

International Cooperation in Combating Cybercrime

*– An Overview of Multi-lateral
Organization Work, and International
Cooperation in Practice -*

AF CyberSec

Cote D'Ivoire – Africa - 2008

Joel Michael Schwarz

Computer Crime & Intellectual Property Section

U.S. Department of Justice, Criminal Division

(202) 353-4253

joel.schwarz@usdoj.gov

Overview



- **Multi-Lateral Organization Cybercrime Work**
 - APEC
 - OAS
 - G8
 - Africa and the Middle East
 - COE
- **International Cooperation**
 - Practical Considerations
- **International Cooperation Case – Kidnapping in South America**

APEC Leaders' Statement



- Heads of State met in October, 2002
 - Three commitments:
 - Legal frameworks
 - Law enforcement investigative units
 - CERT network
- “Endeavor to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). . . .”

APEC Cybersecurity Strategy



- Approved by Ministers in 2002
- Comprehensive Strategy for APEC Work
 - Legal Developments
 - Information Sharing
 - Security and Technical Guidelines
 - Training and Education
 - Wireless and Emerging Technologies

Survey of Laws



- Voluntary Survey of APEC members
- Questions based on the Convention on Cybercrime (2001)
- Excellent collection of cybercrime laws
- Drafting resource for others
- Available at:
www.apectelwg.org/e-securityTG/index.htm

Overview



- **Multi-Lateral Organization Cybercrime Work**
 - APEC
 - **OAS**
 - G8
 - Africa and the Middle East
 - COE
- **International Cooperation**
 - Practical Considerations
- **International Cooperation Case – Kidnapping in South America**

Organization of American States ("OAS")

- Ministers of Justice Group of Government Experts ("REMJA")
- Group of Experts on Cyber Crime established in 1999
- Questionnaire sent to member states to assess legal frameworks
- Developed Ten Recommendations, which were adopted by the Ministers of Justice in March 2000

OAS Recommendations

– Highlights:

- Identify/Create Entity Responsible for Cybercrime
- Enact legislation
- Harmonize cyber-laws to facilitate international cooperation
- Determine training needs
- Join 24-Hour/7-Day a Week Point of Contact Group
- Educate the public



OAS - REMJA Working Group on Cybercrime

Forum for OAS to address cybercrime (since 1999)

- Strengthens regional and global cooperation to combat crimes involving computers and the Internet
- Gathers information from member states on cybercrime threats, legislation and org. expertise
- Conducts regional workshops (since 2004) on cybercrime investigation, forensics, prosecution, international cooperation, and legislation
- Maintains public website: <http://www.oas.org/juridico/english/cyber.htm>, and private web portal

Recent OAS Work



- 2008 workshops focused on developing domestic cybercrime legislation
- 33 of 34 OAS member states participated in Caribbean or Latin American workshops
 - more than 100 attendees, including legislators, judges, prosecutors, investigators, and policy-makers involved in cybercrime matters
- Cybercrime Convention used as framework for domestic legislation
- Participants drafted “country profiles” of existing and draft cybercrime legislation
- Presenters from OAS, Council of Europe, Argentina, Brazil, Canada, Colombia, Dominican Republic, Romania, and United

Trends in the Americas



- Support is growing for Cybercrime Convention
 - Costa Rica, Mexico, and other OAS member states considering accession
- Legislative reform is proceeding rapidly in the region
 - at least 8 countries have existing or draft legislation adequate to combat cybercrime;
 - most other countries are moving forward in developing cybercrime law
- Capacity is growing to investigate and prosecute cybercrime as investigators, forensic specialists, and prosecutors gain knowledge, experience, and the tools needed to combat cybercrime

Overview



- **Multi-Lateral Organization Cybercrime Work**
 - APEC
 - OAS
 - **G8**
 - Africa and the Middle East
 - COE
- **International Cooperation**
 - Practical Considerations
- **International Cooperation Case – Kidnapping in South America**

G8 24/7 Network of High-Tech Points of Contact

- 1997 Established by Group of 8 Nations Ministers
- Participating Countries Provide a 24 hours a day/ 7 days a week Point of Contact for Cybercrime Emergencies
- Expanded beyond the original G8 nations, including many APEC economies
- 50+ member countries



G8 24/7 Network - News



- Upcoming Training
 - still in early planning, but hopefully in 2009 (Italy has Chair in 2009)
- Planning to test network contact points w/in next 12 months
- Now 51 country members
 - recently added a number of African-region countries
- Working on publication of a joint COE/G8 24/7 Network Directory

G8 PRINCIPLES AND ACTION PLAN TO COMBAT HIGH-TECH CRIME



1. Network of knowledgeable personnel to ensure effective response to transnational high-tech cases and designate a 24-7 point-of-contact.
2. Sufficient number of trained/equipped law enforcement allocated to combating high-tech crime and assisting LE.
3. Review legal systems to ensure they criminalize abuses of telecommunications and computer systems and promote investigation of high-tech crimes.
4. Take high-tech crimes into consideration when negotiating mutual assistance agreements.
5. Develop solutions for:
 - preservation of evidence
 - transborder searches
 - computer searches of data where the location of that data is unknown
6. Develop expedited procedures for obtaining and passing traffic data internationally.
7. Work with industry to ensure technologies facilitate combating high-tech crime.
8. Expedited mutual assistance in expedited manner in urgent and appropriate high-tech crime cases.
9. Encourage development of standards for reliable and secure telecomm and data processing.
10. Develop/employ compatible forensic standards for retrieving/authenticating electronic data.

