatile evidence

➢ need for efficient, urgent measures



5 More challenges: cybercrime as transnational crime

More challenges: cybercrime as transnational crime



www.coe.int/cybercrime

15

15

6 Strategic considerations/way ahead

1. Legislation (based on Budapest Convention)
   - Criminalise conduct
   - Procedural law/tools for investigation
   - Safeguards
2. High-tech crime unit - Specialisation (law enforcement/criminal justice)
3. Law enforcement training
4. Judicial training (judges, prosecutors)
5. Public-private (LEA-ISP) cooperation
6. Effective international cooperation
7. Protection of children
8. Data protection

www.coe.int/cybercrime

16

16

Thank you

Alexander.seger@coe.int

17