



www.coe.int/cybercrime

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

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

Cibercrimen?

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

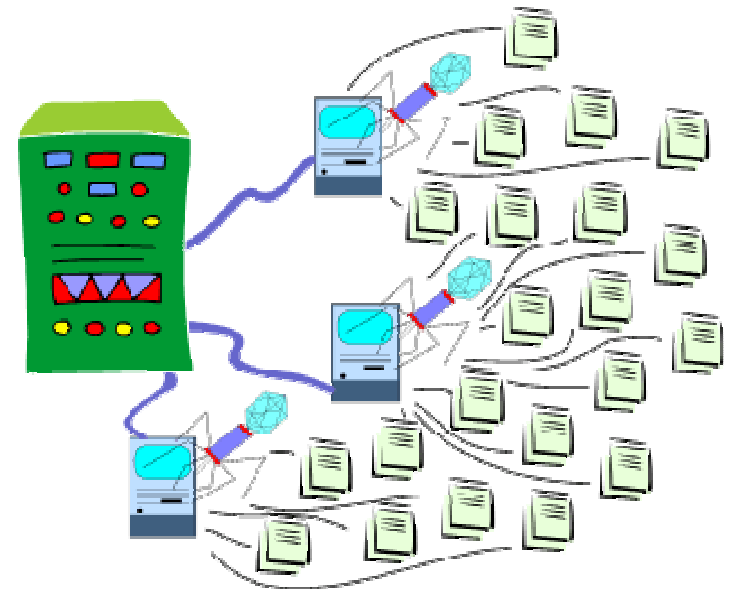
- 1.Criminals infect legitimate website/malicious adverts**
 - 2.Users accessing sites are redirected to a site from where an exploit kit is downloaded**
 - 3.Trojan horse is downloaded to the user`s computer**
 - 4.User computer is an externally controlled bot (robot, zombie)**
 - 5.User access bank 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**

Cibercrimen?

Situation, trends and infrastructure

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



2

Investigating, prosecuting, adjudicating cybercrime: challenges

Evidence



Investigating, prosecuting, adjudicating cybercrime: challenges

Electronic evidence

Sniffer - Local Ethernet (Line speed at 104 Mbps) - [tcp-syn-attack.cap : 2/12 Ethernet frames]

File Monitor Capture Display Tools Database Window Help

No.	Status	Source Address	Dest Address	Summary
1	R	[10.1.0.2]	[10.1.0.1]	TCP: D=34 S=2360 SYN SEQ=277351 LEN=0 WIN=8192
2		[10.1.0.2]	[10.1.0.1]	TCP: D=38 S=2368 SYN SEQ=277393 LEN=0 WIN=8192
3		[10.1.0.2]	[10.1.0.1]	TCP: D=42 S=2376 SYN SEQ=277418 LEN=0 WIN=8192
4		[10.1.0.2]	[10.1.0.1]	TCP: D=36 S=2362 SYN SEQ=277366 LEN=0 WIN=8192
5		[10.1.0.2]	[10.1.0.1]	TCP: D=39 S=2370 SYN SEQ=277399 LEN=0 WIN=8192
6		[10.1.0.2]	[10.1.0.1]	TCP: D=43 S=2378 SYN SEQ=277426 LEN=0 WIN=8192
7		[10.1.0.2]	[10.1.0.1]	TCP: D=36 S=2364 SYN SEQ=277372 LEN=0 WIN=8192
8		[10.1.0.2]	[10.1.0.1]	TCP: D=40 S=2373 SYN SEQ=277405 LEN=0 WIN=8192
9		[10.1.0.2]	[10.1.0.1]	TCP: D=44 S=2380 SYN SEQ=277433 LEN=0 WIN=8192
10		[10.1.0.2]	[10.1.0.1]	TCP: D=37 S=2366 SYN SEQ=277378 LEN=0 WIN=8192
11		[10.1.0.2]	[10.1.0.1]	TCP: D=41 S=2374 SYN SEQ=277411 LEN=0 WIN=8192

TCP: ----- TCP header -----

TCP:

- TCP: Source port = 2368
- TCP: Destination port = 38
- TCP: Initial sequence number = 277393
- TCP: Next expected Seq number = 277394
- TCP: Data offset = 44 bytes
- TCP: Flags = 02
- TCP: ...B... = (No urgent pointer)
- TCP: ...R... = (No acknowledgment)
- TCP:0... = (No push)
- TCP:1... = (No reset)

00000020: 00 01 09 40 00 26 00 04 3b 91 00 00 00 00 00 02 ...B...
00000030: 20 00 04 01 00 00 03 04 05 04 01 09 09 00 01 01 ...H...
00000040: 08 0a 00 00 00 00 00 00 00 00 01 01 04 02

