Vincent DANJEAN
Chief, Information Security Incident Response

Initiatives to enhance Cyber Security

Contact : isirt@interpol.int

Contents

Core Functions

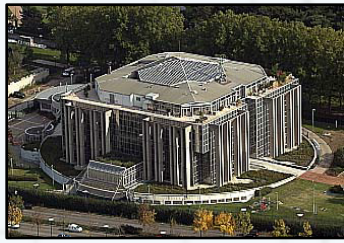
Information security assurance

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

NCBs

Specialised Law enforcement agencies

Airports

Borders

Police stations

Ports

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

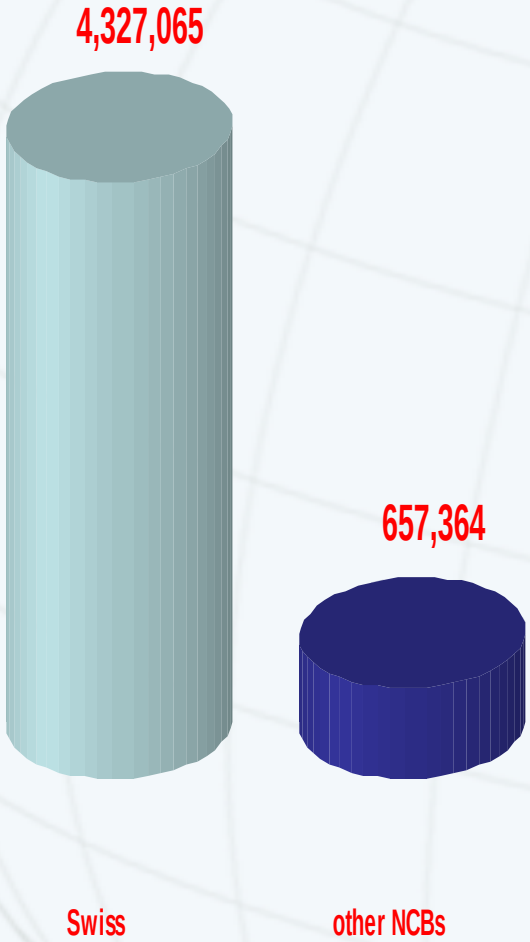
- **MIND Mobile INTERPOL Network Database**
- **FIND Fixed INTERPOL Network Database**

Benefits of FIND and MIND:

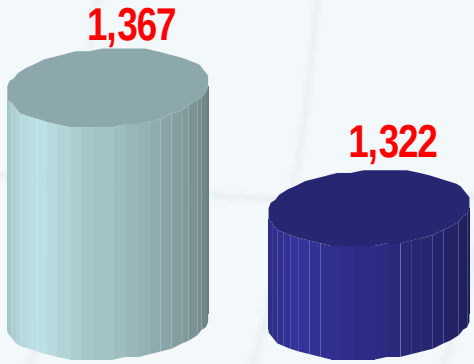
- **Brings the INTERPOL databases to the front line.**
- **Offers real-time information for front-line officers.**
- **Allows external users to access INTERPOL's databases.**
- **No language barriers in technical integration.**

