INTERPOL Capacity Building and Training Activities

Lili SUN
Head of Training Unit – Cybercrime Directorate
June 15, 2017
Outline

1. General introduction to INTERPOL
2. INTERPOL’s policing capabilities for cyberspace
3. Cyber capacity building programmes
4. The way forward
History of 100 years

1914
First International Criminal Police Congress held in Monaco.

1946
- Rebuilding of the organization after the end of World War II
- A new headquarters set up in Paris
- INTERPOL colour-coded notice system initiated

1956
Renamed as International Criminal Police Organization-INTERPOL

2015
Official inauguration of the INTERPOL Global Complex for Innovation in Singapore.

1989
INTERPOL moves its General Secretariat to Lyon, France.
A Global Presence
Global Facilitator

Organized and Emerging Crime

Counter-Terrorism

Cybercrime
Police Databases

17 databases

Nominal

Stolen Motor Vehicles

DNA

Stolen & Lost Travel Documents

Fingerprints

Ballistic Information
• A warning system- INTERPOL Notices
Secure Communication System (VPN)
Project “Follow the Sun”

GMT 22:45 – 07:15
06:45 - 15:15
(local time)

GMT 06:45 – 15:15
07:45 - 16:15
(Winter - local time)
08:45 - 17:15
(Summer - local time)

GMT 14:45 – 23:15
11:45 - 20:15 pm
(local time)
GLOBAL CYBERCRIME STRATEGY

Attribution: Identification of cybercrime and criminals

- Threat assessment and analysis, trends monitoring
- Access to and exploitation of raw digital data
- Harmonization and interoperability
- Correlation of cyber and physical information
- E-evidence management process
Cyber Fusion Centre

Single point of entry for global cyber related information and intelligence
GLOBAL COORDINATION IN CYBERCRIME INVESTIGATIONS
INTERPOL Regional Working Group on Cybercrime

Americas, Africa, Middle East & North Africa, Eurasian
THREAT ASSESSMENT AND ANALYSIS, TRENDS MONITORING

ATTRIBUTION: IDENTIFICATION OF CYBERCRIME AND CRIMINALS

HARMONIZATION AND INTEROPERABILITY

CORRELATION OF CYBER AND PHYSICAL INFORMATION

ACCESS TO AND EXPLOITATION OF RAW DIGITAL DATA

E-EVIDENCE MANAGEMENT PROCESS

GLOBAL COORDINATION IN CYBERCRIME INVESTIGATIONS

INFORMATION SHARING AND ANALYSIS

CYBER TRAINING

DIGITAL FORENSICS

DIGITAL FORENSICS
Develop and provide specific training courses

Provide digital forensic on-site assistance

Contribute to international standards issuance

Provide guidance on using digital forensic tools and equipment
• INTERPOL e-learning modules on cybercrime

- Open Source Intelligence in Investigations (EN-2-932)
- Launch EN-2-932
- INTERNET Basics e-learning Course (EN-2-931)
- Forest Crime e-learning Course (EN-2-046H)
- Cours en ligne sur la criminalité forestière (FR-2-046H)
- Curso en línea sobre los delitos forestales (SP-2-046H)
- Introduction to Digital Forensics (EN-2-930)
- E-Mail Investigations (EN 2-929)
- Dark Web Investigation Fundamentals (EN-2-926)
INTERPOL Specialized Training

MALWARE ANALYSIS TRAINING

MANILA, PHILIPPINES
24-28 APRIL

SUPPORTED BY:

TREND MICRO

WWW.INTERPOL.INT
Training on Darknet and Cryptocurrencies
INTERPOL Digital Security Challenge

22 March 2017

Ransomware – the new INTERPOL digital security challenge

SINGAPORE – The latest edition of the INTERPOL Digital Security Challenge had participants hunting down a suspect who had encrypted confidential medical records with ransomware.

Cybercrime investigators and digital forensic experts from 20 countries and territories were divided into teams, racing against the clock and each other in order to solve the crime, identify the suspect and gather enough evidence for a successful prosecution.

The aim of the exercise is to provide a realistic simulated environment for specialists to further develop their knowledge and exchange expertise in investigating cybercrimes.

Ransomware is one of the fastest growing types of malware, with a report by Trend Micro showing a 752 per cent increase in new ransomware families in 2016 compared to the previous year.

Easy to deploy, ransomware is a type of malware which blocks a computer, or encrypts the data on a system, with money then demanded to restore functionality, and is estimated to cost businesses hundreds of millions of dollars each year.

