



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

**1 Introductory remarks**

**Suchergebnisse** ⊙ Auf Ihrem Computer wurde(n) 13 Bedrohung(en) und 186

**Threats**

- Registry-Wert  
 Registry-Schlüssel  
 **Hoch** Trojan.ISTbar (7 Infizierungen)  
ISTbar is a Trojan downloader which will download a...
- Registry-Wert  
 Registry-Schlüssel  
 **Erhöht** Adware.SideFind (34 Infizierungen)  
SideFind is an Internet Explorer Browser Helper Obj...
- Registry-Wert  
 Registry-Schlüssel  
 **Hoch** Adware.InternetOptimizer (8 Infizierungen)  
InternetOptimizer is adware which will hijack the Inter...
- Registry-Wert  
 Registry-Schlüssel  
 **Hoch** Backdoor.Wootbot.Gen (7 Infizierungen)  
This backdoor allows attackers access to the machin...
- Registry-Wert  
 Registry-Schlüssel  
 **Info** Adware.Component.180Solutions (35 Infizierunge  
Since threats created by 180 Solutions have similar fil...
- Registry-Wert  
 Registry-Schlüssel  
 **Hoch** Worm.Spybot (1 Infizierungen)  
Worm.Spybot refers to a family of worms which initial...
- Registry-Wert  
 Registry-Schlüssel  
 **Hoch** Adware.Component.IST (10 Infizierungen)  
Since threats created by IST have similar files and ke...

[Details ausblenden](#)  
**Worm.Spybot**  
**Threat Level:** Hoch  
**Beschreibung:** Worm.Spybot refers to a family of worms which initially spread over mIRC and the Kazaa file sharing network, but have now evolved to spreading via other methods. Once infected, the worm contacts a server and performs a range of actions including, system logging including passwords and bank details, performing Denial Of Service Attacks and disabling security software.

[Mehr über diese Bedrohung erfah...](#)

Markierte reparieren   Erstellen Sie vor der Entfernung einen "Restore Point".

**Cybercrime affects all of us!**

2

**About the Council of Europe ... [www.coe.int](http://www.coe.int)**

**Measures against economic and organised crime**

in order to promote

**democracy  
rule of law  
human rights**



COUNCIL OF EUROPE    CONSEIL DE L'EUROPE

*Established in 1949  
Currently 47  
member States*

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

3

**The Council of Europe approach against cybercrime**

Standards:  
Convention on Cybercrime  
Protocol on Xenophobia and Racism

**Council of Europe  
action against  
cybercrime**

Follow up:  
Cybercrime Convention  
Committee (T-CY)

Technical cooperation/capacity  
building:  
Project on Cybercrime

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

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

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

5<sup>5</sup>

5

## 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

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

6

6

## 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

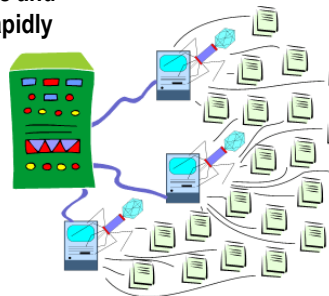
### SPAM

### 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



[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

7

## 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

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

8

8

## 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

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

9

9

4

## Investigating, prosecuting, adjudicating cybercrime: challenges

### Evidence



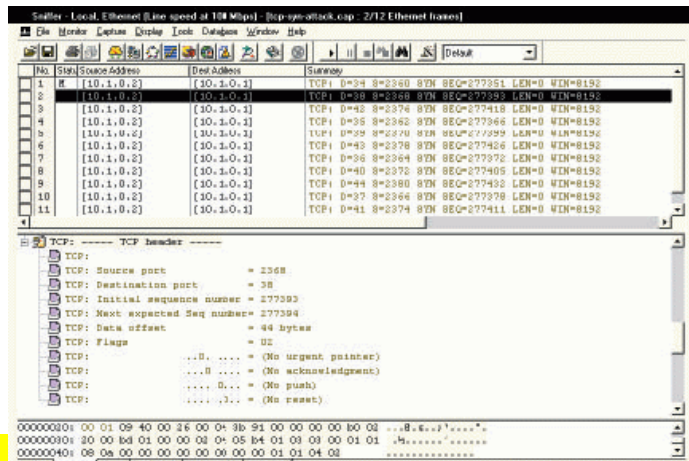
[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