FIND: The Swiss experience

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

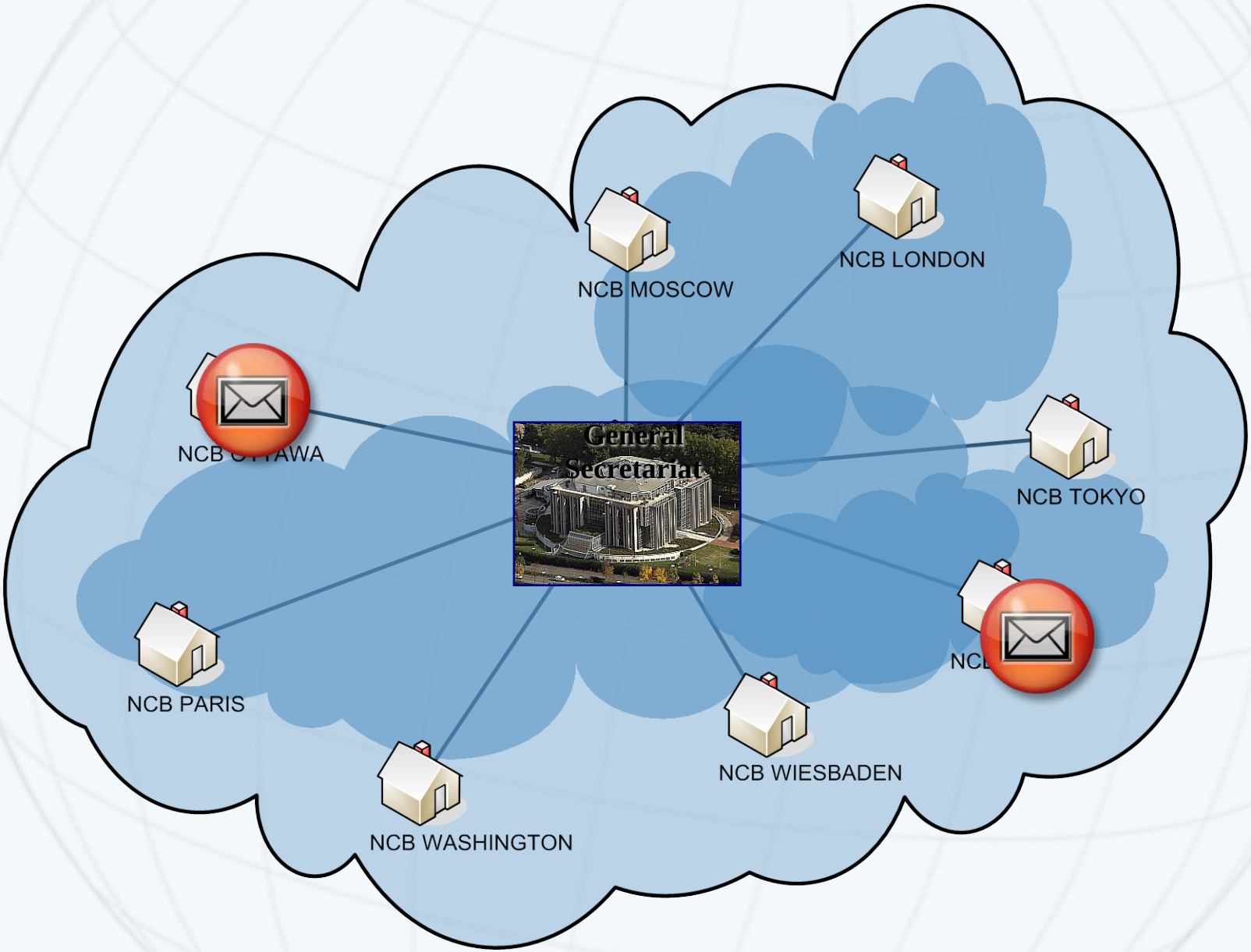


Searches (2006)



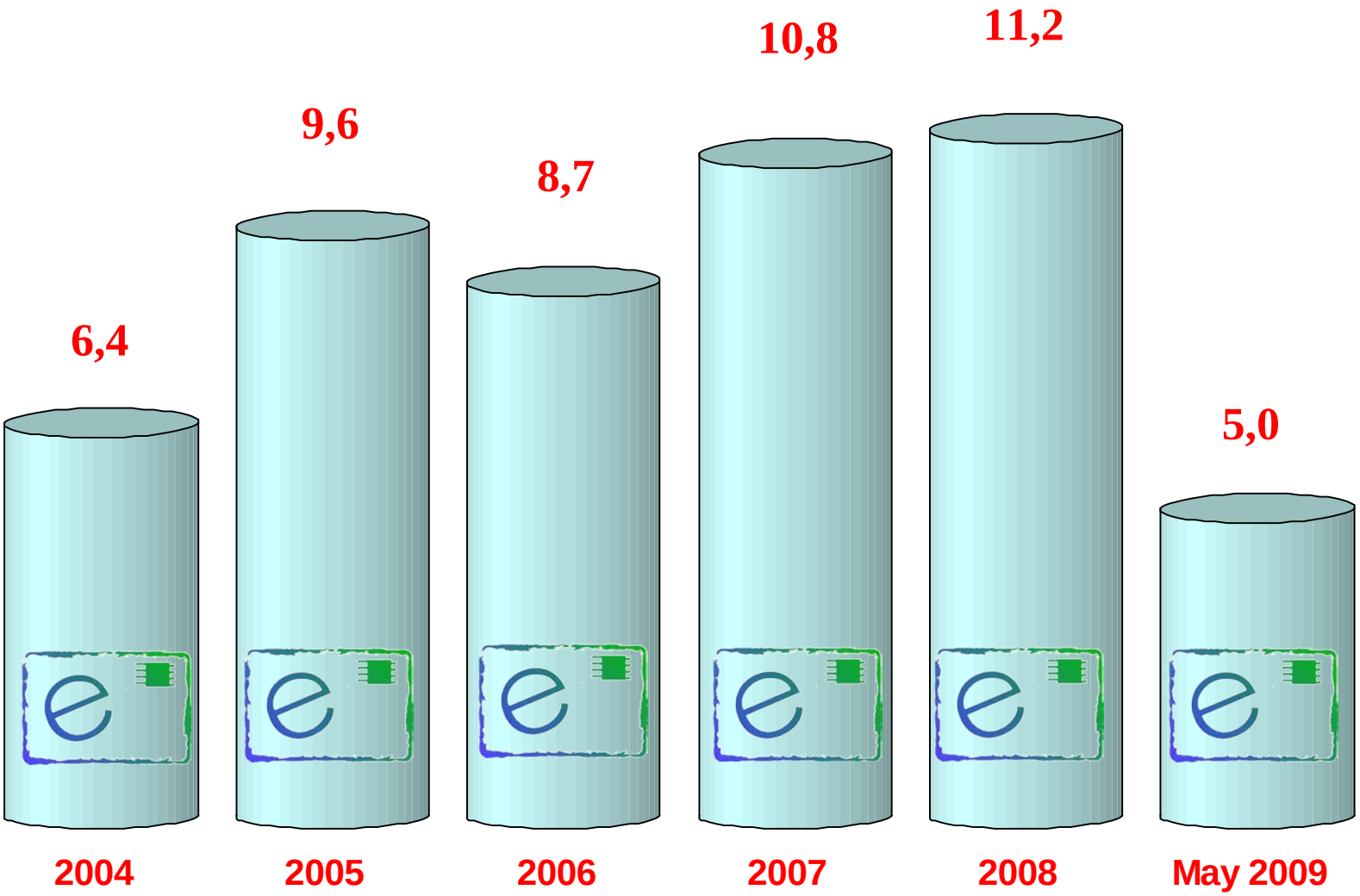
Hits (2006)

