



# La amenaza del Cibercrimen

América Latina: Taller Regional en Cibercrimen  
Ciudad de México, 26 y 27 de Agosto 2010

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

1

**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 (2 Infizierungen)**  
This backdoor allows attackers access to the machin...
- Registry-Wert
- Info Adware.Component.1805 (1 Infizierung)**  
Since threats created by 1805...
- Registry-Wert
- Registry-Schlüssel
- Hoch Worm.Spybot (1 Infizierung)**  
Worm.Spybot refers to a family of worms which initial...
- Registry-Wert
- Hoch Adware.Component.IST (10 Infizierungen)**  
Since threats created by IST have similar files and ke...
- Registry-Wert
- Registry-Schlüssel

**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 erfahren](#)

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

2

## Sobre el Consejo de Europa ... [www.coe.int](http://www.coe.int)

Estrategia  
contra el delito  
económico

para  
promover

La democracia  
El Estado de  
derecho  
Los derechos  
humanos

Medidas contra el  
delito económico y el  
crimen organizado



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

3 3 3

3

## El enfoque contra la ciberdelincuencia

### Elaborar normas

Convenio sobre la ciberdelincuencia (STE 185)  
Protocolo relativo a la penalización de actos de  
naturaleza racista y xenófoba (STE 189)

Ciberdelincuencia

### Velar por el cumplimiento

Consultas de las Partes sobre el  
STE 185 (T-CY)

### Cooperación técnica

Prestar apoyo a través de un proyecto mundial sobre  
la ciberdelincuencia

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

4

4

## 1 Cibercrimen?

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos
  - Acceso ilícito
  - Interceptación ilícita
  - Ataques a la integridad de los datos
  - Ataques a la integridad del sistema
  - Abuso de los dispositivos
2. Estafa informática, Falsedad informática
3. Delitos relacionados con el contenido (Infracciones relativas a la pornografía infantil)
4. Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

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

5

5

## Cibercrimen?

### Case study: Targeting online banking customers (Source: M86 Security)

1. Criminals infect legitimate website/malicious adverts
  2. Users accessing sites are redirected to a site from where an exploit kit is downloaded
  3. Trojan horse is downloaded to the user's computer
  4. User computer is an externally controlled bot (robot, zombie)
  5. User access bank account online; Trojan transfers login and other credentials to CC server
  6. Data of bank transaction form is sent to CC server, instead of bank
  7. System of CC servers decrypts information and selects a mule account
  8. Trojan receives instructions to send an updated transaction form to bank to transfer money to a mule account
- = £ 675,000 stolen in July/August 2010
- Illegal access, illegal interception, data and system interference, forgery and fraud
  - Organised criminals and use of money mules

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

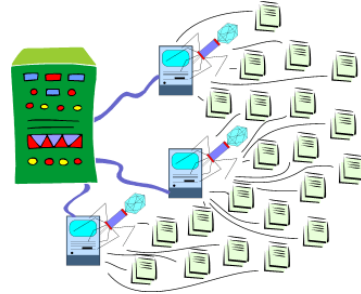
6

6

## Cibercrimen?

### Situation, trends and infrastructure

- Malware
- Botnets
- Underground economy
- Criminal domains
- Social networking platforms
- Cyberwarfare, „hactivism“, espionage, terrorism
- Organised crime
- Cybercrime aimed at proceeds (fraud)



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

7

7

## 2 Investigating, prosecuting, adjudicating cybercrime: challenges

### Evidence



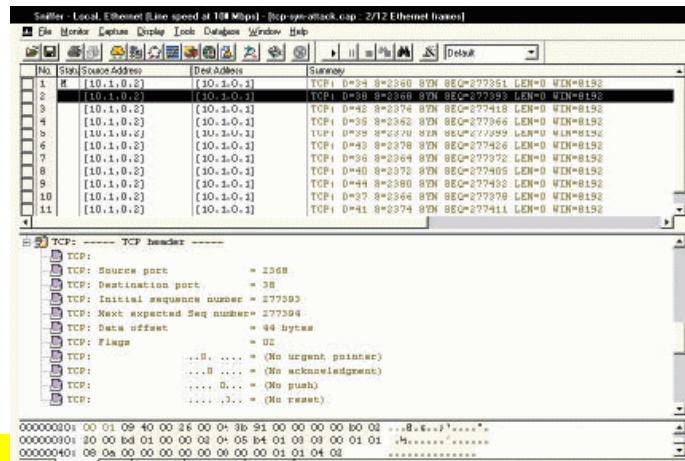
[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

