COUNCIL OF EUROPE CONSEIL DE L'EUROPE

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

1 Cibercrimen?

1. Delitos contra la confidencalidad, la integridad y la disponibilidad de las 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?

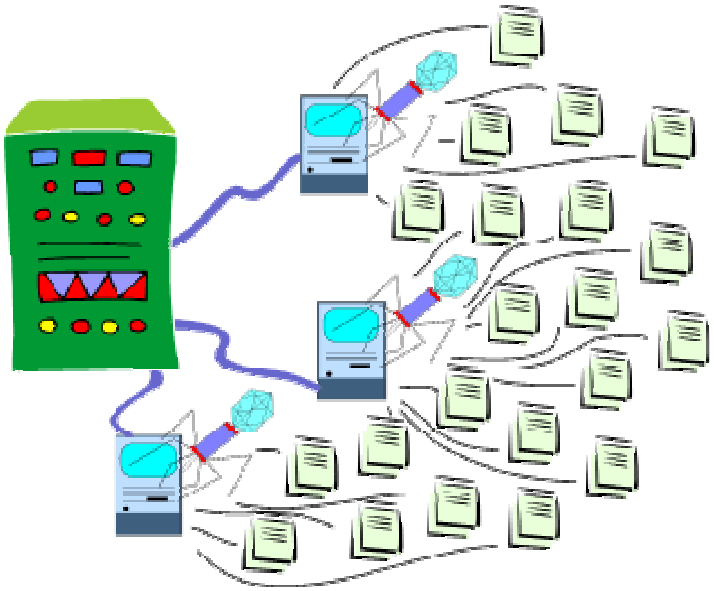
Case study: Targeting online banking customers (Source: M86 Security)

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



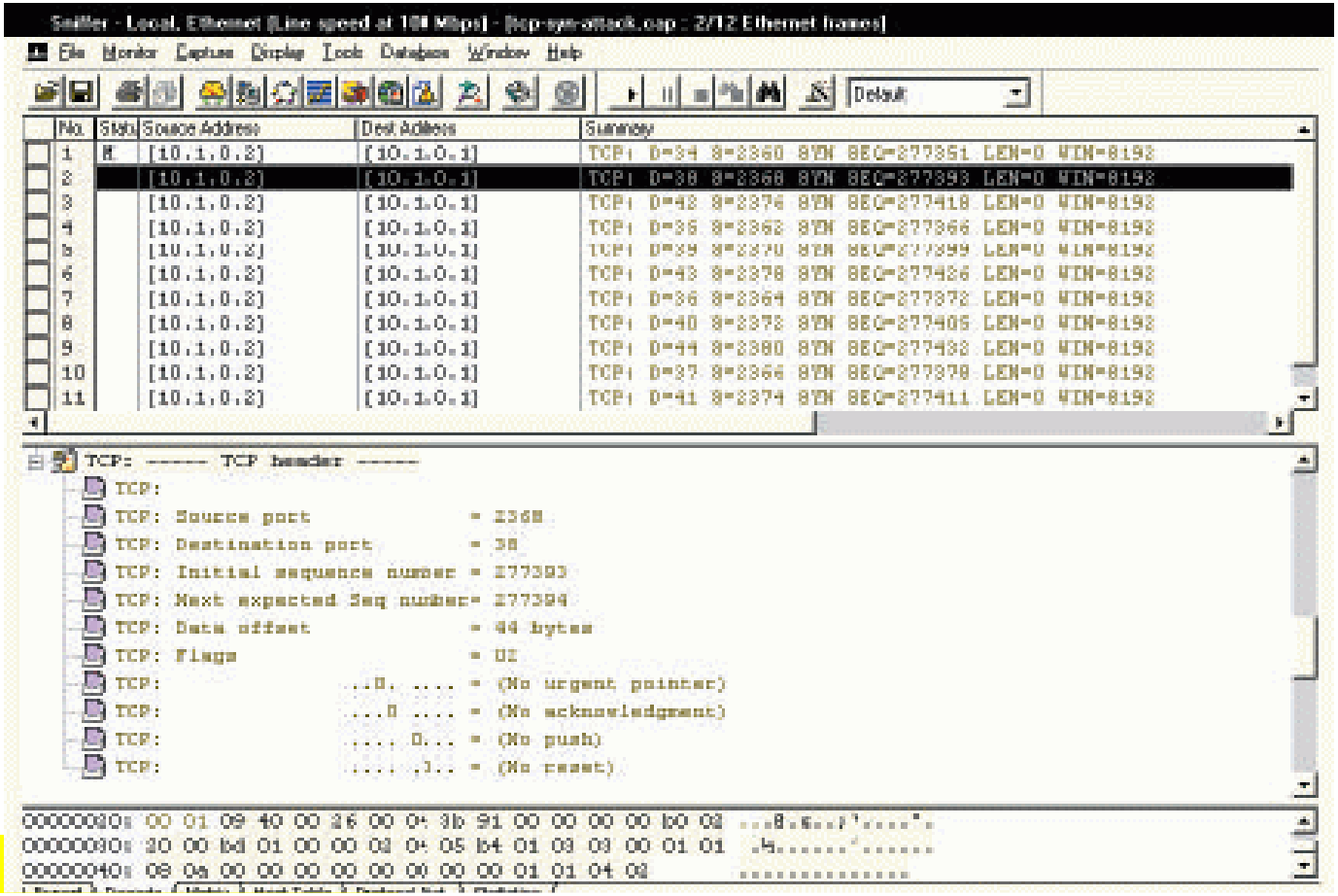
- Malware
- Botnets
- Underground economy
- Criminal domains
- Social networking platforms
- Cyberwarfare, „hacktivism“, espionage, terrorism
- Organised crime
- Cybercrime aimed at proceeds (fraud)

