Harmonizing National Legal Approaches and International Legal Coordination

International Cooperation in Cybercrime Investigations

A Law Enforcement Perspective

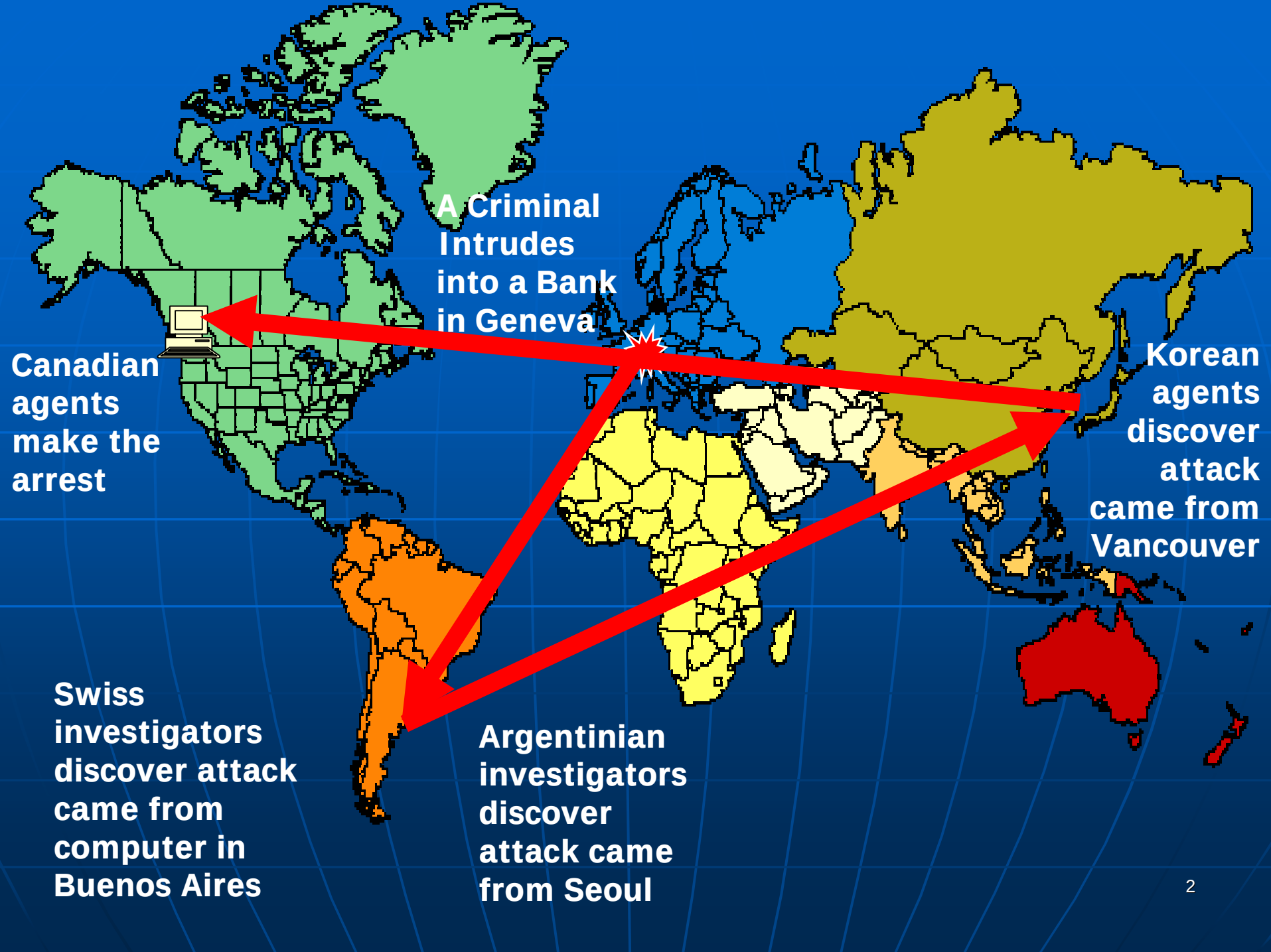
Colonel Claudio Peguero
Commander, High Tech Crimes Investigation Department
National Police
Dominican Republic