Using PCs and laptops pre-loaded with a range of digital forensic tools, the teams won points for each successful stage of the investigation which began with a ‘hospital’ asking for police assistance.
National Cyber Review (NCR)

- Assess and learn from different methods of combating cybercrime
- Towards more harmonized global outlook
Identify specific training needs

Assist in setting up cybercrime investigation or digital forensics

Understand the strength and weakness, as well as identify gaps

Observations and recommendations for enhancing existing institutional, operational, legal and technical framework

DESIRED OUTCOMES
Initiation of National Cyber Review

Inputs to Preliminary Questionnaire

Information Research & Analysis

Country-Visit Consultation

Preparation of Report

Completion of Report
ASEAN Cyber Forensic Investigation Capability

Project start date: 01/01/2015
Project end date: 31/03/2016

Beneficiary agencies:
Specialized units of the Law Enforcement Agencies (LEAs) of ASEAN Countries

Funded by: Global Affairs Canada
Cybercrime Capacity in Latin America and the Caribbean

Project start date: 01/12/2015
Project end date: 31/03/2017

Beneficiary agencies: Cybercrime investigators from targeted member countries in Latin America and the Caribbean.

Funded by: Canada

THE CARIBBEAN: ANGUILLA & BARBUDA, ARUBA, BAHAMAS, BARBADOS, CURACAO, DOMINICAN REPUBLIC, DOMINICA, GRENADA, HAITI, JAMAICA, SINT MAARTEN, ST KITTS & NEVIS, ST LUCIA, ST VINCENT & THE GRENADINES, TRINIDAD & TOBAGO, TURKS & CAICOS
ASEAN Cyber Capacity Development Project

Project start date: Oct. 2016
Project end date: Sep. 2018

Beneficiary agencies: Specialized units of the Law Enforcement Agencies (LEAs) of ASEAN Countries

Funded by: Ministry of Foreign Affairs of Japan
Implementation of Objective 2 activities of GLACY+ Project

Project start date: 01/03/2017
Project end date: 29/02/2020

Beneficiary agencies: Law enforcement officer responsible for cybercrime and electronic evidence in beneficiary countries in Africa, Asia/Pacific, Caribbean and Latin America region.
The Way Forward

INTERPOL Standardized Cyber Curriculum

INTERPOL Cyber Capacity-Building De-confliction Tool/Platform

A

B

C
• Challenges on cybercrime training
  – Improving learning effectiveness
  – Expanding library of content and training programs
  – Delivering consistent service
  – Reducing development cycle times
• Expectations of member countries for INTERPOL
• Roles identified in the Cybercrime lifecycle
• **Frontline officer**
  – Knowledge of ICT
  – Knowledge of current legislation and policies related to crimes using technology
  – Could handle digital evidence properly
• Digital Forensics Specialist
  - Advanced cybercrime awareness
  - Advanced knowledge of legal and jurisdiction issues
  - Expert knowledge in one or more forensics areas
  - Data recovery
  - Chip off forensics
  - Memory forensics
  - Malware analysis and reverse engineering
• Police Officers in various operational units
  – Technical skills
  – Legal skills
• **Cybercrime Intelligence Analyst**
  – Strategic and operational crime analysis
  – Analytical and visualization tools
  – Big data management and analysis
  – Social networks and OSINT
• **Management**
  
  – Profound knowledge of cybercrime
  
  – Advanced knowledge of legal and jurisdiction issues
  
  – Effective relationship management in international cooperation
• Judge/Prosecutor
  – High level cybercrime awareness
  – Knowledge of legal and jurisdiction issues
  – Knowledge of the institutional framework for international cooperation
<table>
<thead>
<tr>
<th>Category</th>
<th>Track</th>
<th>Training</th>
<th>Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Cybercrime Awareness</td>
<td>Responders Track</td>
<td>Fundamentals</td>
<td>INTERPOL Certified Specialist</td>
</tr>
<tr>
<td>Crime Scene Attendance</td>
<td>Digital Forensics Track</td>
<td>Fundamentals</td>
<td>INTERPOL Certified Specialist</td>
</tr>
<tr>
<td>Understanding Digital Evidence</td>
<td>Investigations Track</td>
<td>Fundamentals</td>
<td>INTERPOL Certified Specialist</td>
</tr>
<tr>
<td>General Cybercrime Awareness and types of cybercrimes</td>
<td>Intelligence Track</td>
<td>Fundamentals</td>
<td>INTERPOL Certified Specialist</td>
</tr>
<tr>
<td>Strategic and operational crime analysis</td>
<td>Management Track</td>
<td>Fundamentals</td>
<td>INTERPOL Certified Specialist</td>
</tr>
<tr>
<td>Cybercrime legal issues</td>
<td>Judiciary Track</td>
<td>Fundamentals</td>
<td>INTERPOL Certified Specialist</td>
</tr>
<tr>
<td>General Cybercrime Awareness and types of cybercrimes</td>
<td>Management Track</td>
<td>Fundamentals</td>
<td>INTERPOL Certified Specialist</td>
</tr>
<tr>
<td>General Cybercrime Awareness and types of cybercrimes</td>
<td>Judiciary Track</td>
<td>Fundamentals</td>
<td>INTERPOL Certified Specialist</td>
</tr>
</tbody>
</table>

