



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

***PROSECO & PROJECT ON CYBERCRIME:***

***Applying cybercrime legislation  
in Albania***

*Workshop, Duress, Albania, 16-17 April 2009*

Alexander Seger  
Council of Europe,  
Strasbourg, France  
Tel +33-3-9021-4506  
[alexander.seger@coe.int](mailto:alexander.seger@coe.int)

1

[Session 1: Cybercrime: what is the issue?](#)

[Session 2: Substantive law: what offence?](#)

[Session 4: Procedural measures and investigative tools](#)

[Session 5: International cooperation](#)

2

2

# 1 Cybercrime: what is the issue?

- 1.1 Why worry about cybercrime?
- 1.2 What is cybercrime?
- 1.3 Challenges for judges, prosecutors, law enforcement

3

**Preliminary remarks**

Suchergebnisse

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

Threats

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

**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 erfahren](#)

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

**Software**  
tools for your PC

**Cybercrime  
affects all of  
us!**

4

## 1.1 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

## 1.2 What is cybercrime?



6

6

## ▶ **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**

---

**Cross-cutting issues and combination of offences**

---

**AND: evidence on a computer system**

---

7

7

## **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**

8

8

## 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.

9

9

## What is cybercrime?

### 3. Content-related offences

- Child pornography
- Xenophobia, racism, hate speech

**Issue:**

- Security and protection versus freedom of expression

10

10

## 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

11

11

## What is cybercrime?

### Malware

### Cross-cutting/ Key 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

12

12

## What is cybercrime?

### SPAM

### Cross-cutting/ Key issues

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

13

13

## What is cybercrime?

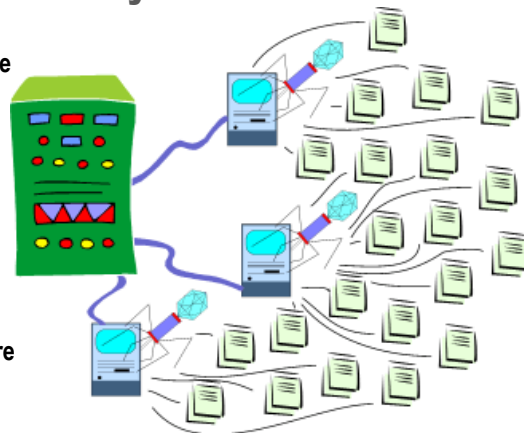
### Bots and botnets

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

### Cross-cutting/ Key issues



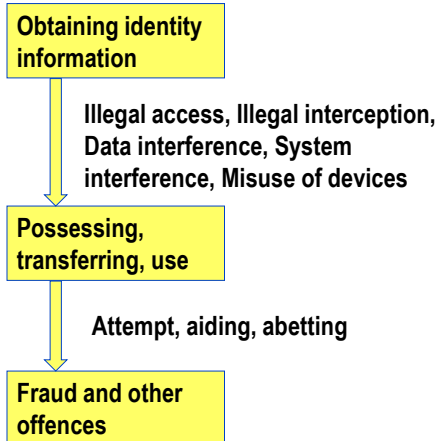
14

14

## What is cybercrime?

### Cross-cutting/ Key issues

### Phishing and other forms of identity theft



15

15

## What is cybercrime?

### Cross-cutting/ Key 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

16

16

## What is cybercrime?

### Terrorist use of the internet/ICT

### Cross-cutting/ Key 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

17

17

## 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?*

18

18

# 1.3 Investigating, prosecuting, adjudicating cybercrime: challenges

## Evidence

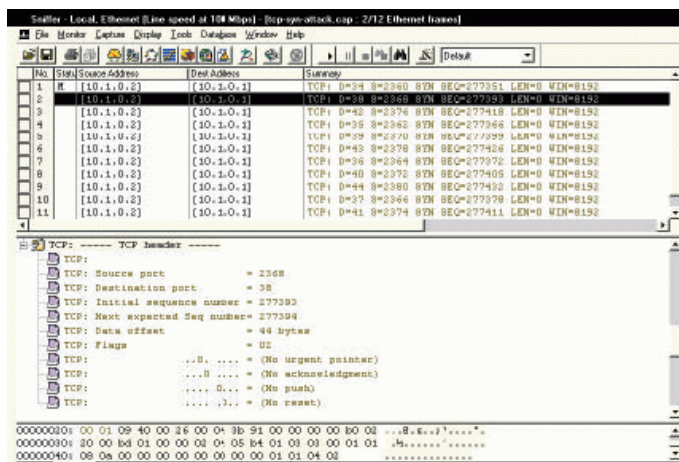


19

19

## Challenges

## Electronic evidence

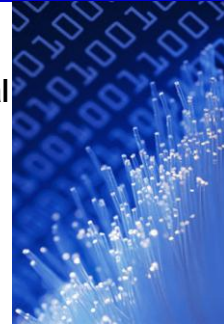


20

## Challenges

### 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

### Many different kind of devices

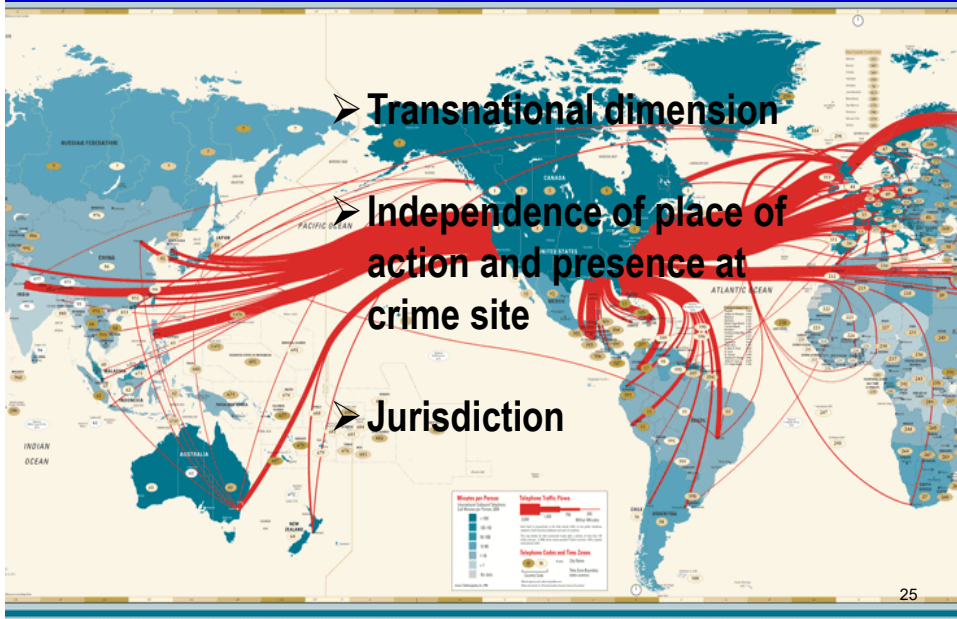


22

22



## Challenges



25

## Challenges

### 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)

26

26

## Challenges

**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**

27

27

## Challenges

**Resources, skills, training, specialisation**

28

28

## Challenges

How will judges, prosecutors and law enforcement deal with these challenges?

29

29

## 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

30

30

## 2 Applying substantive law: what is the offence?

Legislation to deal with – as a minimum:

	Convention	Albanian legislation
Illegal access to a computer system	Art 2	192/b
Illegal interception	Art 3	293/a CC
Data interference	Art 4	293/b CC
System interference	Art 5	293/c CC
Misuse of devices	Art 6	293/d CC
Computer-related forgery and fraud	Art 7+8	186/a, 143/b CC
Child pornography,	Art 9	117 CC
xenophobia, racism	Protocol	74/a, 84/a, 119a CC
Infringement of copyright and related rights	Art 10	148, 149 CC and Law on copyright

31

31

## 4 Procedural law measures and investigative tools

Legislation to provide for – as a minimum:

	Convention	Albanian legislation
Expedited preservation of stored computer data	Art 16	299/a CPC