2 Investigating, prosecuting, adjudicating cybercrime: challenges

Evidence

Investigating, prosecuting, adjudicating cybercrime: challenges

Electronic evidence



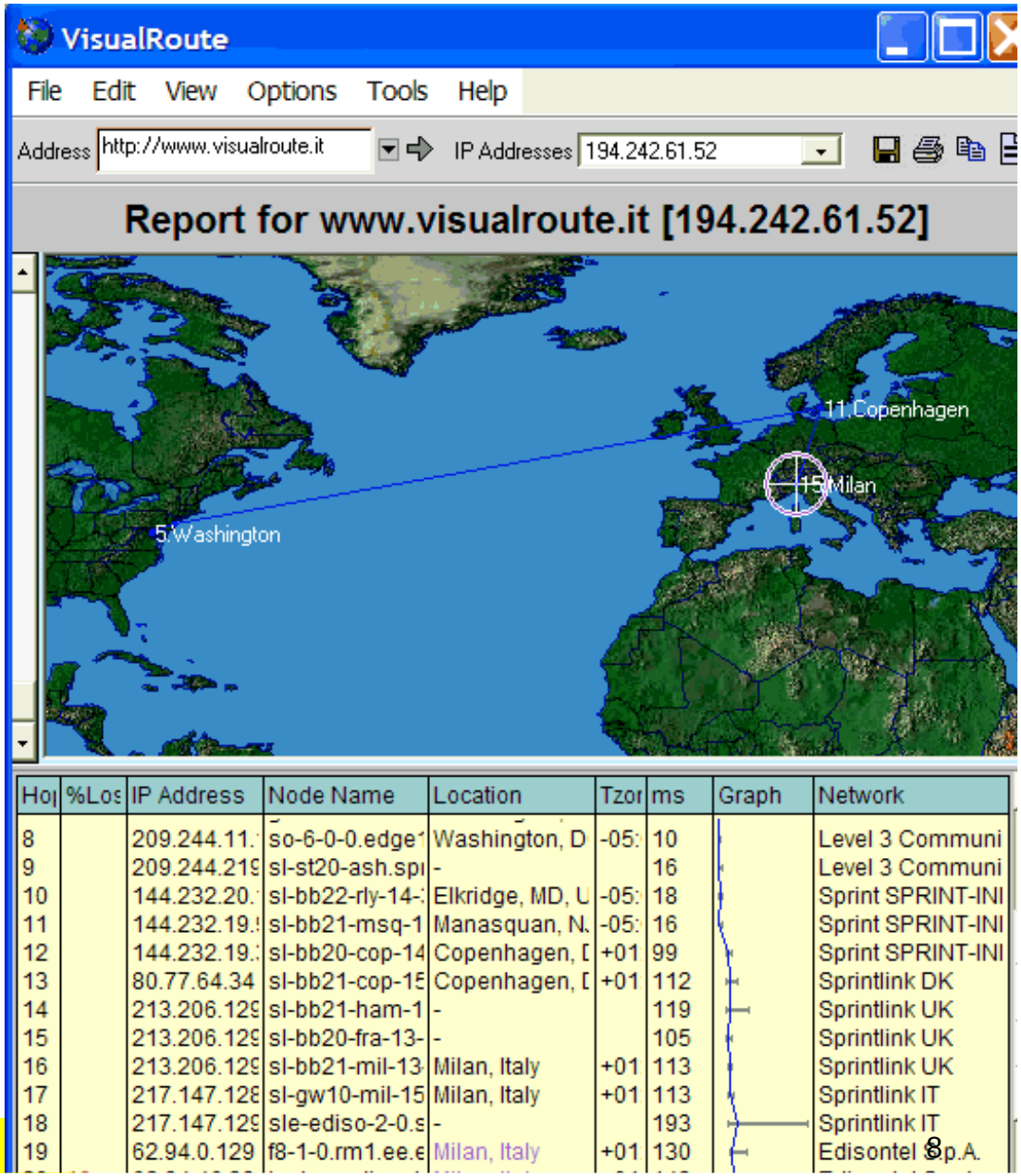
Investigating, prosecuting, adjudicating cybercrime: challenges

