# Improving Cybercrime Legislation

U.S. Department of Justice

# Economic Driver

- Information technology is an engine for economic growth
  - e-Commerce
  - Attraction of foreign investment
  - Information processing industries
  - Development of small- and medium-sized enterprises
- Services for the populace
  - e-Government reduces government bureaucracy and bureaucratic inefficiencies
  - Telemedicine and health care centers
  - Distance learning
- All of these benefits rely on reliable and secure information networks

# 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)

# 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

# Law Enforcement Needs

- 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

# 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?