



Philip A. Guentert
Attaché, U.S. Department of Justice
Embassy of the United States of America
Bangkok, Thailand

BRIDGING THE TECHNICAL AND LEGAL ASPECTS OF CYBERCRIME: MODELS OF LAW ENFORCEMENT COOPERATION




Bridges Within Your Own Borders

Cooperation Against Cybercrime Begins at Home






The Bridges: Domestic Cooperation

- Law enforcement agency partnership
 - Police-prosecutor partnership
 - Public-private partnership
- 




U.S. Justice Department Model of Specialization

- Computer Crime and Intellectual Property Section (CCIPS) in Washington, DC
 - 30-40 dedicated lawyers and prosecutors
 - Computer Crime, IP and Evidence Teams
 - Computer Hacking and Intellectual Property Units (“CHIP” Units)
 - Specialized units in U.S. Attorney’s Offices
- 




Why CHIP Units?

- Response to growing frequency, sophistication and cost of computer crime and technical aspects of offense
 - Other advantages and efficiencies of specialization
 - Industry education and outreach – build partnerships and trust
 - Overcome victim reluctance to report crime
- 



The CHIP Unit Concept

- Computer Hacking and Intellectual Property (CHIP) Units in U.S. Attorney's Offices
 - First unit created in early 2000 in San Jose
 - Created by Robert S. Mueller, III (now FBI Director)
- CHIP Units now expanded to 25 U.S. Attorney's Offices
- CHIP Coordinators in all 94 USAOs




Law Enforcement Agency Partnership

How can we work together best to investigate and
prosecute cybercrime cases?





Investigative Resources

- FBI
 - National Cyber Division and IPR Unit
 - Local Hi-Tech Crime Squads
 - US Secret Service
 - USSS Electronic Crimes Task Forces
 - ICE
 - Regional Computer Forensic Laboratories
- 

Cooperation Regarding Cybercrime Forensic Resources





HOMECONTACTSURVEY

National Program

Continuing Education

Newsroom

Speakers Bureau

RCFL Directory

CONTACT US

p: (703)985-3677

f: (703)985-3979

email: NPO@rcfl.gov

Contact your local

WELCOME TO THE NATIONAL RCFL PROGRAM

Welcome to the National RCFL Program's Web page. This site is a gateway to the premier digital forensics laboratory network in the country.

The RCFL Program provides overtime pay, cell phones and vehicles to our state/local Examiners - click [here](#) to learn about our [benefits of participation](#).

RCFLS IN THE NEWS



6/30/11: State Grand Jury Indicts Three People for Crimes Against Children – Three South Jersey residents face multiple charges of sexual depravity and exploitation of children. The indictments were the result of an investigation conducted by the [New Jersey State Police](#) and the [New Jersey Division of Criminal Justice](#) – both are participating agencies in the [New Jersey RCFL](#) who is providing digital forensics expertise to investigators – [learn more](#).



6/28/11: Old Fashioned Police Work Combined With Modern

MOST POPULAR



NEW! 5 Basics About Live Capture Bookmark [Download it](#)



2010 Webcast on Live Capture [See it](#)



FY10 Annual Report [Read it](#)




Mobile Forensics




Police/Prosecutor Partnership


How can we work together best to investigate and prosecute cybercrime cases?






Benefits of a Prosecutor Role in the Initiation of the Case

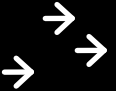
- Prosecutors are trained and experienced in evaluating cases for the probability of success in court (conviction).
 - Prosecutors are in the best position to implement a consistent set of priorities and unified strategy for law enforcement.
- 



Benefits of a Prosecutor Role in the Investigation

- Understanding the elements of the potential offenses that can be charged.
 - Assessing whether the evidence being gathered is proof beyond a reasonable doubt of the elements of those offenses.
 - Advising on the legal requirements for gathering admissible evidence.
- 

From Prosecuting Computer Crimes, U.S. Justice Department (2010)



Violation of section 1030 was the year. Thus, the CORP and RICO Act added the offenses listed in section 2332b(g)(5)(B) to 18 U.S.C. § 1961(1), making them predicate offenses for prosecutions under the Racketeer Influenced and Corrupt Organizations (RICO) statute. As a result, any “RICO enterprise” (which may include terrorist groups) that violates section 1030(a)(1) (or section 1030(a)(5)(A)) can now be prosecuted under the RICO statute.

