Computer Crime and Intellectual Property Section
Criminal Division, United States Department of Justice
www.cybercrime.gov

International Cooperation in Cybercrime Investigations

Overview

Challenges to international cooperation
Collecting and sharing electronic evidence internationally
Efforts to improve international cooperation

I. Challenges to International Cooperation

A. Computers, computer crimes, and electronic evidence

1. Computers and the Internet profoundly affect the nature of crime

2. Storing, manipulating, and communicating data is easy

3. Criminals use networks not only to commit crimes but also to:

   a. Further criminal activity

   b. Conceal criminal activity

   c. Hide data

4. Electronic evidence is created any time criminals use a digital device or communicate electronically – <u>any crime is likely to have an electronic evidence component</u>

B. Networks are international; they ignore jurisdictional boundaries

1. Substantially increase the reach and scope of crime

   a. <u>Intentional</u> use the Internet for trans-national crime, impacting thousands of victims; for example, “Nigerian” email scams

   b. <u>Unintentional</u> international electronic trail; for example, an email communication to a co-conspirator in the same city may travel to another conti-

nent in the course of transmission, leaving logs and copies on servers in other countries

2. Make national laws harder to enforce; for example, content restrictions such as child pornography

3. Create difficulties for investigation that now involve multiple countries and multiple jurisdictions

   a. Globe-spanning evidence: Traffic data, tools, stolen information, and communications may all be stored on foreign systems

   b. Multiple legal systems and procedural laws

   c. Limits on domestic law enforcement to investigate outside of jurisdiction

C. Example: Finding the source of a computer intrusion

1. Requires investigative work by four different agencies on different continents

2. The complexity of this example international intrusion can apply to any computer-related crime today, such as intellectual property violations or terrorist communications

3. Every country is forced to rely on others to help solve this type of crime

4. In addition to government efforts, investigations require information from non-government sources

D. Barriers to cooperation: Law enforcement personnel face barriers to effective international cooperation including:

1. Sovereignty
2. Chain of custody and authentication problems
3. 19th Century protocols being applied to 21st Century needs
4. Disparity of resources

E. Locating and identifying criminals – technical challenges

1. May be easy to determine what happened – much more difficult to identify the person responsible
2. Applies to hacking crimes as well as other crimes facilitated by computer networks
3. Tracing a communication
   a. Two ways to trace electronic communication:
      i. While it is occurring
      ii. Using data stored by service providers
   b. Tracing challenges:
      i. Does the infrastructure generate traffic data?
      ii. Do service providers keep sufficient data to allow for tracing?
      iii. Where are the service providers?
      iv. Does the legal regime allow for timely access by law enforcement?
      v. Without alerting customers?

II. Collecting and Sharing Electronic Evidence Internationally

A. Collecting and sharing electronic evidence internationally

1. Will evidence collected in one country be admissible in another country?
2. Will computer forensics procedures be accepted?
3. Will an MLAT or other legal assistance procedure cover electronic evidence?

B. Traditional methods

1. Unilateral measures taken by law enforcement without need for permission from the foreign government
    a. Publicly available information; for example law enforcement use of "Whois" lookup for information about domain names or Internet protocol addresses
    b. Consent of owner
2. Informal cooperation between law enforcement agencies of different countries
    a. Advantages: Fast, with few or no institutional requirements
    b. Disadvantages: Domestic legal limits and difficulty in finding appropriate contacts in other jurisdictions
3. Formal cooperation between governments
    a. Mutual legal assistance treaties (MLAT)
        i. Advantages:
            1) (Relative) speed and efficiency
            2) Central authority to central authority
            3) Obligation to assist
            4) Available at investigative and trial stages
            5) May include procedures for law enforcement and protections for defendants
        ii. Disadvantages:
            1) Still quite slow – especially for electronic evidence

2) Possible dual criminality requirement

3) Foreign law enforcement may not have legal authority to obtain evidence

b. Letters rogatory

i. Even slower

ii. No central authority

iii. No obligation to assist

iv. Not always available during investigation

C. New methods of cooperation

1. Interpol Network for Computer-Related Crime

a. 60+ countries are connected to Interpol's network

b. Works through National Central Reference Points; usually a specialist unit; however, Interpol NCRPs do not always provide 24-hour capability

c. Cooperation based on same principles otherwise applicable to Interpol co-operation