I-24/7 Email


NCB MOSCOW
NCB LONDON
NCB OTTAWA
General Secretariat
NCB TOKYO
NCB PARIS
NCB WIESBADEN
NCB WASHINGTON

Traffic exchange through the network

(In Millions)



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

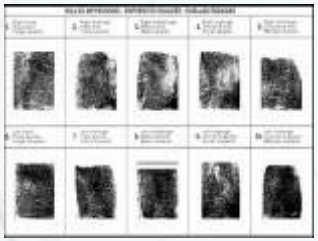
68 792 notices and diffusions as of May 2009

INTERPOL Databases

Nominals

DNA

SLTD - Stolen and Lost Travel Documents



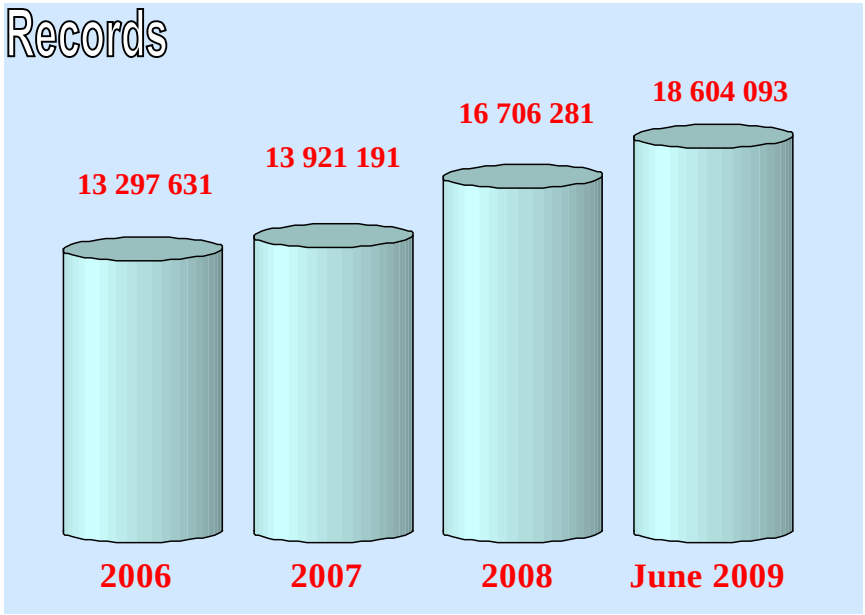