8

8

# Investigating, prosecuting, adjudicating cybercrime: challenges

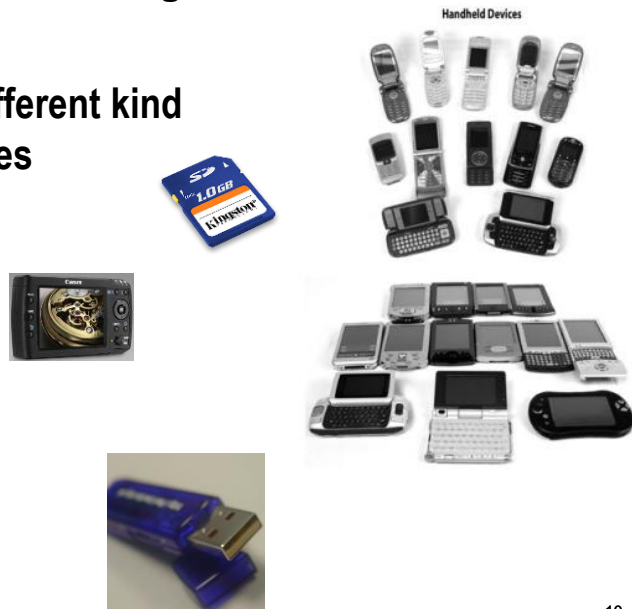
## Electronic evidence



[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

Hop	%Loss	IP Address	Node Name	Location	Tz	ms	Graph	Network
8		209.244.11	so-6-0-0.edge	Washington, D	-05	10		Level 3 Communi
9		209.244.216	sl-st20-ash.spl			16		Level 3 Communi
10		144.232.20	sl-bb22-ty-14-	Elkridge, MD, U	-05	18		Sprint SPRINT-INT
11		144.232.19	sl-bb21-msq-1	Manasquan, N.	-05	16		Sprint SPRINT-INT
12		144.232.19	sl-bb20-cop-14	Copenhagen, [	+01	99		Sprint SPRINT-INT
13		80.77.64.34	sl-bb21-cop-15	Copenhagen, [	+01	112		Sprintlink DK
14		213.206.129	sl-bb21-ham-1			119		Sprintlink UK
15		213.206.129	sl-bb20-fra-13-			105		Sprintlink UK
16		213.206.129	sl-bb21-mil-13	Milan, Italy	+01	113		Sprintlink UK
17		217.147.128	sl-gw10-mil-15	Milan, Italy	+01	113		Sprintlink IT
18		217.147.128	sl-e-ediso-2-0.s			193		Sprintlink IT
19		62.94.0.129	f8-1-0.rm1.ee.e	Milan, Italy	+01	130		EdisonTel S.p.A.