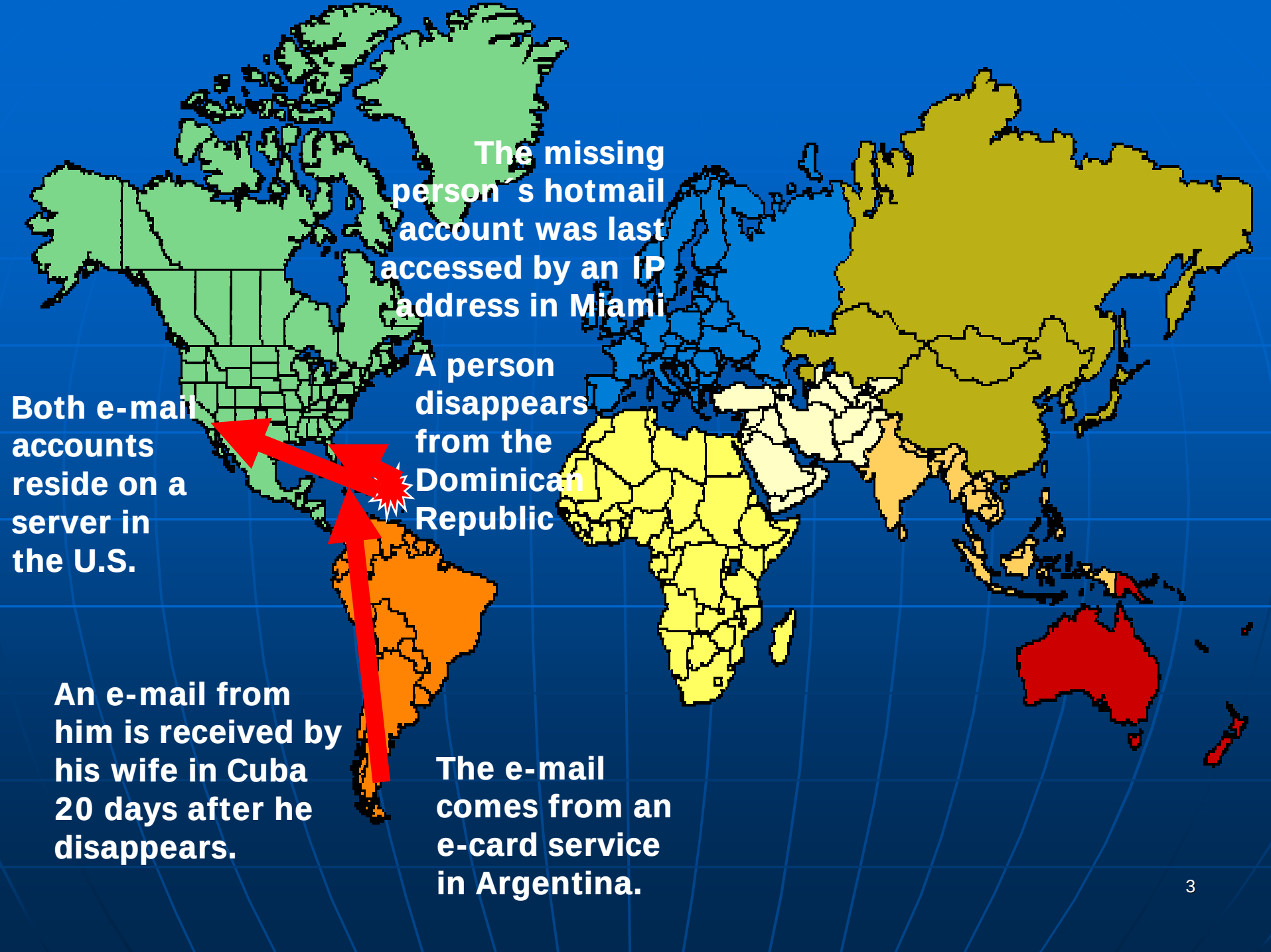
ITU / WSIS Thematic Meeting on Cybersecurity
Geneva, Switzerland June 28 – July 1, 2005

world summit on the information society
Geneva 2003 - Tunis 2005

ITU International Telecommunication Union

Indotel


A Criminal Intrudes into a Bank in Geneva
Canadian agents make the arrest
Korean agents discover attack came from Vancouver
Swiss investigators discover attack came from computer in Buenos Aires
Argentinian investigators discover attack came from Seoul


The missing person´s hotmail account was last accessed by an IP address in Miami
A person disappears from the Dominican Republic
Both e-mail accounts reside on a server in the U.S.
An e-mail from him is received by his wife in Cuba 20 days after he disappears.
The e-mail comes from an e-card service in Argentina.