Overview



- **Multi-Lateral Organization Cybercrime Work**
 - APEC
 - OAS
 - G8
 - **Africa and the Middle East**
 - COE
- **International Cooperation**
 - Practical Considerations
- **International Cooperation Case – Kidnapping in South America**

Training Initiatives - Africa



- CCIPS held two training workshops in Botswana – June 2006
 - cybercrime capacity-building
 - Approx. 20 sub-Saharan African nations (judges, policy-makers, senior law enforcement officials and the private sector)
 - 1 held for Anglophone and 1 for Francophone countries
 - 2 African countries joined 24/7 Network shortly after
- Workshop in Benin for West African countries – July 2008
 - Cybercrime assistance and legislative drafting
 - Approx. 10 – 15 Francophone countries
 - Another African country joined 24/7 Network shortly after
- FUTURE Work: Multi-lat Training Workshop
 - East Africa – Kenya – December 2008

Other CCIPS African Initiatives



- CCIPS legislative drafting assistance to African countries, including
 - Nigeria, Botswana and many others...
- Nigerian capacity-building workshop in November 2006
- African-focused ListServ
- Participation in African based conferences (ITU, African Multi-lat Orgs, etc.)

“Cairo Declaration Against Cybercrime 2007”

- 400 representative from public/private sector across Arab region & other countries, as well as NGOs and International Organizations
- “Budapest Convention (2001) on Cybercrime is recognized as the global guideline for development of cybercrime legislation.”
 - “Egypt and other countries of the Arab region may want to consider accession to this treaty”
- “Countries are encouraged to set up specialized units for cybercrime investigations, as well as ensure that prosecutors and judges are sufficiently trained.”
- “[t]he Arab region should consider establishing Computer Emergency Response Teams (CERTs).”
- “Countries of the Arab region should consider establishing contact points available 24 hours per day, seven days per week to facilitate urgent international investigations involving electronic evidence, and joining the network of contact points of the G8 and the Council of Europe.”

Overview



- **Multi-Lateral Organization Cybercrime Work**
 - APEC
 - OAS
 - G8
 - Africa and the Middle East
 - **COE**
- **International Cooperation**
 - Practical Considerations
- **International Cooperation Case – Kidnapping in South America**

Council of Europe



- First Comprehensive Multinational Cyber Crime Treaty
- Completed in Fall 2001
- Drafted by 40 member states, plus U.S., Canada, Japan, and South Africa
 - In English and French (both original drafting languages)
- 30 countries signed at the signing ceremony in November 2002
- Now open to qualifying countries around the world
- COE Rep covers in greater detail
 - COE assistance with legislative drafting

Overview



- Multi-Lateral Organization Cybercrime Work
 - APEC
 - OAS
 - G8
 - Africa and the Middle East
 - COE
- International Cooperation
 - Practical Considerations
- International Cooperation Case – Kidnapping in South America

International Cooperation Mechanisms for Criminal Prosecutions



- Law enforcement exercises its functions in foreign jurisdiction only with consent of foreign government.
- If evidence (or criminal) is located in another country, need to have the assistance of criminal law enforcement in that country
 - while some cc is domestic, criminals have become proficient at routing through countries, finding open proxies, botnets, etc.
- May need to engage in cross-border criminal assistance – to get evidence (E-mails from ISP, apprehend criminal, consider extradition, etc.)
- Two types of criminal law enforcement-to-law enforcement assistance
 - 1. informal assistance (domestic investigation - investigative agencies / prosecuting offices contact each other)
 - 2. formal assistance - “Central Authorities” = Justice /LE

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
 - Potential problems using in court

Formal Assistance



- *MLAT's* (treaties) or MLAA (executive agreement)
 - limited in scope
 - May not cover newer crimes, such as computer crime or spam
 - Often, minimum potential jail time of over 1 year
 - Request made to/from Central Authority (Defined in MLAT – usually a Justice Ministry or other Law Enforcement entity)
- Letters Rogatory
 - Court-to-Court assistance; from Court's "inherent powers"
 - Only basis is comity – helping friends when in interest
 - No obligation to provide assistance