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

11

**3**

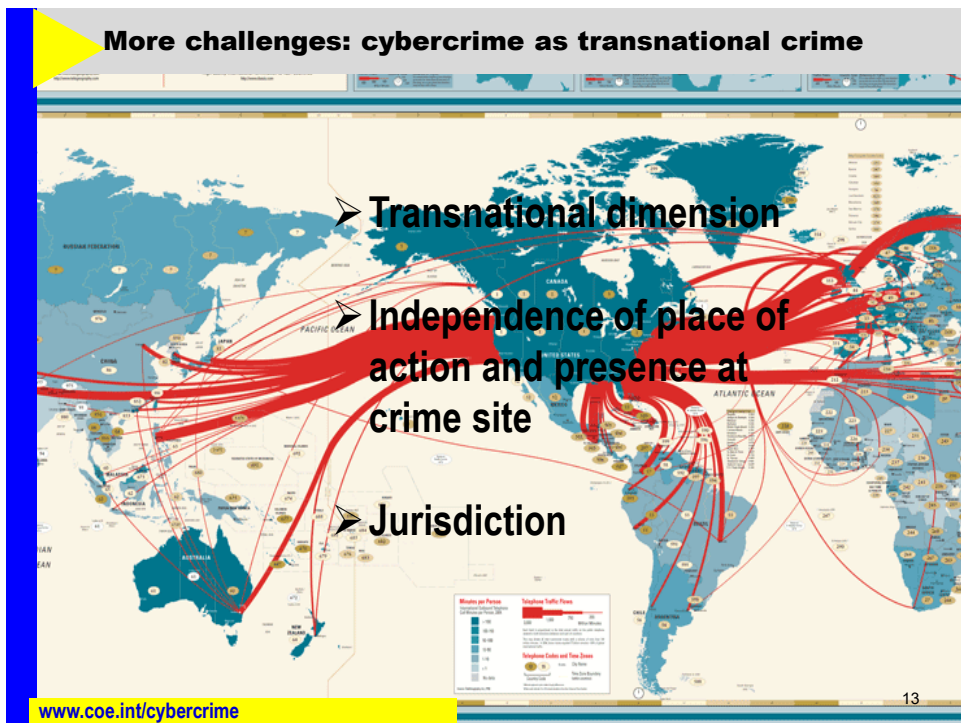
**More challenges: cybercrime as transnational crime**



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

12

12



13

## 4 Una respuesta: El Convenio sobre la ciberdelincuencia

- Penalizar una conducta determinada ► **Derecho penal sustantivo**
- Velar por que las autoridades policiales/la justicia penal tengan medios a su alcance para investigar, juzgar y sentenciar por los ciberdelitos (acciones inmediatas, pruebas electrónicas) ► **Derecho procesal**
- Prever una cooperación internacional eficiente ► armonizar la legislación, elaborar disposiciones y establecer instituciones para la **cooperación policial y judicial**, y concluir o suscribir acuerdos

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

1  
4

14

**Una respuesta: El Convenio sobre la ciberdelincuencia**

Penalizar una conducta determinada ► **Derecho penal sustantivo**

Legislación para tratar – como mínimo:

- Acceso ilícito
- Interceptación ilícita
- Ataques a la integridad de los datos
- Ataques a la integridad del sistema
- Abuso de los dispositivos
- Falsificación informática
- Fraude informático
- Delitos relacionados con la pornografía infantil
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

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

1  
5

15

**Una respuesta: El Convenio sobre la ciberdelincuencia**

Velar por que las autoridades policiales/la justicia penal tengan medios a su alcance para investigar, juzgar y sentenciar por los ciberdelitos (acciones inmediatas, pruebas electrónicas) ► **Derecho procesal**

Legislación para prever – como mínimo:

- Conservación rápida de los datos informáticos almacenados y de los datos relativos al tráfico
- Orden de presentación
- Registro y confiscación de datos informáticos almacenados
- Obtención en tiempo real de datos informáticos (datos de tráfico, interceptación de datos relativos al contenido)
- Condiciones y salvaguardias

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

1  
6

16

**Una respuesta: El Convenio sobre la ciberdelincuencia**

Prever una cooperación internacional eficiente  $\square$  armonizar la legislación, elaborar disposiciones y establecer instituciones para la **cooperación policial y judicial**, y concluir o suscribir acuerdos

**Art. 37 – Adhesión al Convenio para:**

- Cooperación internacional, extradición, etc., en casos de ciberdelincuencia
- Conservación rápida de datos informáticos almacenados y de los datos informáticos conservados
- Asistencia en relación con el acceso a datos informáticos almacenados
- Acceso transfronterizo a datos informáticos almacenados, con consentimiento o cuando sean accesibles al público
- Asistencia para la obtención en tiempo real de datos de tráfico, asistencia en relación con la interceptación de datos relativos al contenido
- Red 24/7

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

1  
7

17



**Thank you**

**Alexander.seger@coe.int**



18