Improving Domestic Legislation and International Cooperation on Cybercrime

U.S. Department of Justice

Why people commit intrusion offenses

- Economic reasons
  - Identity theft
  - Fraud
  - Extortion
  - Spam
- National security/espionage
- Economic espionage
- Trade secrets

Cybercrime is growing

- 2013 US estimates of US $100 billion in losses from cybercrime and cyberespionage (Wall Street Journal, July 22, 2013)
  - Precise numbers are hard to identify because cybercrime is an underreported crime
  - For comparison, the cost of car crashes for the U.S. in 2010, estimated between $99 billion and $168 billion

Wide range of cases

- State sponsored attacks
  - Sony breach?
- Targeted "spear-phishing" attacks
- Credit card/health information data breaches
  - U.S. v. Vladimir Drinkman, et. al.
- Ransomware
  - Cryptolocker
- Mobile payment systems
  - Target/Home Depot breaches
- Securities Fraud and other online fraud
  - U.S. v. Ivan Turchynov, et. al.

Challenges

- 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

First Challenge: Applicable Laws

- "Dual criminality" usually necessary for two countries to cooperate on a specific criminal matter
  - Basis of extradition treaties and mutual legal assistance regimes
- The laws of each country do not have to be exactly the same
  - The same concept is usually sufficient
- What to criminalize?
  - OAS Cybersecurity Strategy
  - UNODC Draft Comprehensive Report on Cybercrime, 2013

Consensus on Fundamentals

"*While consensus exists about broad areas of legal intervention for the prevention and combating of cybercrime*, levels of harmonization of legislation as between countries viewed as important for cooperation, within regions, and with multilateral instruments, are perceived to be highly variable. This includes in the area of cybercrime offence penalties [….]"

Draft Comprehensive Study (2013)

Goals of Cybercrime Legislation

- Setting clear standards of behavior for the use of computer devices
- Deterring perpetrators and protecting citizens
- Enabling law enforcement investigations while protecting individual privacy
- Providing fair and effective criminal justice procedures
- Requiring minimum protection standards in areas such as data handling and retention
- Enabling cooperation between countries in criminal matters involving cybercrime and electronic evidence

Draft Comprehensive Study (2013)

An International standard

- The Budapest Convention on Cybercrime
  - Crimes related to computers and the Internet
  - Provisions for investigating cyber crime
  - International legal cooperation
  - Protection of human rights and liberties

- "A significant amount of cross-fertilization exists between all instruments, including, in particular, concepts and approaches developed in the Council of Europe Cybercrime Convention."

Draft Comprehensive Study on Cybercrime (2013)

Budapest Convention on Cybercrime

- First instrument of its type to set out an international standard for cybercrime laws
- Does not dictate statutory language or method of implementation
- Instead, it sets out CAPABILITIES and allows maximum flexibility in implementation
- Membership includes countries from every continent

Substantive Provisions

- Attacks on a computer system, in whole or in part, without right (damage to computers or data)
- Data interference (deletion, modification, or suppression of computer data)
- System interference, hindering the functioning of a system without right, i.e. "denial of service"
- Obtaining electronic communications, without right
- Misuse of "devices" (credit card fraud, passwords)
- Computer-related fraud
- Child pornography
- Copyright infringement, in line with a country's treaty commitments

Procedural Authority

- Expedited preservation of computer data up to 90 days
- Production order for data stored by a provider
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Real-time collection of electronic communications
- Extradition, or domestic prosecution
- Support 24/7

Second Challenge: Adequate Resources

- Experts dedicated to high-tech crime
  - 24/7 Network of contacts
- Continuous Training
- Continuously updated equipment
- Leverage domestic expertise

Solutions aren't easy

- Cybersecurity strategy must be developed
- Difficult budget issues
- Commitment from senior government officials
- Cooperation with private sector

Third Challenge: Procedural Tools to Investigate

- First investigative step is to locate the source of the attack or communication

- What happened is easy to discover; attribution to a person may be difficult

Third Challenge: Obtaining the Data

- Can electronic communications be traced?

- Only two ways to trace:
  - While communication ongoing
  - Reviewing data stored by communications providers

Basic Procedural Tools

- Infrastructure must generate traffic data
- Communications providers must keep sufficient data to allow tracing
- Laws must allow for timely access by law enforcement that does not alert customer
- Laws must allow for timely sharing of information with foreign law enforcement partners

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 take different approaches to balance privacy concerns with law enforcement access
  - Private sector likely will have views about appropriate data retention periods.

Law Enforcement Access

- Domestic legal framework must authorize law enforcement to access traffic data, both stored and real-time
  - Countries establish different requirements for police access
- Domestic legal framework should authorize preservation of evidence
  - Critical because formal international legal assistance procedures are slow
  - Should be able to preserve without "dual criminality" requirement

Fourth Challenge: Sharing Evidence

- Does domestic law allow evidence obtained in a foreign country?
- Potential evidentiary problems
  - Authenticity of the evidence
  - Chain of custody of the evidence
  - Quality of the forensics and witnesses
- Do current mutual legal assistance treaties accommodate electronic evidence?

Formal Cooperation – MLAT, Agreements

- Advantages
  - Efficient and satisfies evidentiary requirements
  - Central authority to central authority (quality control)
  - Legal obligation to assist

- Disadvantages
  - May be slow for capturing electronic evidence
  - May require dual criminality
  - Law enforcement and technical resources limits

Informal Cooperation – Police to Police

- Advantages
  - Flexible and faster
  - Joint investigation
  - Existing law enforcement contacts

- Disadvantages
  - Does domestic law permit informal cooperation
  - Do you know who to call?
  - Potential admissibility problem for evidence

UNODC Experts Group on Cybercrime

- Report on the Meeting of the Expert Group, February 2013

"In discussions concerning the study, it was noted that there was broad support for capacity-building and technical assistance, and for the role of UNODC in that regard. Diverse views were expressed regarding the content, findings and options presented in the study."