**Intermediate:***

<table>
<thead>
<tr>
<th>Track</th>
<th>Training</th>
<th>Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Mobile Phone Forensics</td>
<td>Fundamentals</td>
<td>Cybercrime legal issues</td>
</tr>
<tr>
<td>Network Investigations Fundamentals</td>
<td>Fundamentals</td>
<td>Cybercrime legal issues</td>
</tr>
<tr>
<td>Cyber legislation concepts</td>
<td>Fundamentals</td>
<td>Cybercrime legal issues</td>
</tr>
<tr>
<td>Live Data Forensics</td>
<td>Internet Investigations</td>
<td>Cybercrime legal issues</td>
</tr>
<tr>
<td>Network Investigations</td>
<td>Fundamentals</td>
<td>Cybercrime legal issues</td>
</tr>
<tr>
<td>Intermediate Network Forensics</td>
<td>Fundamentals</td>
<td>Cybercrime legal issues</td>
</tr>
<tr>
<td>Linux as an Investigative Tool, part 1</td>
<td>Social media and Open Source Intelligence (OSINT)</td>
<td>Cybercrime legal issues</td>
</tr>
<tr>
<td>Social media and Open Source Intelligence (OSINT)</td>
<td>Big data management and analysis</td>
<td>Cybercrime legal issues</td>
</tr>
<tr>
<td>Introduction to Malware Analysis</td>
<td>Network Investigations</td>
<td>Cybercrime legal issues</td>
</tr>
<tr>
<td>Forensic Scripting</td>
<td>Linux as an Investigative Tool, part 2</td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Advanced Malware Analysis</td>
<td>Databases and data mining</td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Deep web and Virtual Currencies - Darknets</td>
<td>Social media and Open Source Intelligence (OSINT)</td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Cloud Forensics</td>
<td>Wireless LAN &amp; VOIP Investigations</td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Cryptocurrencies forensics</td>
<td>DNS abuse and criminal use of DNS</td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Advanced Mobile Forensic Techniques: JTAG and Chip-off Forensics</td>
<td></td>
<td>Network Investigations</td>
</tr>
<tr>
<td>IOT devices</td>
<td></td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Audio/Video Forensics</td>
<td></td>
<td>Network Investigations</td>
</tr>
</tbody>
</table>

**Advanced:**

<table>
<thead>
<tr>
<th>Track</th>
<th>Training</th>
<th>Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Malware Analysis</td>
<td>Fundamentals</td>
<td>Cybercrime legal issues</td>
</tr>
<tr>
<td>Forensic Scripting</td>
<td>Linux as an Investigative Tool, part 2</td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Advanced Malware Analysis</td>
<td>Databases and data mining</td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Deep web and Virtual Currencies - Darknets</td>
<td>Social media and Open Source Intelligence (OSINT)</td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Cloud Forensics</td>
<td>Wireless LAN &amp; VOIP Investigations</td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Cryptocurrencies forensics</td>
<td>DNS abuse and criminal use of DNS</td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Advanced Mobile Forensic Techniques: JTAG and Chip-off Forensics</td>
<td></td>
<td>Network Investigations</td>
</tr>
<tr>
<td>IOT devices</td>
<td></td>
<td>Network Investigations</td>
</tr>
<tr>
<td>Audio/Video Forensics</td>
<td></td>
<td>Network Investigations</td>
</tr>
</tbody>
</table>
• A certification system
  – INTERPOL Certified Cyber Fundamentals
  – INTERPOL Certified Specialist
  – INTERPOL Certified Expert
• A Train the Trainer approach
  – Scalable
  – Sustainable
De-confliction Tool

- Capacity builders
- Requestors
- Facilitator
1. Optimizing resource utilization/prioritization
2. Coordinate efforts between capacity builders
3. Window for global cyber capacity building
Current status

– Platform has been deployed on INTERPOL Secure Cloud
– A working prototype stage
– Access to approved users will be by username/password issued by INTERPOL, via INTERPOL secure website (https)
Questions:

• Priority countries? Any relating programmes?
• Challenges & solutions?
• The best way to progress?
• Any other matters?
Thank You-Merci-Gracias

l.sun@Interpol.int