Investigating, prosecuting, adjudicating cybercrime: challenges

Many different kind
of devices



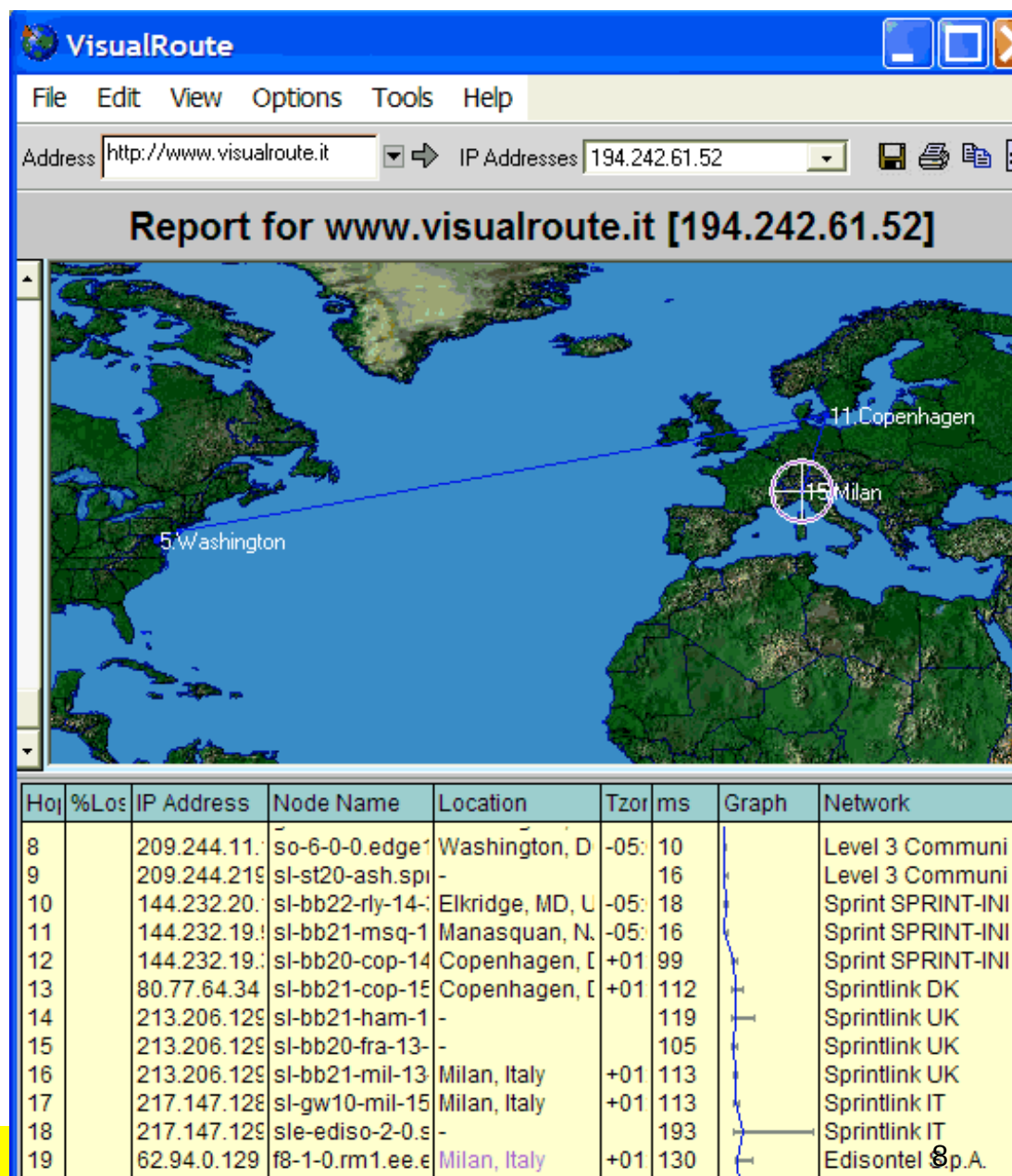
Handheld Devices



Investigating, prosecuting, adjudicating cybercrime: challenges

Electronic
evidence is volatile
evidence

➤ need for efficient,
urgent measures

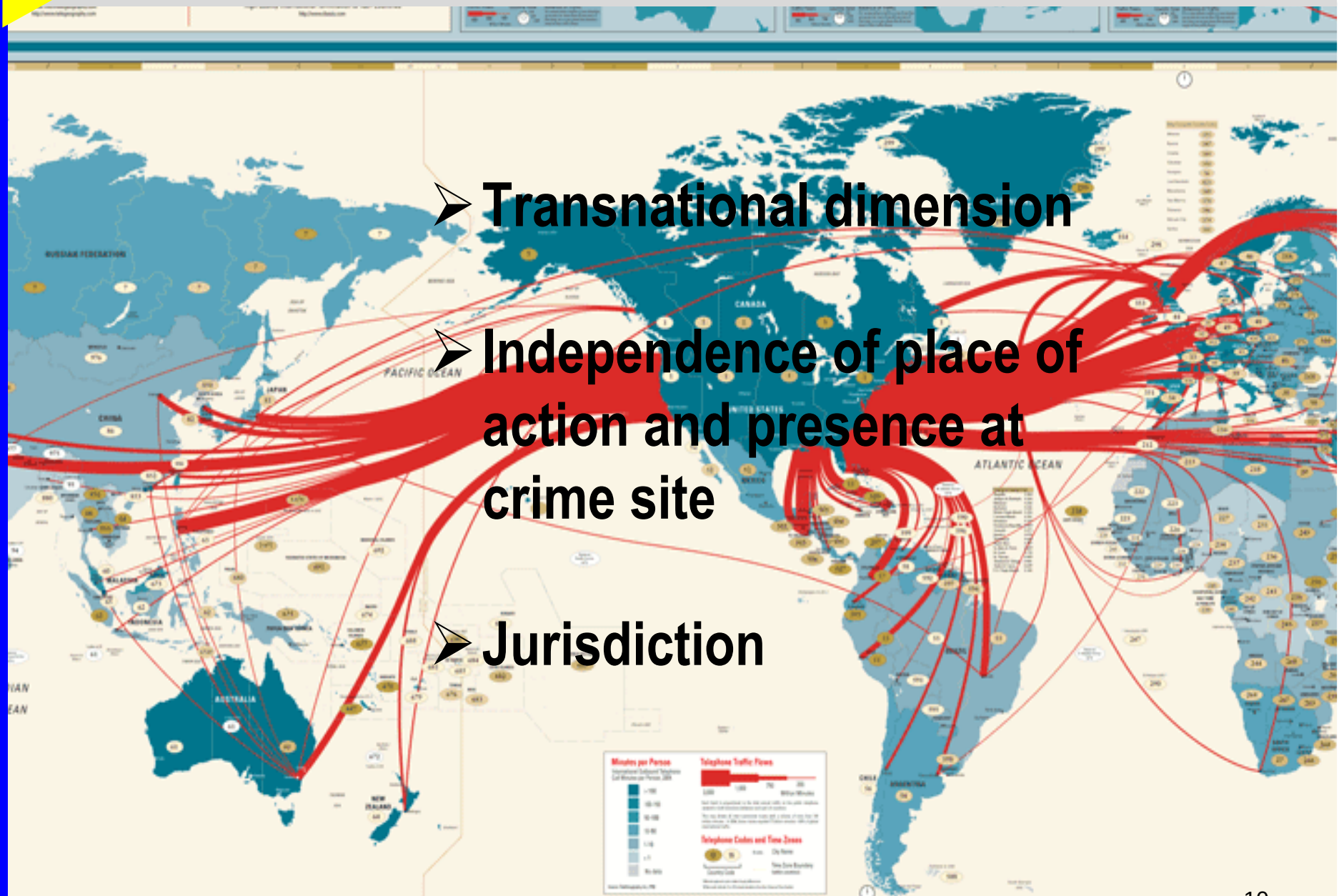


3

More challenges: cybercrime as transnational crime



More challenges: cybercrime as transnational crime



➤ **Transnational dimension**

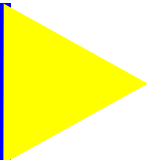
➤ **Independence of place of action and presence at crime site**

➤ **Jurisdiction**

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



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**

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:

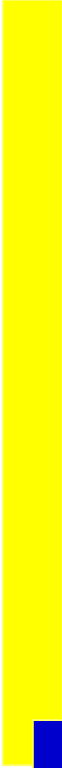
- **Conservación rápida de los datos informáticos almacenados y de los datos relativos al tráfico**
- **Orden de presentación**
- **Registro y confiscación de datos informáticos almacenados**
- **Obtención en tiempo real de datos informáticos (datos de tráfico, interceptación de datos relativos al contenido)**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

Una respuesta: El Convenio sobre la ciberdelincuencia

Prever una cooperación internacional eficiente – 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 ciberlincuencia**
- **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**



Thank you

Alexander.seger@coe.int