The Challenges of Globalization of Criminal Investigations

- Countries need to:
  - Enact sufficient **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** to bring criminals to justice.

The Challenges of Globalization of Criminal Investigations

- Countries need to:
  - Enact sufficient **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** to bring criminals to justice.

I. The Need for Criminalization of Attacks on Computer Networks

- Where Country *A* criminalizes certain conduct & Country *B* does not, a bridge for cooperation may not exist
- Extradition treaties
- Mutual Legal Assistance Treaties

Bridging The "Dual Criminality" Divide

- Countries need to reach consensus about what to criminalize
  - APEC Cybersecurity Strategy (2002)
  - U.N. General Assembly Resolution 55/63 (2001)
- Effort to do so: Cybercrime Convention
  - Provides a baseline for substantive law
- Countries then need to actually amend their laws

The Challenges of Globalization of Criminal Investigations

- Countries need to:
  - Enact sufficient **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** to bring criminals to justice.

II. Law Enforcement Needs

- Experts dedicated to High-tech Crime
- Experts available 24 hours a day (home & beeper)
- Continuous training
- Continuously updated equipment (no longer a “flashlight and a gun”)
- Each country needs this expertise

The Challenges of Globalization of Criminal Investigations

- Countries need to:
  - Enact sufficient **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** to bring criminals to justice.

III. The Problem of Locating and Identifying Criminals

- Primary investigative step is to locate source of the attack or communication
  - Very often what occurred is relatively easy to discover, but identifying the person responsible is very difficult
  - Applies to hacking crimes as well as other crimes facilitated by computer networks

In Order to Trace a Communication:

- Only 2 ways to trace a communication:
  1. While it is actually occurring
  2. Using data stored by communications providers

In Order to Trace a Communication:

- Infrastructure must generate traffic data in the first place
- Carriers must have kept sufficient data to allow tracing
  - E.g.: "anonymizers" choose not to collect the data
  - Certain legal regimes require destruction of data
- The legal regime must allow for timely access by law enforcement that does not alert customer
- The information must be shared quickly

Solving the Tracing Dilemma I: Traffic Data

- Countries should encourage providers to generate, and permit them to retain, critical traffic data

- Law enforcement's ability identify and criminals and terrorists is enhanced by access to the data

Solving the Tracing Dilemma II: Law Enforcement Access

- Legal systems must give law enforcement appropriate authorities to access traffic data
  - E.g.: access to stored log files and to traffic information in real-time
- Preservation of evidence by law enforcement
  - Critical given the speed of international legal assistance procedures
  - Must be possible without “dual criminality”
  - Convention on Cybercrime, Article 29

Solving the Tracing Dilemma III: Sharing Evidence

- Countries must improve their ability to share data quickly
- If not done quickly, the electronic "trail" will disappear
- Yet most cooperation mechanisms take months (or years!), not minutes
- Convention on Cybercrime, Article 30: expedited disclosure of traffic data

Solving the Tracing Dilemma III: Sharing Evidence

- When law enforcement gets a request, it should be able to
  1. Preserve all domestic traffic data
  2. Notify the requesting country if the trace leads back to a third country
  3. Provide sufficient data to the requesting country to allow it to request assistance from the third country
- Countries must be able to do this for each other quickly, and on a 24/7 basis

The Challenges of Globalization of Criminal Investigations

- Countries need to:
  - Enact sufficient **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** to bring criminals to justice.

IV. Collecting and Sharing Evidence

- Will evidence collected in the U.S. be admissible in Switzerland?

- Computer forensics:
  - It is easier to deny the threatening e-mail
  - It is easier to hide evidence on a computer
  - It is easier to change electronic evidence by mishandling it

Solutions for Collecting and Sharing Evidence

- Convention on Cybercrime
  - 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