C. Accessing a Computer and Obtaining Information: 18 U.S.C. § 1030(a)(2)

The distinct but overlapping crimes established by the three subsections of section 1030(a)(2) punish the unauthorized access of different types of information and computers. Violations of this section are misdemeanors unless aggravating factors exist.

Title 18, United States Code, Section 1030(a)(2) provides:

Whoever—

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—


1030(a)(2) Summary (Misd.)

1. Intentionally access a computer
2. without or in excess of authorization
3. obtain information
4. from
 - financial records of financial institution or consumer reporting agency
 - OR
 - the U.S. government
 - OR
 - a protected computer





(Felony)

5. committed for commercial advantage or private financial gain



Benefits of a Prosecutor Role (continued)

- Helping protect the rights of the defendant
 - Prosecutors can play a unique role in obtaining the cooperation of defendants during or at the end of the investigation
- 




The Role of the Agent/Police When/After Case is Charged



- Advising on initial charges
- Continuing to gather evidence to rebut defenses and support new charges
- Preparing trial witnesses: the role of the “prover”
- Testifying at trial
- Handling trial logistics
- Presentation of evidence at sentencing



Promoting Police-Prosecutor Partnerships

- Preserve flexibility: cooperation by choice—shared objectives and professional culture--rather than rule
 - Hire across disciplines
 - Train across disciplines
 - But remember: goal is teamwork, each partner with a unique role. Prosecutors are not police.
- 

State/Federal and Police/Prosecutor Partnership Against Cybercrime



Rapid EnFORCEment Allied Computer Team

- Home
- NEWS
- Publications
- Links
- PC 530.8
- Report a crime
- Industry BOLD's
- About us
- Alumni

About the REACT Task Force.

Our Team

A partnership of 17 local, state, and federal agencies, with the Santa Clara County District Attorney's Office designated as the lead agency. The REACT Task Force is one of five in the State of California and authorized under California Penal Code 13848.

All Agents of the React Task Force are either California Peace Officers and/or U.S. Federal Agents

Our History

REACT was established in 1997 by the California State Department of Justice, in response to both public and industry concerns over the spread of new types of crime directly tied to our increasingly computer-oriented economy and widespread use of the Internet. High tech companies and industry councils provide specialized training, liaison personnel and internal support for task force investigations.

By creating a multi-jurisdictional team that combines resources and specific investigative skills, along with federal jurisdiction to conduct investigations across state and international lines, and a close working partnership with the high tech industry, REACT has been able to arrest and prosecute a wide range of criminal offenders and provide a more effective level of service to local communities and the high tech business community.

How to contact us

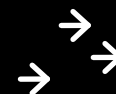


Public/Private Partnership

How can we work together best to investigate and prosecute cybercrime cases?



Partnership with Private Experts and Sources of Technology



National Cyber-Forensics & Training Alliance

[NCFTA Home](#) [About the NCFTA](#) [NCFTA Initiatives](#) [Become a Partner](#) [Knowledge Base](#) [NCFTA News](#) [Report Cyber Incident](#) [Career Center](#) [Contact Us](#)

[NCFTA Home](#) »

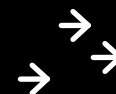
NCFTA – Cracking Down on Cyber Crime

Cyber crime today is becoming increasingly complex and international in nature. A domestic cyber breach can quickly change into a convoluted, on-line ID theft or global money laundering matter. To effectively address such crimes, organizations must quickly identify and leverage the most complete intelligence and be capable of following that trail.

The NCFTA functions as a conduit between private industry and law enforcement with a core mission to identify, mitigate and neutralize cyber crime. In an effort to streamline intelligence exchange, the NCFTA will often organize SME interaction into threat-specific initiatives. Once a significant online scheme is realized and a stakeholder consensus defined, an initiative is developed wherein the NCFTA manages the collection and sharing of intelligence with the affected parties, industry partners, appropriate law enforcement, and other SMEs.