10

10

# Investigating, prosecuting, adjudicating cybercrime: challenges

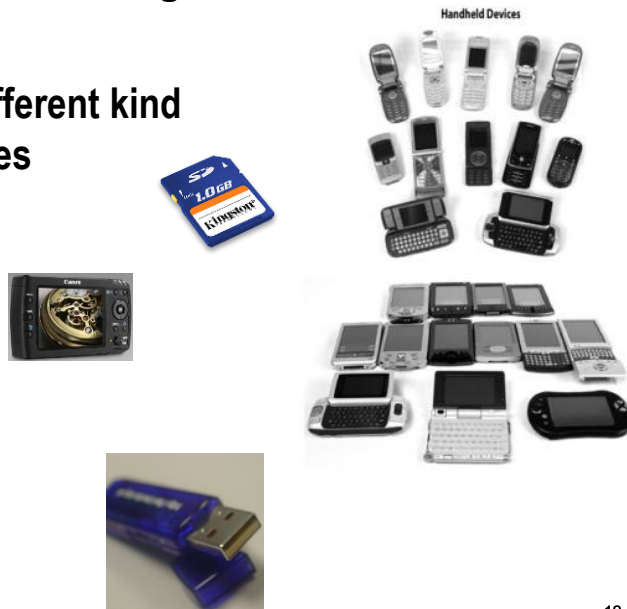
## Electronic evidence



[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

# Investigating, prosecuting, adjudicating cybercrime: challenges

## Many different kind of devices

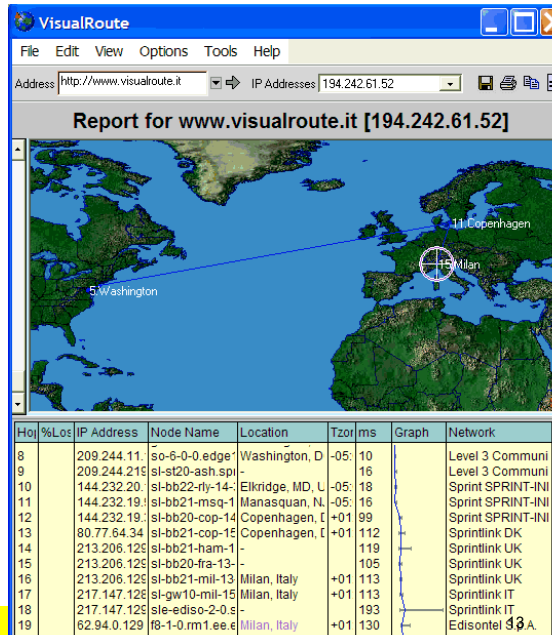


[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

**Investigating, prosecuting, adjudicating  
cybercrime: challenges**

**Electronic  
evidence is volatile  
evidence**

- need for  
efficient, urgent  
measures



[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

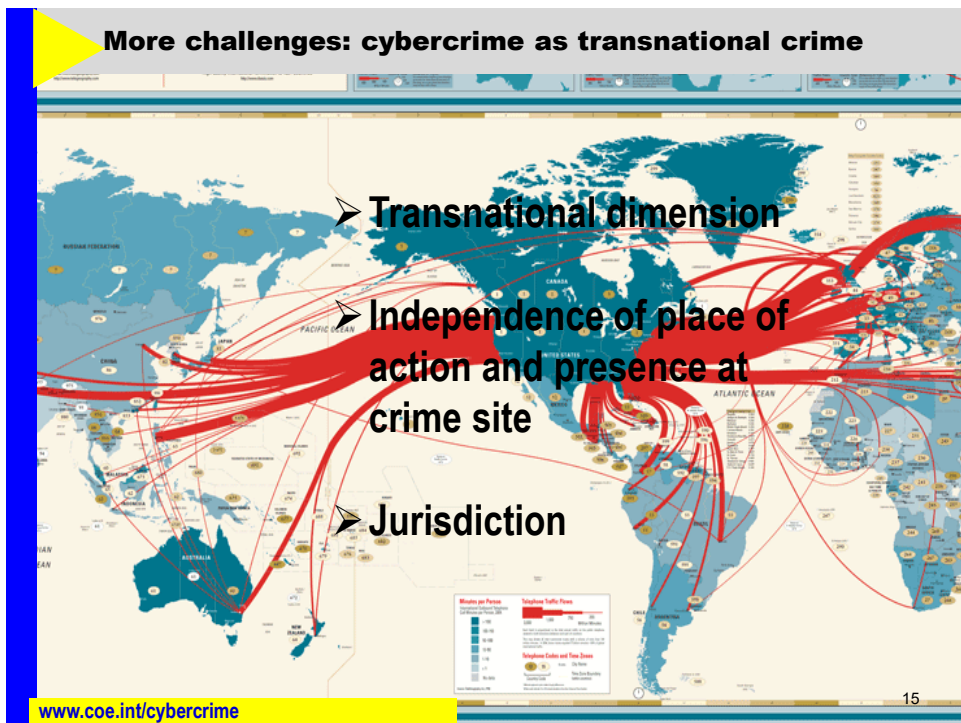
13

**5 More challenges: cybercrime as  
transnational crime**



[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

14



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](http://www.coe.int/cybercrime)

1  
6

16



**Thank you**

**Alexander.seger@coe.int**