Conclusion

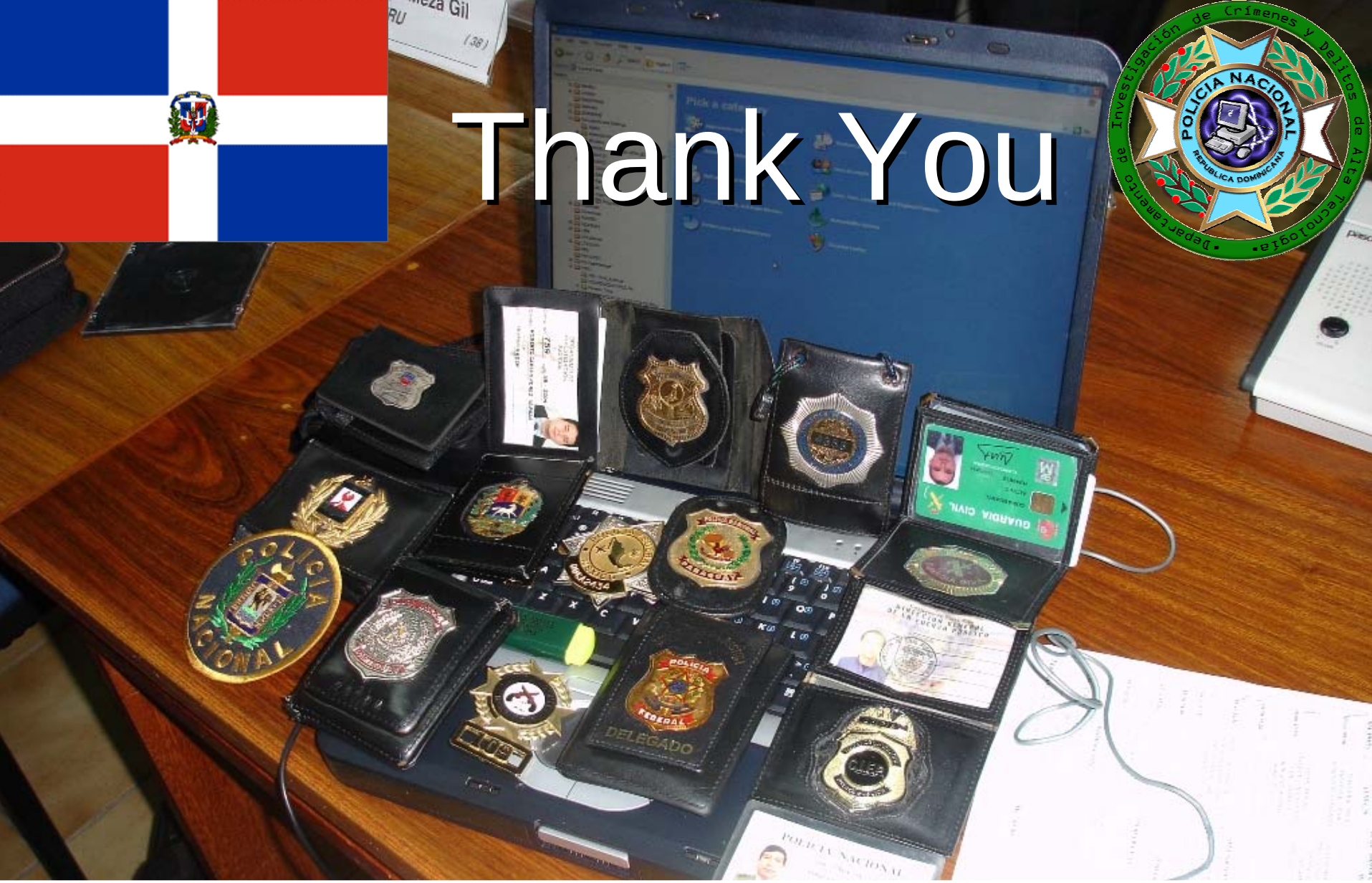
- Every country relies on the others for assistance in responding to the threat of cybercrime

- Each country needs to:
  - Enact adequate substantive and procedural laws
  - Empower its law enforcement authorities to collect evidence for other countries
  - Work to enhance the rapid collection and international sharing of electronic evidence

Future Challenges

We need to start thinking of:

- Cyber-cafés.
  - 70% of criminal activity is coming from public access places.
  - There´s currently no way to identify the user of a computer in a cyber-café.
  - Urgent Need for some level of regulation.
- Wireless networks. Hot Spots


Thank You
POLICIA NACIONAL
REPUBLICA DOMINICANA
Departamento de Investigación de Crímenes y Delitos de Alta Tecnología
POLICIA NACIONAL
POLICIA FEDERAL
DELEGADO
GUARDIA CIVIL