International Cooperation in Cybercrime Investigations

Joel Schwarz
Computer Crime & Intellectual Property Section
Criminal Division, US Department of Justice
Joel.schwarz@usdoj.gov
Challenges from a LE perspective:
- Enact sufficient 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 to bring criminals to justice.
Where Country A criminalizes certain conduct & Country B does not, a bridge for cooperation may not exist - “dual criminality”

- Extradition treaties
- Mutual Legal Assistance Treaties

Convention on Cybercrime

- Acts as a Mutual Legal Assistance Treaty where countries do not have an MLAT
- Model to ensure act is criminalized in each country
- Laws don’t need to have same name, or same verbiage
  - just similar elements
Experts dedicated to High-tech Crime
Experts available 24 hours a day (home & beeper)
Continuous training
Continuously updated equipment
Each country needs this expertise
Solutions Are Not Always Easy

- Difficult budget issues arise (even in the U.S.)
- Requires the commitment of the most senior officials
- Often close cooperation with the private sector can help
- Disparity of resources:
  - Criminal: crossing border is a trivial action
  - LE: cooperating across those same borders is very difficult for investigators
A Criminal Intrudes into a Bank in Manila

Philippine investigators discover attack came from computer in Namibia

Namibian investigators discover attack came from Seoul

Korean agents discover attack came from Vancouver

Canadian agents make the arrest
Primary investigative step is to locate source of the attack or communication

- Very often what occurred is relatively easy to discover, but identifying the person responsible is very difficult
- Applies to hacking crimes as well as other crimes facilitated by computer networks
Only 2 ways to trace a communication:
1. While it is actually occurring
2. Using data stored by communications providers
Infrastructure must generate traffic data in the first place.

Carriers must have kept sufficient data to allow tracing.
- Certain legal regimes require destruction of data.

The legal regime must allow for timely access by law enforcement that does not alert customer.

The information must be shared quickly.

Preservation of evidence by law enforcement is critical given the speed of international legal assistance procedures.
- Must be possible without “dual criminality”.
- Convention on Cybercrime, Article 29.
Countries must improve their ability to share data quickly
If not done quickly, the electronic “trail” will disappear
Yet most cooperation mechanisms take months (or years!), not minutes
Solutions for Collecting and Sharing Evidence

- **Convention on Cybercrime**
  - Parties agree to provide assistance to other countries to obtain and disclose electronic evidence

- **Convention on Cybercrime, Article 30**: expedited disclosure of traffic data
  1. Preserve all domestic traffic data
  2. Notify requesting country if trace leads to a third country
  3. Provide sufficient data to allow requester to request assistance from the third country
LE Problem: MLA on computer/internet cases

Solution: 24/7 emergency contact network
- Knowledgeable LE point of contact – tech & law
- Data preservation, advice, ISP contacts, start mutual legal assistance process
- Available 24/7

Participation
- About 50 countries – open to all, not exclusive club
- South Africa, Namibia, Mauritius, Korea, Taiwan, etc.
Requirements: person on call

- Technical knowledge
- Know domestic laws and procedures
- No big office or fancy command center needed
- No promise of assistance – just immediate availability
- Doesn’t supplant ordinary mechanisms -- it enhances and fills a gap
- Contact CCIPS if interested...

All countries need advice (large and small)

- Borrow each other’s expertise, help with policy
- Expect another training for 24/7 countries in 2008

It works! South American kidnapping case...
APEC leaders committed to:
- Modernize legal frameworks
- Develop cybercrime investigative units and 24/7 response capability
- Establish threat and vulnerability information sharing

OAS: providing assistance to member states
- Regional workshops
- 1st series: Policy and legislative development
- 2nd series: Computer investigations and forensics, international cooperation
- 3rd series: Being developed

OECD: “Culture of Security”

Africa – what’s going on locally?
June 2006 -- 2 training workshops (1 week each)
  • 20 sub-Saharan African nations attended
  • Results of workshops:
    • 2 additional African countries join 24/7 Network
    • CCIPS asked for legislative draft assistance

Currently finalizing planning and funding for next African-region workshops – likely in West Africa in 2008
  • looking for regional partners and hosts

African-focused ListServ:
AfricanCyberInfoNetwork@afrispa.org
  • share insights, seek help and guidance from others, update each other on in-country/region developments
Every country relies on the others for assistance in responding to the threat of cybercrime

Each country needs to:
- Enact adequate substantive and procedural laws
- Empower its law enforcement authorities to collect evidence for other countries
- Work to enhance the rapid collection and international sharing of electronic evidence