Partnership With Victims of Cybercrime



The screenshot shows the homepage of the Internet Crime Complaint Center (IC3). At the top is a blue banner with the IC3 logo on the left, which consists of a stylized 'i' and 'C' with a '3' and an orbital ring. To the right of the logo, the text 'INTERNET CRIME COMPLAINT CENTER' is written in large, bold, white capital letters. Below this, in smaller white text, is '... an FBI - NW3C Partnership'. Below the banner is a navigation bar with links: 'Home', 'File a Complaint', 'Press Room', 'About IC3', and 'Contact Us'. The main content area on the left has a heading 'Welcome to IC3' followed by a paragraph explaining the center's partnership with the FBI, NW3C, and BJA. Below this is another paragraph about the center's mission to serve as a vehicle for receiving, developing, and referring criminal complaints. A yellow box contains the heading 'Filing a Complaint with IC3' and a paragraph about the online filing process. On the right side, there is a search bar with a 'Search' button. Below the search bar is a list of links: 'FAQs', 'Legal', 'Disclaimer', 'Privacy Notice', 'Protect Yourself', 'Internet Crime Prevention Tips', 'Internet Crime Schemes', 'Public/Private Alliances', and 'Site Map'. At the bottom right, there is a yellow box with the text 'Protect Yourself With The Latest IC3 Consumer Alerts!' and a link to 'Mass Market Fraud' with a small icon of a document.

INTERNET CRIME COMPLAINT CENTER
... an FBI - NW3C Partnership

[Home](#) [File a Complaint](#) [Press Room](#) [About IC3](#) [Contact Us](#)

Welcome to IC3

The Internet Crime Complaint Center (IC3) is a partnership between the [Federal Bureau of Investigation](#) (FBI), the [National White Collar Crime Center](#) (NW3C), and the [Bureau of Justice Assistance](#) (BJA).

IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy -to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes. [read more >>](#)

Filing a Complaint with IC3

IC3 accepts online Internet crime complaints from either the person who believes they were defrauded or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request that you provide the following information when filing a complaint:

- ▶ [FAQs](#)
- ▶ [Legal](#)
- ▶ [Disclaimer](#)
- ▶ [Privacy Notice](#)
- ▶ [Protect Yourself](#)
- ▶ [Internet Crime Prevention Tips](#)
- ▶ [Internet Crime Schemes](#)
- ▶ [Public/Private Alliances](#)
- ▶ [Site Map](#)

Protect Yourself With The Latest IC3 Consumer Alerts!

▶ [Mass Market Fraud](#)




Bridges Across Borders

International cooperation against cybercrime







Cybercrime is:

- Transnational crime. Computers and networks allow criminals to operate across national boundaries.
 - Difficult to investigate and prosecute because those boundaries are more of a barrier to law enforcement than criminal organizations. Obstacles are limits to jurisdiction and sovereignty of other countries. Evidence and defendants cannot be obtained unilaterally.
- 





The Bridges: Foreign Cooperation

- Practices supporting bilateral law enforcement cooperation
 - Institutions supporting bilateral law enforcement cooperation
 - Cooperation beyond the treaty
 - Capacity-building through mutual legal assistance
- 




