Workshop
International Cooperation and the Functioning of the 24/7 Network of Contact Points

****

Council of Europe Conference on Cooperation Against Cybercrime

Strasbourg, France

24/7 Network

- "The 24/7 Network for Data Preservation"
  - G8
  - COE Article 35
- Points of contact in participating countries that require **urgent** assistance with investigations involving electronic evidence
- About 56 participating countries from all over the world

2

Preservation and Investigations

- Electronic evidence is often at an ISP
  - An ISP's server may be anywhere in the world
  - Often in the United States
- Working with the ISP
  - Law enforcement point of contact
  - Requests from outside the country
- Data **retention** practices differ
  - ISP policy
  - A country's laws
- Data **preservation** is key step in investigation

3

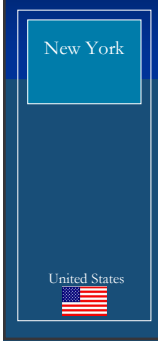
Why a 24/7 Network?

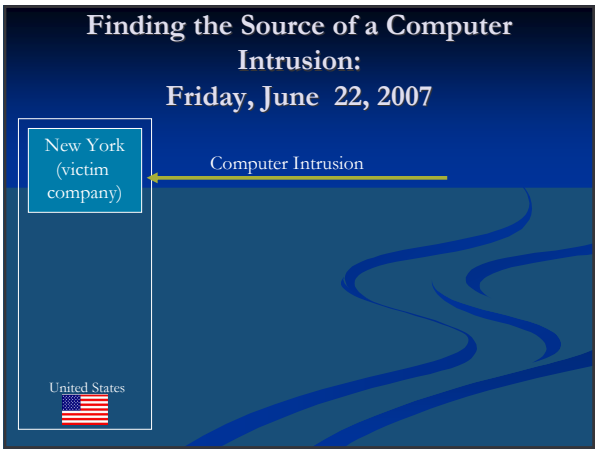
- Importance of timely response to cybercrimes
- Need to find and preserve electronic evidence quickly
  - Data stored on computers and storage devices
  - Data and records kept by ISP
- Need to identify points of contact
  - Law enforcement organization with cyber expertise
  - Knowledge of local laws and procedures

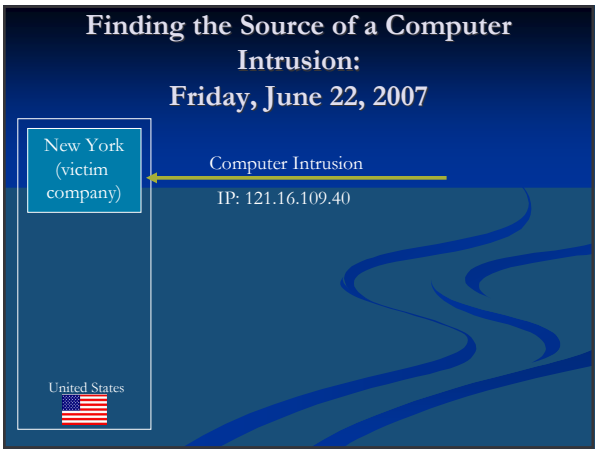
4

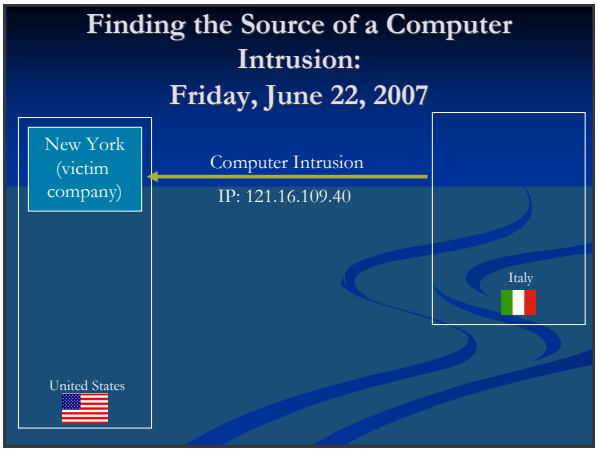
Example: Finding the Source of A Computer Intrusion

