Vincent DANJEAN
Chief, Information Security Incident Response

Initiatives to enhance Cyber Security

Contact : isirt@interpol.int
Contents

Core Functions
Information security assurance
Information security incident response

What can INTERPOL bring?
INTERPOL

- Created in 1923
INTERPOL is the world’s largest international police organisation, with 187 member-countries

- General Secretariat based in Lyon, France
+ Seven Regional Bureaus
+ Special Representatives:
  - United Nations (New York)
  - European Union (Brussels)

- UNODC initiative - Anti-corruption Academy

- Four official languages
Arabic, English, French, and Spanish

- National Central Bureau (NCB) in each Member Country (MC)
National Central Bureaus - NCBs

General Secretariat

Specialised Law enforcement agencies

Airports

Ports

Borders

Police stations
INTERPOL’s Core Function #1

1. Secure global police communications services
2. Operational data Services and Databases for police
3. Operational police support services
4. Police training and development
I-24/7 communications system

187 member countries are connected
I-24/7 Architectures
Connecting police, securing the world

- High-security global police network
  - VPN
  - AES

National Security Officers (NSO)
I-24/7 Features

Connecting police, securing the world

Services available on I-24/7 Network

- NCB web portal
- Automated database queries
- Email (I-24/7 Message)
MIND / FIND
Integrated solutions to access INTERPOL’s databases

• MIND Mobile INTERPOL Network Database
• FIND Fixed INTERPOL Network Database

Benefits of FIND and MIND:
• Brings the INTERPOL databases to the front line.
• Offers real-time information for front-line officers.
• Allows external users to access INTERPOL’s databases.
• No language barriers in technical integration.
FIND: The Swiss experience

SLTD database made accessible to 20,000 Swiss front-line officers in December 2005

Searches (2006)
- Swiss: 4,327,065
- other NCBs: 657,364

Hits (2006)
- Swiss: 1,367
- other NCBs: 1,322
Traffic exchange through the network
(In Millions)

Core function #1: Secure global police communications services
INTERPOL’s Core Function #2

1. Secure global police communications services
2. Operational data Services and Databases for police
3. Operational police support services
4. Police training and development
INTERPOL Notices & Diffusions

- Wanted persons
- Collect information
- Warning about known criminals
- Missing persons
- Unidentified bodies
- Special Interpol-UN Security Council
- Threat Warnings
  + Diffusions
INTERPOL Nominal data

68 792 notices and diffusions as of May 2009

Core function #2: Operational data services and databases for police
INTERPOL Databases

Nominals

DNA

SLTD - Stolen and Lost Travel Documents

Fingerprints

SMV – Stolen Motor Vehicles

ICAID - Child Abuse Images

WOA – Stolen Works of Art

Core function #2: Operational data services and databases for police
INTERPOL stolen and lost travel documents (SLTD) database

Records

<table>
<thead>
<tr>
<th>Year</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>June 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records</td>
<td>13,297,631</td>
<td>13,921,191</td>
<td>16,706,281</td>
<td>18,604,093</td>
</tr>
</tbody>
</table>

Searches

<table>
<thead>
<tr>
<th>Year</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>June 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Searches</td>
<td>4,819,907</td>
<td>19,910,488</td>
<td>75,796,392</td>
<td>117,882,531</td>
</tr>
</tbody>
</table>

Hits

<table>
<thead>
<tr>
<th>Year</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>June 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hits</td>
<td>2,543</td>
<td>6,157</td>
<td>16,465</td>
<td>12,105</td>
</tr>
</tbody>
</table>

145 countries participating as of June 2009
Core function #2: Operational data services and databases for police

INTERPOL nominal database

187 countries participating as of December 2008

Records

2006: 172,980
2007: 177,236
2008: 174,256
June 2009: 174,165

Searches

2006: 704,345
2007: 1,102,071
2008: 7,302,822
June 2009: 7,302,822

32 Million 29 June 09

Wanted

2006: 40,467
2007: 45,652
2008: 49,940
June 2009: 50,902

Hits

2006: 54,620
2007: 117,473
2008: 97,270
June 2009: 54,999

54,999 29 June 09
INTERPOL stolen motor vehicle (SMV) database

Core function #2: Operational data services and databases for police

Records

<table>
<thead>
<tr>
<th>Year</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>3,677,898</td>
</tr>
<tr>
<td>2007</td>
<td>4,247,396</td>
</tr>
<tr>
<td>2008</td>
<td>4,641,016</td>
</tr>
<tr>
<td>June 2009</td>
<td>4,707,830</td>
</tr>
</tbody>
</table>

Searches

<table>
<thead>
<tr>
<th>Year</th>
<th>Searches</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>3,248,946</td>
</tr>
<tr>
<td>2007</td>
<td>2,950,724</td>
</tr>
<tr>
<td>2008</td>
<td>3,835,212</td>
</tr>
<tr>
<td>June 2009</td>
<td>2,207,781</td>
</tr>
</tbody>
</table>

Hits

<table>
<thead>
<tr>
<th>Year</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>33,204</td>
</tr>
<tr>
<td>2007</td>
<td>37,132</td>
</tr>
<tr>
<td>2008</td>
<td>31,332</td>
</tr>
<tr>
<td>June 2009</td>
<td>11,050</td>
</tr>
</tbody>
</table>

121 countries participating as of June 2009
Core function #2: Operational data services and databases for police

Fingerprint database – number of records

Total number of hits: 340
Period 01/01/2009 – 31/05/2009
156 countries participating as of May 2009
DNA database – number of profiles

Total number of hits: 22 for period 01/01/2009-31/05/2009
50 countries participating as of May 2009
Extradition

Comparison resulted that suspect known by two other names and wanted for burglary in Germany