Fingerprints

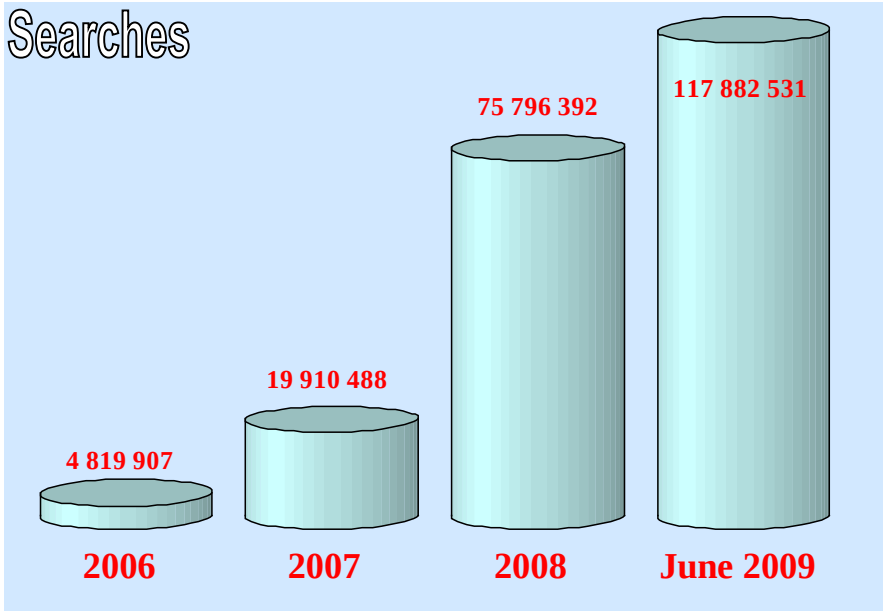
SMV – Stolen Motor Vehicles

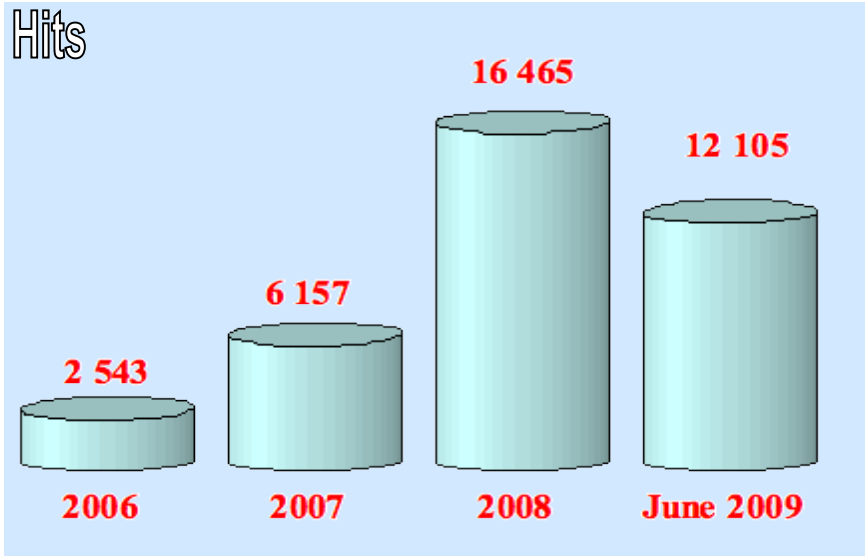
ICAID - Child Abuse Images

WOA – Stolen Works of Art

INTERPOL stolen and lost travel documents (SLTD) database





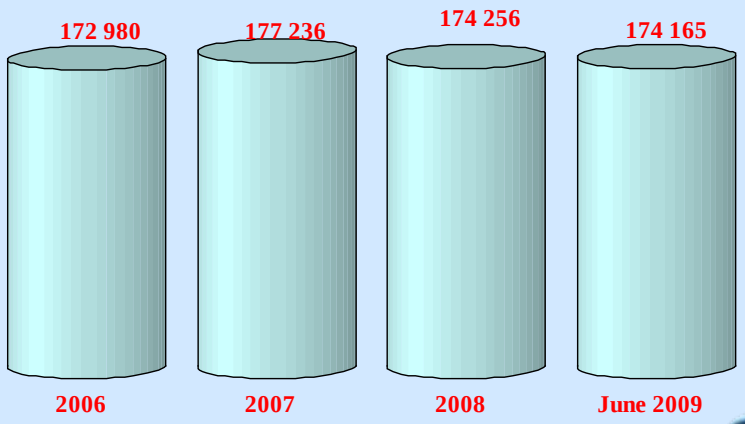


145 countries participating as of June 2009

INTERPOL nominal database

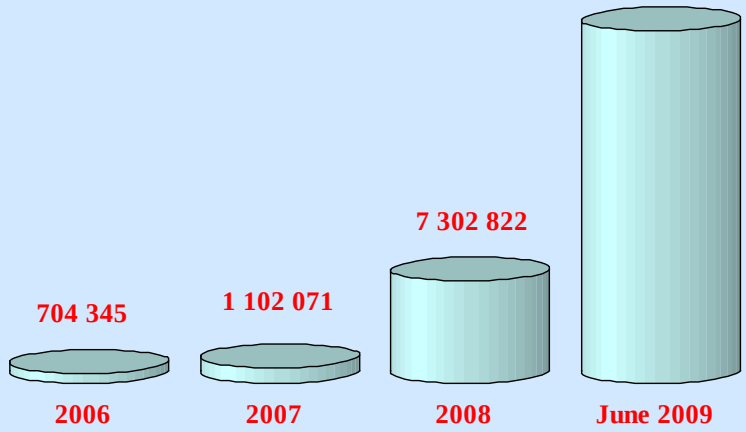
187 countries participating as of December 2008

Records



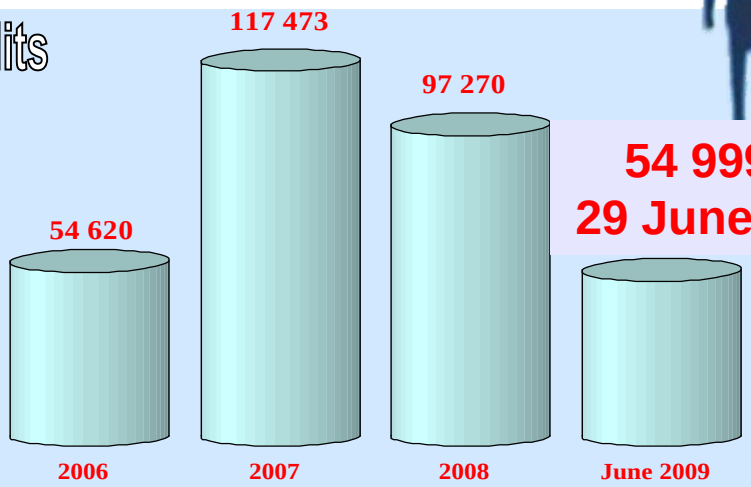
Searches

32 Million 29 June 09

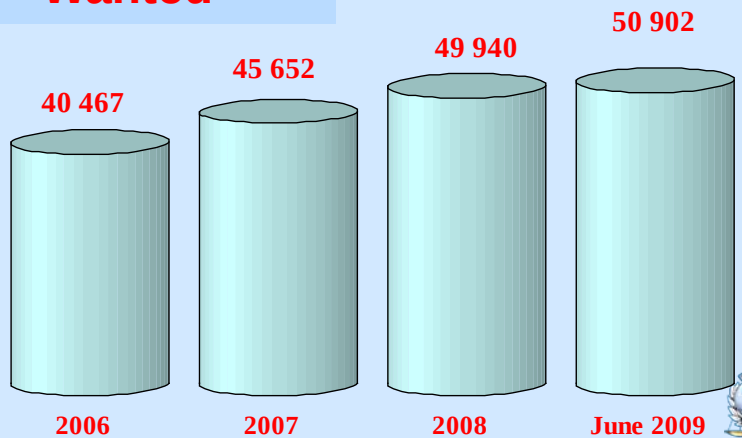


Hits

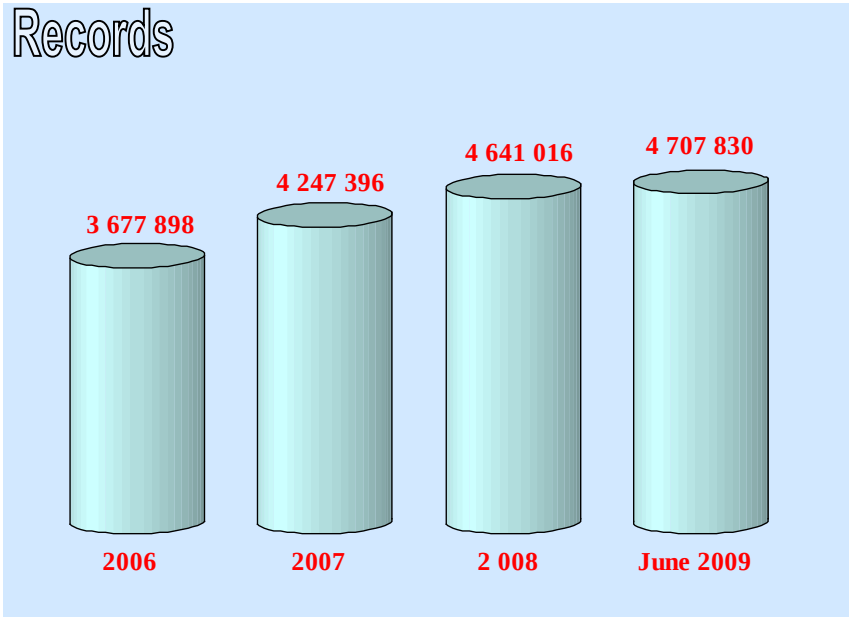
54 999 29 June 09

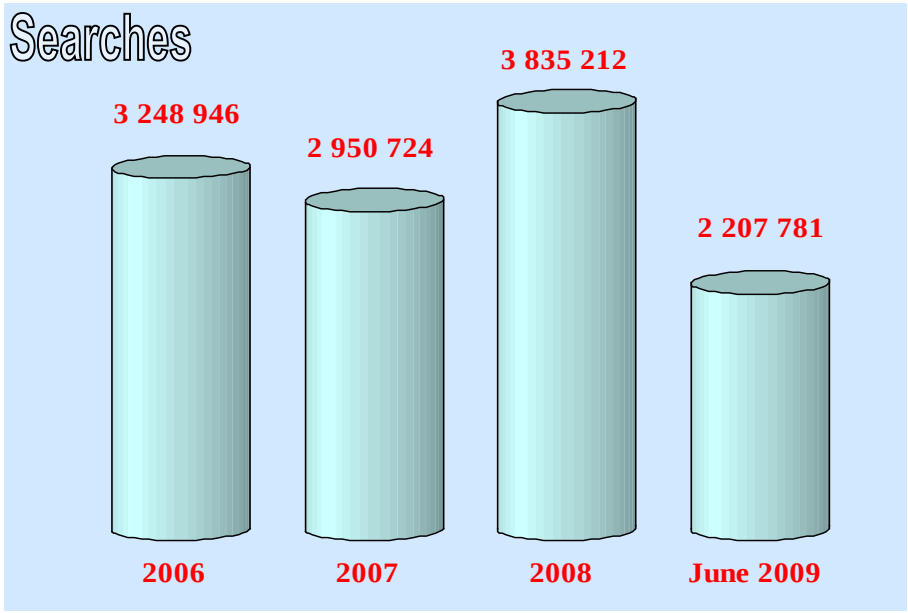


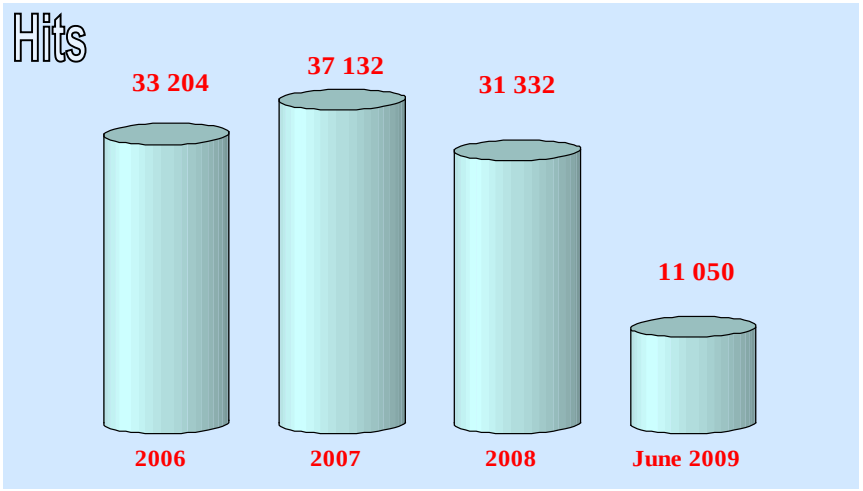
Wanted



INTERPOL stolen motor vehicle (SMV) database







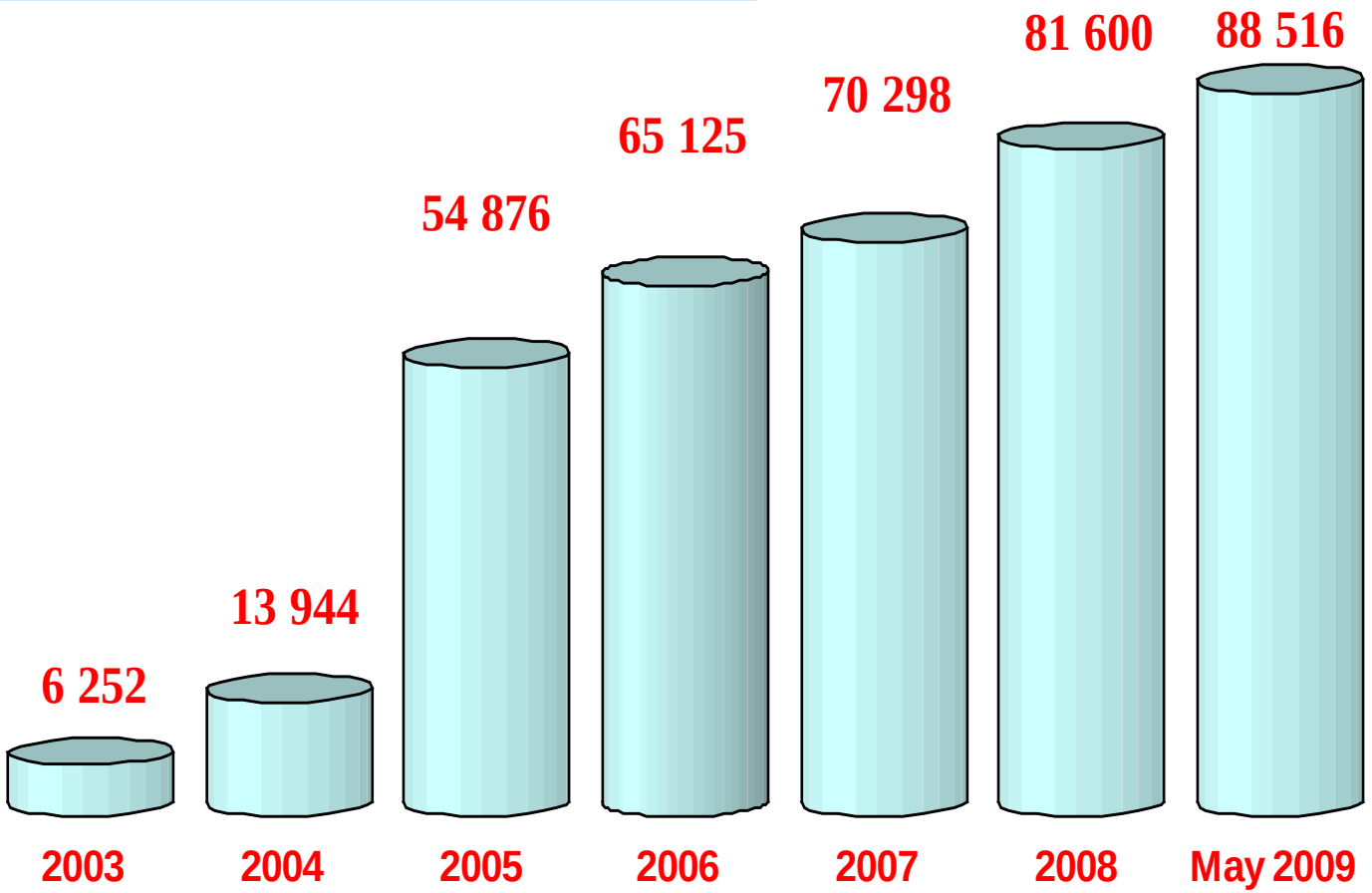
121 countries participating as of June 2009

Fingerprint database – number of records

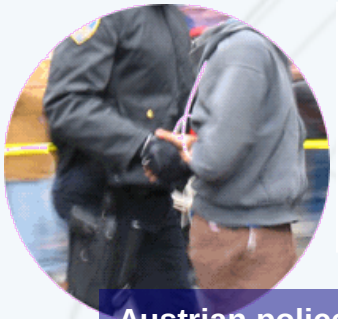
Total number of hits: 340
Period 01/01/2009 – 31/05/2009
156 countries participating
as of May 2009

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



INTERPOL databases - a success story



Austrian police arrested a suspect on burglary charges

DNA profile sent to INTERPOL

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

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

Croatian police confirmed the suspect's identity

Match with Croatian sample from a burglary suspect in 2003

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

Operational Police Support Services

Public Safety and Terrorism

Financial and High-Tech Crime

Drugs and Organized Crime

Fugitives Investigative Support

Trafficking in Human Beings

Anti-Corruption

CCC

INTERPOL's Command and Co-ordination Centre

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
Kyrgistan
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

INTERPOL ISIRT

"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."

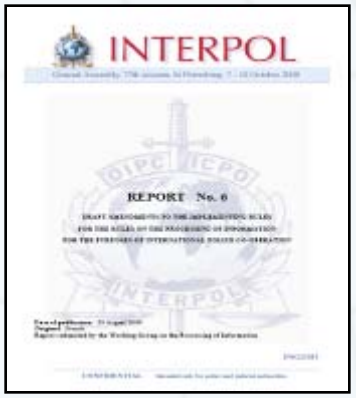
Ronald K. Noble
INTERPOL Secretary General
October 8, 2008

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**

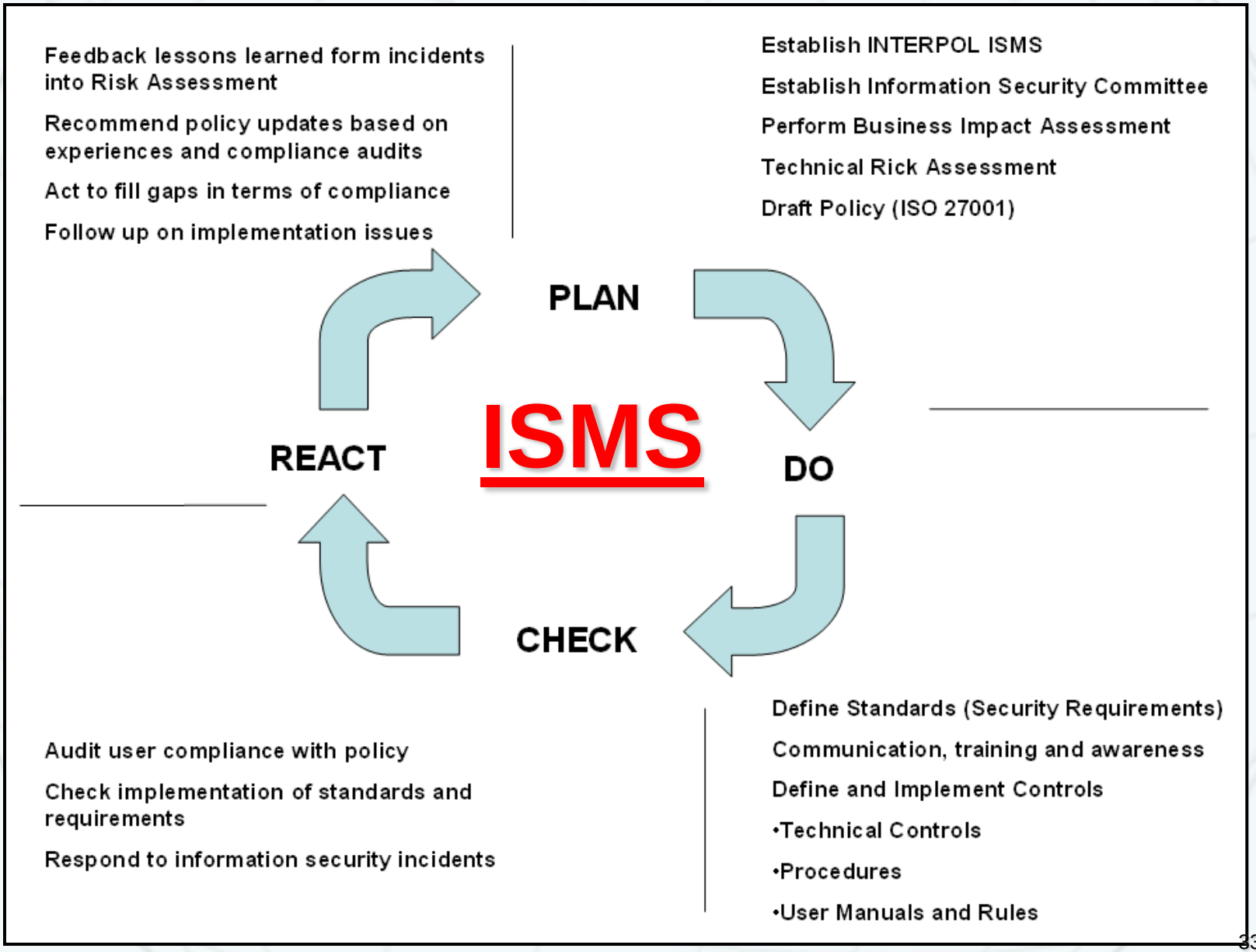
Tasked INTERPOL General Secretariat to define security policy based on risk assessment *in line with the "internationally accepted standards"* and *in collaboration with the National Central Bureaus*

International Standards

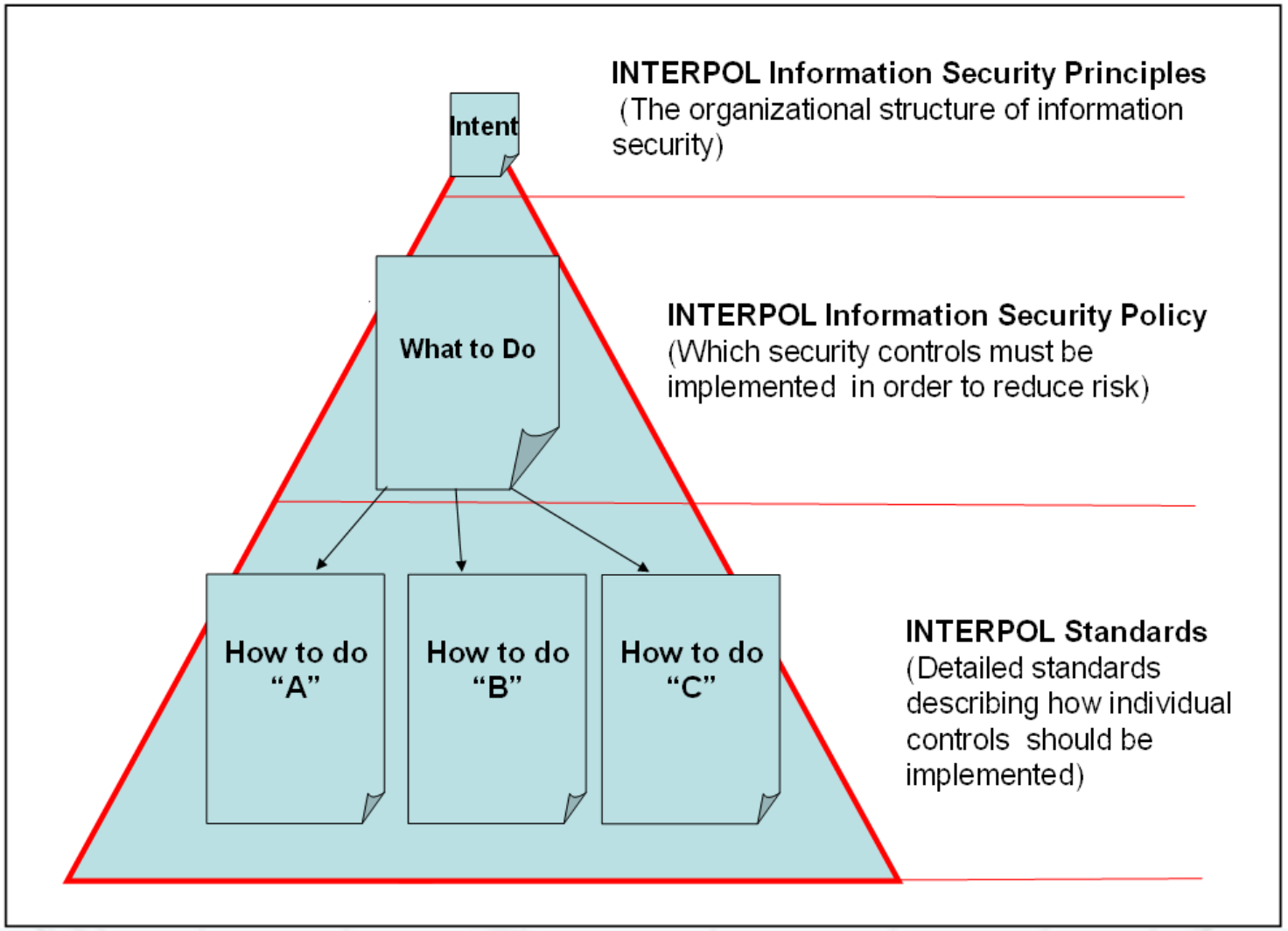
❑ Information Security Management System (ISMS)

- ISMS is A Code of Best Practice for Information Security, based on International Standard ISO/IEC 27001
- It aims to reduce the the highest risks by employing various controls
- Applicable within IPSG (including SRBs)
- Implemented in consultation with NCBs

ISMS - Continuous Improvement



Key Documentation



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

Vincent DANJEAN
Chief, Information Security Incident Response

Contact : isirt@interpol.int