Practices supporting international cooperation

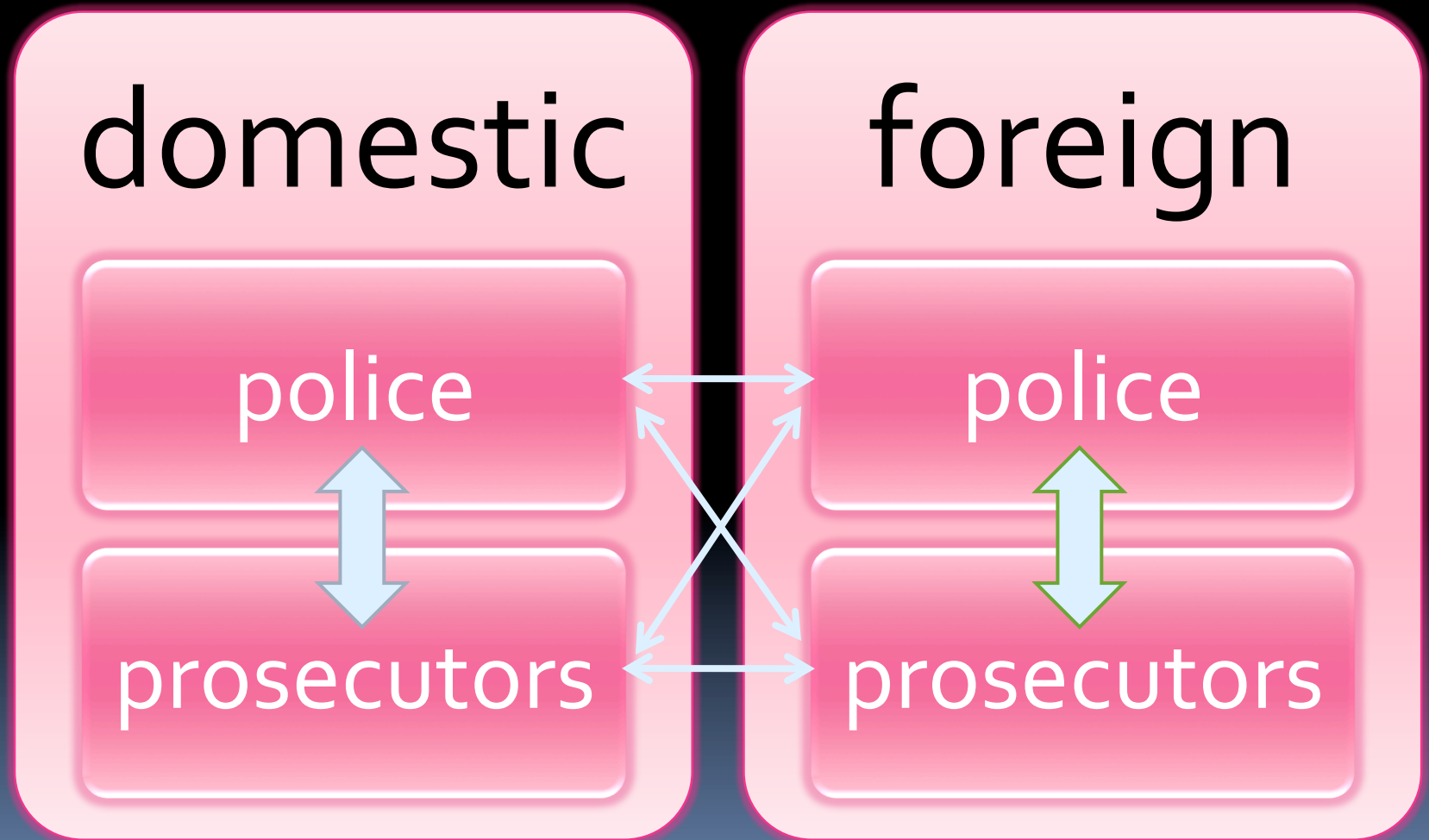
- The stages of bilateral development
 - Informal cooperation “cop-to-cop”
 - Cooperation prosecutor-to-prosecutor
 - Use of formal legal process for mutual legal assistance (MLA) and lawful return
 - Where appropriate, MLA and extradition treaties
- 




Practices supporting international cooperation


- Lessons
 - Informal cooperation is vital
 - The role of prosecutor—domestic and foreign--is vital
 - Invoking formal legal process for obtaining admissible evidence
 - Shaping the investigation
 - Making the relationship truly bilateral
 - Communicating based on shared professional training, values, objectives, and experience
- 