Expedited preservation and partial disclosure of traffic data	Art 17	299/b CPC
Production order	Art 18	191/a CPC
Search and seizure of stored computer data	Art 19	202/a CPC
Real-time collection of traffic data	Art 20	
Interception of content data	Art 21	221, 222
Procedural safeguards	Art 15	221, 222

Scope: Do provisions on evidence generally apply to electronic evidence?

32

32

## 5 International cooperation

### The Budapest Convention on Cybercrime

- Substantive criminal law: criminalising conduct
  - Procedural measures: expedited preservation, production order, search and seizure, interception of data
  - International cooperation
- Opened for signature in Budapest in November 2001
  - Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA
  - CCC common standard: used in 100+ countries world wide

### The Protocol on Xenophobia and Racism Committed through Computer Systems

33

33

## International cooperation

### Structure and content of the Convention

#### Chapter I: Definitions

#### Chapter II: Measures at national level

Section 1 - Substantive criminal law (offences to be criminalised)

Section 2 - Procedural law

Section 3 - Jurisdiction

#### Chapter III: International cooperation

Section 1 - General principles

Section 2 - Specific provisions

#### Chapter IV: Final provisions

34

34

## **Chapter III - International cooperation**

Legal and institutional basis for

- Expedited, urgent measures
- Legal cooperation in cybercrime matters

35

35

## **Chapter III - International cooperation**

### **Section 1 – General principles**

- Art 23 General principles on international cooperation
- Art 24 Principles related to extradition
- Art 25 Principles related to mutual legal assistance
- Art 26 Spontaneous information
- Art 27 MLA in the absence of applicable international instruments
- Art 28 Confidentiality and limitation on use

- Legal provisions in Albania?
- Competent authorities for extradition + mutual legal assistance
- Possibilities for direct contacts?

36

36

## International cooperation

Possibilities for direct contacts? See:

*2nd Additional Protocol to the Convention on Mutual Legal Assistance (ETS 182)*

### Article 4 – Channels of communication

Article 15 of the Convention shall be replaced by the following provisions:

1 Requests for mutual assistance, as well as spontaneous information, shall be addressed in writing by the Ministry of Justice of the requesting Party to the Ministry of Justice of the requested Party and shall be returned through the same channels. However, they may be forwarded directly by the judicial authorities of the requesting Party to the judicial authorities of the requested Party and returned through the same channels...

9 Requests for mutual assistance and any other communications under this Convention or its Protocols may be forwarded through any electronic or other means of telecommunication provided that the requesting Party is prepared, upon request, to produce at any time a written record of it and the original.... <sup>37</sup>

37

## International cooperation

### Chapter III - International cooperation...

#### Section 2 – Specific provisions

- Art 29 - Expedited preservation of stored computer data
- 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

Provisions in national legislation?  
 Authorities responsible in Albania?  
 Experience?

- Art 35 - 24/7 network

38

38

## **International cooperation**

### **Article 35 – 24/7 Network**

Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

- a the provision of technical advice;
- b the preservation of data pursuant to Articles 29 and 30;
- c the collection of evidence, the provision of legal information, and locating of suspects.

39

39

## **International cooperation**

Article 35 cont'd

**2 a** A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

**b** If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

**3** Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

40

40

**International cooperation****Functioning of the contact point in  
Albania:**

- **Set up and authority**
- **Experience**
- **Interaction with authorities for  
MLA**

41

41

**Thank you****Alexander.seger@coe.int**  


42

42