DNA profile sent to INTERPOL

Match with Croatian sample from a burglary suspect in 2003

Austrian police arrested a suspect on burglary charges

INTERPOL databases - a success story

Croatian police confirmed the suspect’s identity

NCB Zagreb sent nominal info + DNA samples + fingerprints to IPSG & NCB Vienna

Austrian police arrested a suspect on burglary charges

Core function #2: Operational data services and databases for police
INTERPOL’s Core Function #3

1. Secure global police communications services
2. Operational data Services and Databases for police
3. Operational police support services
4. Police training and development
Public Safety and Terrorism

Financial and High-Tech Crime

Drugs and Organized Crime

Fugitives Investigative Support

Trafficking in Human Beings

Anti-Corruption

Core function #3: Operational police support services
Operates 24 hours a day
7 days a week
in INTERPOL’s four official languages

Key activities

- Coordinating exchange of information among INTERPOL member countries
- Monitoring message traffic and media sources
- Providing crisis support:
  - Incident Response Teams (IRTs)
  - Disaster Victim Identification (DVI) teams
- INTERPOL Major Events Support Teams (IMESTs)
93 INTERPOL IRT / IMEST / IFST / ILT deployed, as of June 2009

Deployed countries

- Austria
- Bangladesh
- Barbados
- Bosnia H.
- Cameroon
- Cape Verde
- China
- Columbia
- Côte d'Ivoire
- Croatia
- Cyprus
- Egypt
- El Salvador
- Finland
- France
- FYROM
- Germany
- Ghana
- Greece
- Guinea.B
- Guatemala
- Honduras
- Hong Kong
- India
- Indonesia
- Italy
- Jamaica
- Jordan
- Kenya
- Kyrgyzstan
- Lebanon
- Liberia
- Lesotho
- Maldives
- Mauritania
- Mexico
- Morocco
- Pakistan
- Paraguay
- Peru
- Philippines
- Portugal
- Qatar
- S.Arabia
- Senegal
- Singapore
- South Africa
- Spain
- Sri Lanka
- Switzerland
- Thailand
- Trinidad
- Turkey
- Uganda
- Uzbekistan
- USA

48 IRTs – INTERPOL Response Teams
39 IMESTs – INTERPOL Major International Events
1 IFSTs - INTERPOL Field Support Team
5 ILMs - INTERPOL Liaison Mission
INTERPOL’s Core Function #4

1. Secure global police communications services
2. Operational data Services and Databases for police
3. Operational police support services
4. Police training and development
INTERPOL Worldwide Training

60 Training per Year – 1600 trainees

- Train the Trainer
- International Police Training Program (IIPTP)
- Anti-corruption Academy
- Awareness programs
- Forensics and specialised training's

Cyber crime -> Mobile Class Room
"Law enforcement is continually challenged in a more complex and interdependent world to devise innovative ways to protect our citizens and disrupt the criminals that threaten our collective security. Cyber security, transnational threats, drug and human trafficking, terrorist financing – these are problems that transcend boards and cannot be easily addressed unless we take a global approach to fighting them."

Ronald K. Noble
INTERPOL Secretary General
October 8, 2008
INTERPOL ISIRT

Why?

- 2 major attacks against INTERPOL early in 2008
- Both specifically crafted to arm INTERPOL
- A global trend: Historical crime makes more use of ICT
RESULT

- 2008 General Assembly

Tasked INTERPOL General Secretariat to define security policy based on risk assessment *in line with the “internationally accepted standards”* and *in collaboration with the National Central Bureaus*
International Standards

- Information Security Management System (ISMS)

- ISMS is A Code of Best Practice for Information Security, based on International Standard ISO/IEC 27001

- It aims to reduce the highest risks by employing various controls

- Applicable within IPSG (including SRBs)

- Implemented in consultation with NCBs
ISMS - Continuous Improvement

Feedback lessons learned form incidents into Risk Assessment
Recommend policy updates based on experiences and compliance audits
Act to fill gaps in terms of compliance
Follow up on implementation issues

Establish INTERPOL ISMS
Establish Information Security Committee
Perform Business Impact Assessment
Technical Risk Assessment
Draft Policy (ISO 27001)

PLAN

ISMS

DO

CHECK

Audit user compliance with policy
Check implementation of standards and requirements
Respond to information security incidents

Define Standards (Security Requirements)
Communication, training and awareness
Define and Implement Controls
• Technical Controls
• Procedures
• User Manuals and Rules
Key Documentation

INTERPOL Information Security Principles
(The organizational structure of information security)

INTERPOL Information Security Policy
(Which security controls must be implemented in order to reduce risk)

INTERPOL Standards
(Detailed standards describing how individual controls should be implemented)
Information Security Incident Response

- INTERPOL ISIRT
  - Established - Feb 2009
  - 24/7 coverage

- International cooperation
  - June 28 - Annual conference of FIRST
    - Law Enforcement CSIRT Co-operation SIG
      (Kyoto, Japan)

- Capacity Building
  - Sept. 09 - NSO training (Central and South Americas)
A UNIQUE POSITION

Because

- Same issues that the FIRST Members
- Reaching out to 187 National Law Enforcement Forces

A unique understanding of seemingly conflicting interests:

MITIGATE DAMAGE

VS

BRING CRIMINALS INTO JUSTICE
Help each other?

Our roles as Incident Response

Crime statistics and trends
Centralise queries and relay them globally
Promote new tools for both communities
Report crimes

Our roles as Law Enforcement ISP

Continued extension of I-24/7
Training for I-24/7 National Security Officers
Provide first hand information on current attacks
Provide early warning
LOOKING FORWARD TO ANY BRILLIANT IDEAS