Some Solutions for Collecting and Sharing Evidence

- Convention on Cybercrime
 - Sets forth the capabilities and substantive crimes countries should have in place to criminalize acts that involve computers/networks
 - Many criminal cases implicate network crimes – unauth. access, DDOS, use of computers to commit fraud, etc.
 - Acts as a Mutual Legal Assistance Treaty where countries do not have an MLAT
 - Parties agree to provide assistance to other countries to obtain and disclose electronic evidence
 - Also allows for a finding of dual criminality on substantive offenses, if needed in order to cooperate
- MOUs and agreements between various law enforcement agencies
- 24/7 Network of High-Tech Crime Points of Contact

Overview



- Multi-Lateral Organization Cybercrime Work
 - APEC
 - OAS
 - G8
 - Africa and the Middle East
 - COE
- International Cooperation
 - Practical Considerations
- International Cooperation Case – Kidnapping in South America

Anatomy of an Investigation: Kidnapping in South America

- 4:34 P.M. -0500 GMT- It begins....
- You are a Prosecutor for the Dept of Justice – you've been on duty all day
- You receive a call from a representative from the Embassy of Country A, in Washington, D.C. - they need your help
- Elderly woman kidnapped approximately 2 weeks ago - No witnesses
- Husband was given 2 index cards by someone unrelated to the kidnapping
 - First index card – name of a hotmail account, kidnapped@hotmail.com, along with a password and instructions
 - Second index card – another hotmail account, we-have-your-wife@hotmail.com, but with no password
 - Asks for \$250,000.00

4:36 P.M. -0500 GMT

- Country A's law enforcement has been investigating for 2 weeks
- No physical evidence
- Need help with Hotmail – which is based in the US
- Country A contacted Hotmail on its own, but:
 - Hotmail – have consent of account holder?
 - Hotmail - need court order from US Court, to release the personal info.
- Country A now seeking US assistance

4:38 P.M. -0500 GMT

- Your first decision – immediate threat to life and limb?
 - elderly woman, but already missing 2 weeks
 - courts still open – will close in a few hours
- Begin drafting papers
- 6:04 P.M. –0500 GMT - race over to the courthouse in a taxi
- Hand papers to judge and wait in chambers
- 6:18 P.M. -0500 GMT - Judge signs
- 6:19 P.M. -0500 GMT - Clerk of Court office
- 6:36 P.M. -0500 GMT - Taxi back to your office
- Call Hotmail and fax order

6:57 P.M. -0500 GMT

- Wait by the phone for Hotmail
- 7:12 P.M. -0500 GMT – Hotmail calls back
 - Name, address and subs info. – bogus
 - Financial data – none (Hotmail = free)
 - IP addresses
- 7:14 P.M. -0500 GMT
 - Provide information to Country A's authorities
- 7:58 P.M. -0500 GMT – Country A finishes contacting providers
 - all IP addresses trace back to cyber-cafes

8:00 P.M. -0500 GMT

- Call from Country A
 - Drive bys of address = abandoned lot
 - Phone = disconnected (registered name = bogus)
 - Name = no hits
- Family received another E-mail
 - attached picture of victim – she's going down hill very fast (looks sick and is missing her meds)
- Only hope is to apprehend while online (to provide drop info) – in cyber café'

8:18 P.M. -0500 GMT

- Speak with FBI Office in D.C. and explain the need to have an FBI agent assigned ASAP – and what the agent will be expected to do
- 8:20 P.M. -0500 GMT - Contact Hotmail (set up pen/trap and link to cell/beeper)
- 8:24 P.M. -0500 GMT – Contact FBI Office in CA – agent assigned
- 8:28 P.M. -0500 GMT – Hotmail activates P/T – automatically copied to agent's cell phone

7:50 A.M. -0500 GMT – Next Morning

- FBI Agent's cell phone goes off – hotmail account accessed
- Agent logs in, runs check on the IP address indicated
- 7:51:35 A.M. –0500 GMT – Agent calls you and you conference in Country A's authorities
- 7:52:42 A.M. – 0500 GMT– Country A's authorities ascertain local address using trace on the IP address (real-time)
- 7:53:00 A.M. –0500 GMT - police car nearest the cyber café' is dispatched
- 7:54:22 A.M. – 0500 GMT – Cyber café' surrounded – kidnapper apprehended while on café' computer
- 7:58 A.M. –0500 GMT – using information provided by suspect, police raid nearby house and recover woman
- 8:00 A.M. –0500 GMT – remaining kidnappers placed under arrest – elderly woman taken to hospital

1st kidnap victim recovered alive, in years

Only accomplished through:

- ability of public safety officials being able to investigate and track in real-time
- ability of public safety officials to cooperate in hours, not days, weeks or months – the speed of traditional international cooperative mechanisms
- and information controller (in this case ISP) being able to disclose information and cooperate with LE in an expedient manner

Lawyer-like disclaimer . . .

- FIN-



Joel Schwarz
joel.schwarz@usdoj.gov
202-353-4253



WWW.CYBERCRIME.GOV

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