Model of International Cooperation

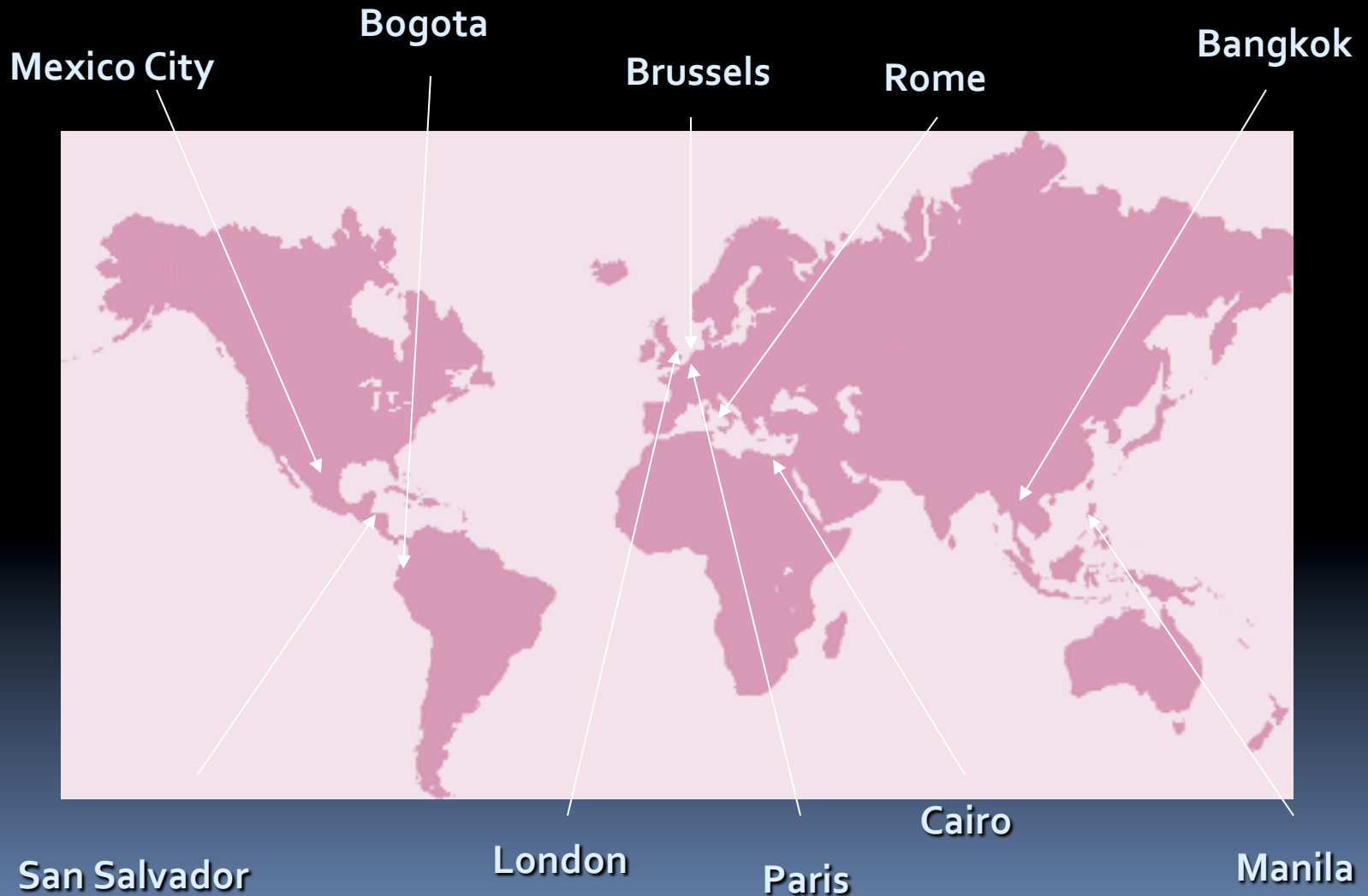




Institutions supporting international cooperation


- Domestic prosecution/law enforcement agencies with international presence
 - International networks
 - E.g., the 24/7 Cybercrime Network
- 

Department of Justice Attachés






The 24/7 Cybercrime Network

- Currently 56 members, including U.S. and Malaysia
 - U.S. point of contact is Computer Crime and Intellectual Property Section at the Justice Department
 - Note that parties to the International Cybercrime Convention are obligated to have a mechanism (usually statutory) to preserve data upon request
- 





Cooperation Beyond the Treaty

- Importance of formal mechanisms outside the treaty context
 - Importance of domestic law on foreign exchange of evidence and subjects
 - Importance of informal mechanisms outside the treaty context
- 




Capacity-Building Through Mutual Legal Assistance

- In the same way that international cooperation is promoted through shared training and other capacity-building exercises, the reverse is true. . .
- 



Successful Cybercrime Cooperation: Example

- November 2010: Operation In Our Sites v. 2.0
 - Undercover purchases of counterfeit goods online resulting in seizure warrants for 82 domain names of commercial websites
 - Task force comprising public and private partners of IPR Center, CCIPS, DOJ Money Laundering Section, and nine U.S. Attorney's Offices, as well as foreign law enforcement components.
- 



Questions and comments to:

Philip A. Guentert

GuentertPA@state.gov