2. G8 Network of 24/7 Contacts for High Tech Crime

a. 50+ countries have shared high tech law enforcement contact information with each other

b. Contact points are available 24/7, English speaking, technically knowledgeable, and knowledgeable about domestic law and policies regarding international assistance and electronic evidence

III. Efforts to Improve International Cooperation

A. Domestic laws on computer abuses

1. Extradition, mutual legal assistance and other types of formal cooperation depend on domestic law

a. Domestic laws form basis for extraditable offenses or mutual legal assistance

b. Treaty may limit cooperation to certain enumerated offenses

c. Conduct alleged must generally be criminal under the laws of both the requested and requesting states – "dual criminality"

2. International efforts focus on improving domestic cybercrime laws

a. United Nations General Assembly Resolution 55/63: "Combating the Criminal Use of Information Technologies"

> *Legal systems should protect the integrity of data and computer systems from impairment and ensure that criminal abuse is penalized*

b. Council of Europe Convention on Cybercrime

i. Has substantive, procedural and cooperative provisions

ii. First signed in 2001 in Budapest, Hungary; entered into force 2004; also known as the "Budapest Convention"

iii. Open to all countries; 22 countries are parties (including U.S.), 21 additional countries have signed

iv. Obliges parties to:

1) Establish substantive domestic laws against cybercrime

2) Ensure that domestic law enforcement officials have procedural authority to investigate and prosecute cybercrime

3) Provide international cooperation to other parties in the fight against cybercrime

4) Consider the criminal offenses they establish as extraditable offenses under their applicable extradition treaties

v. Does not oblige parties to extradite persons in the absence of a bilateral treaty

vi. A framework for domestic laws even for countries that are not in a position to accede to the Convention

vii. Council of Europe staff will consult on national legislation

viii. The convention, explanatory report and other information is located on the Council of Europe website, www.conventions.coe.int

B. Resource allocation

1. Commitment from senior officials
2. National strategy for cybersecurity and to combat cybercrime
3. Cooperation with private sector
4. No longer just a "flashlight and a gun"; fighting cybercrime requires:
    a. Dedicated experts
    b. 24-hour availability
    c. Continuous training
    d. Updated equipment

C. Improving information sharing

1. Law enforcement should be able to:
    a. Request preservation of domestic traffic data
        i. "Preservation" is a requirement that a service provider not delete specific evidence, pending a formal request for disclosure
        ii. A "quick freeze"
        iii. Existing evidence only
        iv. This allows time for a formal request, such as an MLAT request
    b. Notify the requesting country if the data leads to a third country
    c. Provide sufficient data to the requesting country to allow it to request assistance from the third country
2. Interpol Regional Working Parties on Information Technology Crime
    a. Consist of the heads or experienced members of national computer crime units.
    b. European, African Regional, Asia - South Pacific, and Latin America Working Parties
3. UN General Assembly Resolution 55/63

Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations

4. OAS training programs, through the Group of Experts on Cybercrime and Inter-American Committee Against Terrorism

5. The Council of Europe Convention on Cybercrime

   a. Operates as an MLAT where countries do not have one

   b. Parties agree to provide assistance to others in obtaining and disclosing electronic evidence

   c. Requires parties to have key procedural mechanisms available for use in international cases; for example, preservation of electronic evidence

6. G8 1997 Justice and Home Affairs Ministerial: "Ten Principles & Ten-point Action Plan"

   a. Countries should develop compatible forensics standards

   b. Created 24/7 Network of Contact Points

7. G8 1999 G8 Justice and Home Affairs Ministerial: "Principles on Transborder Access to Stored Computer Data"; recommends that countries should:

   a. Develop means for timely preservation of data

   b. Establish procedures for expedited data sharing

   c. Agree to allow access to data when it is publicly available, or with consent of the legal custodian

IV. Conclusions

A. Every country relies on others for assistance in responding to cybercrimes

B. Successful investigations are possible using available tools and law

C. Everyone's ability to fight cybercrime improves as countries implement adequate substantive, procedural, and mutual legal assistance laws

---

This presentation was developed by the Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, www.cybercrime.gov