Many different kind of devices

Investigating, prosecuting, adjudicating cybercrime: challenges

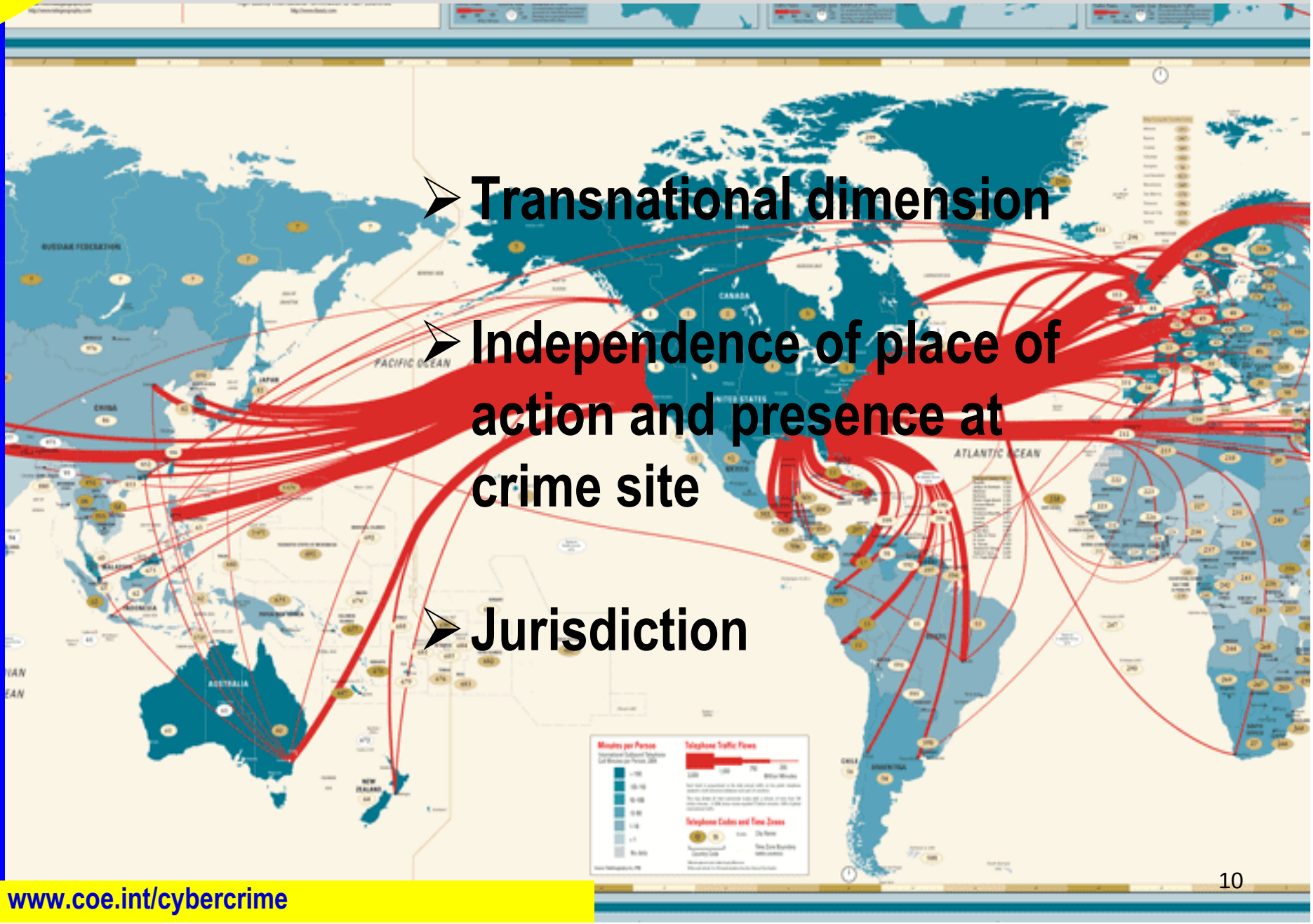
Electronic evidence is volatile evidence

➢need for efficient, urgent measures



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