International Cooperation in Cybercrime Investigations

Albert Rees
Computer Crime & Intellectual Property Section
Criminal Division, U.S. Department of Justice
A Criminal Intrudes into a Bank in Bangkok

Thai investigators discover attack came from computer in Buenos Aires

Argentinean investigators discover attack came from Bucharest

Canadian agents make the arrest

Romanian agents discover attack came from Vancouver
The Challenges of International Cybercrime Investigations

- Countries must:
  - Enact laws to **criminalize computer abuses**
  - Commit adequate **personnel and resources**
  - Improve abilities to **locate and identify** criminals
  - Improve abilities to **collect and share evidence internationally**
CHALLENGE:

Enacting Laws to Criminalize Computer Abuses
The Need to Make Attacks on Computer Networks a Crime

• “Dual Criminality” usually necessary for two countries to cooperate on a particular criminal matter

• Dual Criminality forms the basis for:
  – Extradition treaties
  – Mutual Legal Assistance Treaties
Overcoming the Dual Criminality Divide

• Countries must agree on what to criminalize
  – OAS Cybersecurity Strategy
  – UN General Assembly Resolution 55/63

• Effort to do so: Cybercrime Convention
  – A baseline for substantive law

• Countries must amend their laws to implement
CHALLENGE:

Committing Adequate Personnel and Resources
Law Enforcement Needs

- Experts dedicated to high-tech crime
- Experts available 24 hours a day
- Continuous training
- Continuously updated equipment
  - no longer a “flashlight and a gun”

- Each country needs this expertise
Solutions Are Not Always Easy

• Cyber security strategy must be formulated

• Difficult budget issues arise (even in the US)

• Requires commitment from senior officials

• Cooperation with the private sector can help
CHALLENGE:

Improve Ability to Locate and Identify Criminals
The Problem of Locating and Identifying Criminals

• Primary investigative step is to locate source of the attack or communication
  – What occurred may be relatively easy to discover
  – Identifying the person responsible is very difficult

• Applies to hacking crimes as well as other crimes facilitated by computer networks
Tracing a Communication

• Only 2 ways to trace a communication:

1. While it is actually occurring
2. Using data stored by communications providers
Tracing a Communication

- Infrastructure must generate traffic data
- Carriers must keep sufficient data to allow tracing
- Laws and procedures must allow for timely access by law enforcement that does not alert customer
- Information must be shared quickly
Solving the Tracing Dilemma I: Traffic Data

- Countries should encourage providers to generate and retain critical traffic data
- Law enforcement’s ability to identify criminals is enhanced by access to traffic data
  - Countries have taken different approaches to balancing this need against other societal concerns
  - Industry will have views about appropriate retention periods
Solving the Tracing Dilemma II: Law Enforcement Access

- Legal systems must give law enforcement authority to access traffic data
  - For example: access to stored log files and to traffic information in real-time

- **Preservation of evidence by law enforcement**
  - Critical because international legal assistance procedures are slow
  - Must be possible without “dual criminality”
  - Convention on Cybercrime, Article 29
Solving the Tracing Dilemma III: Sharing Evidence

• Countries must improve their ability to share data quickly

• If not done quickly, the electronic “trail” will disappear
  – Most cooperation mechanisms take months (or years!), not minutes
  – Convention on Cybercrime, Article 30: expedited disclosure of traffic data
Solving the Tracing Dilemma III: Sharing Evidence

• When law enforcement gets a request, it should be able to:
  1. Preserve all domestic traffic data
  2. Notify the requesting country if the trace leads back to a third country
  3. Provide sufficient data to the requesting country to allow it to request assistance from the third country

• Countries must be able to do this for each other quickly, and on a 24/7 basis
CHALLENGE:

Improve Abilities to Collect and Share Evidence Internationally
Collecting and Sharing Evidence

• Will evidence collected in one country be admissible in another country’s courts?

• Potential for evidentiary problems
  – Collection of digital evidence
  – Tracing electronic communications across the globe
  – Computer forensics

• Current mutual legal assistance treaties may not accommodate electronic evidence
Solutions for Collecting and Sharing Evidence

• Convention on Cybercrime
  – Acts as a Mutual Legal Assistance Treaty where countries do not have one
  – Parties agree to provide assistance to other countries to obtain and disclose electronic evidence

• Developing international technical standards
  – International Organization for Computer Evidence
Unilateral Evidence Collection

- Publicly available information
- Obtaining electronic evidence with consent of owner
  - G-8 and Council of Europe acceptance
Informal Cooperative Measures

- Investigator to investigator
  - Advantage: fast
  - Disadvantages:
    - Frequent domestic legal restrictions on providing assistance
    - May be difficult to locate an investigator who can and will provide assistance
Other Cooperative Measures

- Joint investigation

- Some US points of contact in your country
  - FBI Legal Attaché (LEGATT), an FBI agent
  - Department of Justice Legal Attaché, a prosecutor
  - Immigration & Customs Enforcement (ICE)
  - Secret Service (USSS)

- INTERPOL and similar organizations
FOR MORE INFORMATION

Albert Rees

+1 (202) 514-1026

albert.rees@usdoj.gov

WWW.CYBERCRIME.GOV

Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice