INTERPOL’s
Cyber Centre

ITU Regional Cybersecurity Forum for the Americas

November 2009

Overview

- A glance at INTERPOL
- Introduction to Cybercrime situation
- INTERPOL’s response:
  - Cybercrime Initiative
  - Cybercrime Strategy

INTERPOL – a global organization

- Created in 1923, INTERPOL is the world's largest international police organization, with 188 member countries
- General Secretariat in Lyon, France, six Regional Bureaus, one Liaison Office, and Special Representatives of INTERPOL to the United Nations and to the European Union in Brussels.

- Four official languages: Arabic, English, French and Spanish
- A National Central Bureau (NCB) in each member country

Introduction to Cybercrime Situation

- Internet, a new global scenario
  - Real presence → vurtual presence
  - Hacking, trojan, malware, DOS attack, skimming…
  - Risks?

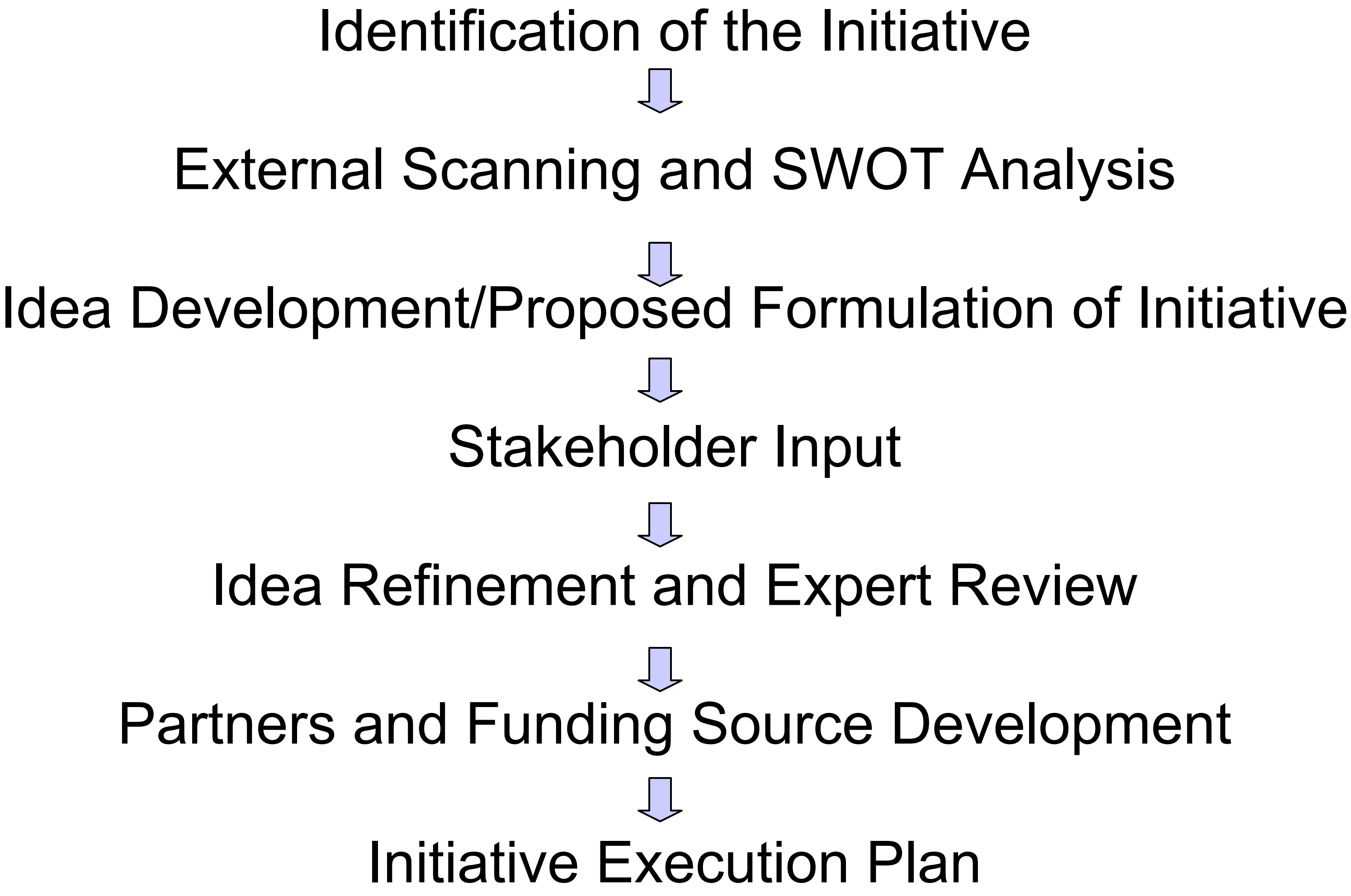
Past state → Future state?

$$Pr(Xn+1= xn+1 \mid X1 = x1, X2 = x2, X3 = x3,\ldots, Xn=xn) = Pr(Xn+1= xn+1 \mid Xn= xn)$$

Cybercrime Initiative

- Supports decisions made at 2008 General Assembly - creation of the Forensics Unit
- The threat is global and expanding
- Member countries vary widely in their capacity, technology, and connectivity

Cybercrime Initiative: A Process Template



Identification of the Initiative

⇩

External Scanning and SWOT Analysis

⇩

Idea Development/Proposed Formulation of Initiative

⇩

Stakeholder Input

⇩

Idea Refinement and Expert Review

⇩

Partners and Funding Source Development

⇩

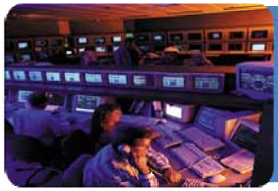
Initiative Execution Plan

INTERPOL

Cybercrime Strategy: Five Focus Areas

1. Computer Forensics, Analysis of Evidence, and Online Investigations

2. Training, Capacity Building, & In-House Support



3. Cyber Domain Situational Awareness

4. Build Public-Private Partnerships

5. Review & Evaluate Technology Impact Law Enforcement

Focus Area One: *Computer Forensics, Analysis of Evidence, and Online Investigations*

Mission Focus

Computer Forensics & Analysis of Evidence

a) Provide core team with technical equipment and subject matter expertise

b) Establish case officers to liaise with associated crime verticals

Online Monitoring & Investigations

a) Establish common protocols for monitoring

b) Provide direct support to member countries

c) Preemptively alert member countries of cyber threats

d) Serve as a trusted broker to expedite sensitive information exchange

Focus Area 2 – Training, Capacity Building, and In-House Support

Mission Focus

Focus Area 2 will expand cyber-based training initiatives, enhance member country capabilities, expand regional partnerships, and provide support for internally-oriented elements of the Center.

1. ***Training & Capacity Building***
   - a) Establish critical mass of accredited trainers
   - b) Provide supplement equipment resources on-the-ground
   - c) Promote remote e-learning opportunities
   - d) Advise private industry on how to properly connect with law enforcement on select cyber incidents
   - e) Promote regional partnerships to scale / replicate internal training efforts
   - f) Subsidize training for less developed countries
   - g) Set initial standards and/or guidelines in cooperation with Training Office
2. ***In-House Support***
   - a) Author basic principles for first responders
   - b) Develop common techniques to ensure anonymous network monitoring
   - c) Implement professional development to keep pace with technological change

Focus Area 3 – Cyber Domain Situational Awareness

Mission Focus

Focus Area 3 will establish a common operating picture (both internal and external) for emerging threats to global networks while leveraging INTERPOL's existing communications and data exchange infrastructure.

1. ***External Component***
   a) Connect domestic cybercrime units to I-24/7 network
   b) Establish incoming link to private Secure Operating Centers to eliminate prevailing disconnect between responding to an incident (temporary patch) and investigating an incident (long-term prevention)
   c) Enable rapid-action response (see potential legal constraint)
   d) Institute early warning system (e.g., purple notices)
   e) Catalog incoming data from the private sector

2. ***Internal Component***
   a) Match compatible databases and aggregate trends observed in crime verticals alongside general cyber trends
   b) De-conflict "blue-on-blue" operations

Focus Area 4 – Build Public-Private Partnerships

Mission Focus

Focus Area 4 will encourage INTERPOL to invest energy in organizations that sit at the nexus between policy and practice, where it can effectively enhance its position and reputation as the global authority on cybercrime.

1. ***Academia***
   a) Construct "cloud" of cyber subject matter experts (networked think tank model)
2. ***International Organizations***
   a) Seed select organizations with presence to establish INTERPOL as the law enforcement authority in cybercrime (e.g., IMPACT)
   b) Continue to influence the policy landscape and forthcoming legislative proposals related to cyber (EC)
   c) Expand focus to other regional groups
3. ***Private Organizations***
   a) Establish data link with Internet Service Providers / DNS Registry Systems
   b) Establish data link with Banking and Financial System
   c) Specialized law enforcement data (e.g., Cymru)
   d) Computer Emergency Response Teams
   e) SANS Institute (Internet Storm Center)

INTERPOL

Focus Area 5 – Review and Evaluate the Impact of Emerging Technology on Law Enforcement

Mission Focus

Focus Area 5 will attempt to mitigate the gap that has grown between the emerging threat and countervailing solutions by investing time in understanding solutions before they come to market.

- Understand emerging technology in the context of its impact on law enforcement (advanced previews)
- Evaluate and endorse hardware / software tools to ensure a progressive baseline for IT security
- Survey development efforts within the law enforcement community and publish new or innovative investigative techniques
- Continue to monitor and advise on malicious toolsets and techniques that are emerging from the hacker community

“We are what we repeatedly do.
Excellence then, is not an act,
but a habit”.

Aristotle

Challenges Ahead

- Sharing information
- Procedures
- Standardized laws
- Predicting emerging risks
- Stakeholders

QUESTIONS?

Jaime Ansieta
Financial and High Tech Crime
ICPO INTERPOL
j.ansieta@interpol.int