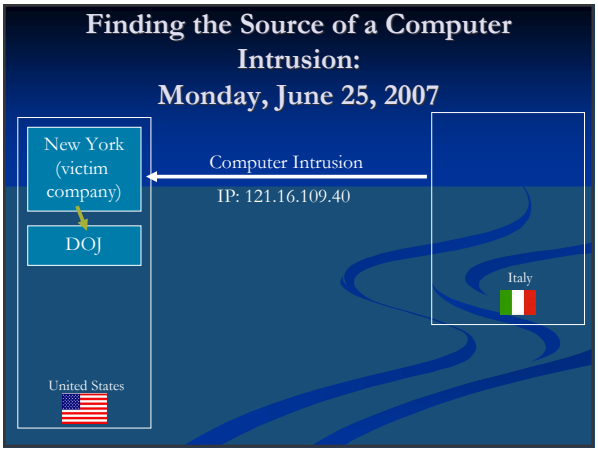
Finding the Source of a Computer Intrusion: Friday, June 22, 2007

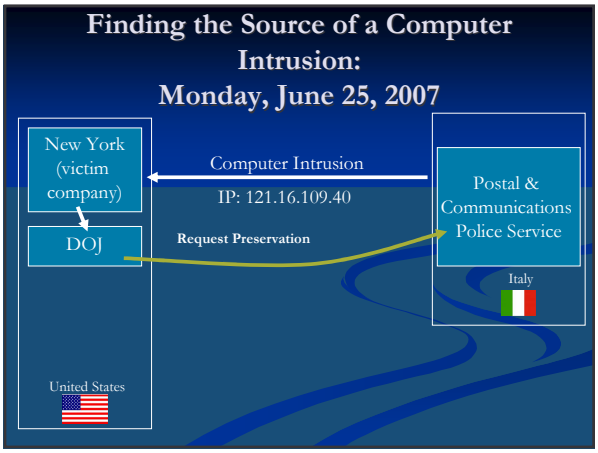


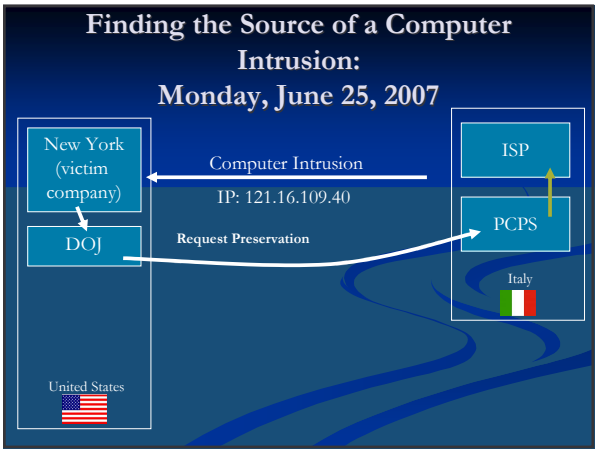

Finding the Source of a Computer Intrusion:
Friday, June 22, 2007
New York (victim company)
Computer Intrusion
United States


Finding the Source of a Computer Intrusion:
Friday, June 22, 2007
New York (victim company)
Computer Intrusion
IP: 121.16.109.40
United States


Finding the Source of a Computer Intrusion:
Friday, June 22, 2007
New York (victim company)
Computer Intrusion
IP: 121.16.109.40
Italy
United States


Finding the Source of a Computer Intrusion:
Monday, June 25, 2007
New York (victim company)
DOJ
Computer Intrusion
IP: 121.16.109.40
Italy
United States


Finding the Source of a Computer Intrusion:
Monday, June 25, 2007
New York (victim company)
DOJ
Computer Intrusion
IP: 121.16.109.40
Request Preservation
Postal & Communications Police Service
Italy
United States


Finding the Source of a Computer Intrusion:
Monday, June 25, 2007
New York (victim company)
DOJ
Computer Intrusion
IP: 121.16.109.40
Request Preservation
ISP
PCPS
Italy
United States

- Other examples, life and limb, kidnapping, threats

Ongoing Activities and Work With COE

- Ping test, Best Practice procedures for acknowledging requests, checklist, training conferences (next tentatively Nov 09), network portal
- Work with COE to combine Directory
  - Expand network, make sure contact points are consistent, make sure there are similar opeataional protocals, participate in training

Improving Assistance

- Can you preserve data based only on foreign request?
  - based on law or cooperation?
- Can you get the data and share it internationally?
  - difference between sharing intelligence & evidence
  - difference in cooperation if there is a crime in your country
  - what minimum facts allow you to open an investigation?
- Is it a crime if a person in your country hacks into a foreign computer?
- How long to get and share evidence –
  - if domestic crime? if no domestic crime?
- Any advice to make process faster? Easier?