



INTERPOL

# INTERPOL Capacity Building and Training Activities

Lili SUN

Head of Training Unit – Cybercrime Directorate

June 15, 2017

# Outline



**General introduction to INTERPOL**



**INTERPOL's policing capabilities for cyberspace**



**Cyber capacity building programmes**



**The way forward**

# History of 100 years

First International Criminal Police Congress held in Monaco.

**1914**



Renamed as International Criminal Police Organization-INTERPOL

**1956**



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

**2015**



**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

**1989**

INTERPOL moves its General Secretariat to Lyon, France.



# A Global Presence



**Organized and  
Emerging Crime**



**Cybercrime**



**Counter-Terrorism**



# 17 databases

**Nominal**



**Stolen Motor Vehicles**



**DNA**



**Stolen & Lost  
Travel Documents**



**Fingerprints**



**Ballistic Information**

## Police Databases

- A warning system- INTERPOL Notices





**I-24/7**

# Secure Communication System(VPN)



# Project “Follow the Sun”

## Singapore



**GMT 22:45 – 07:15**

06:45 - 15:15

(local time)

## Lyon



**GMT 06:45 – 15:15**

07:45 - 16:15

(Winter - local time)

08:45 - 17:15

(Summer - local time)

## Buenos Aires



**GMT 14:45 – 23:15**

11:45 - 20:15 pm

(local time )

**Command and Coordination Centre (CCC)**





# 1 INFORMATION SHARING AND ANALYSIS



# Cyber Fusion Centre

Single point of entry for global cyber related information and intelligence

**HARMONIZATION AND INTEROPERABILITY**

**ATTRIBUTION:  
IDENTIFICATION  
OF CYBERCRIME  
AND CRIMINALS**

**CORRELATION OF  
CYBER AND PHYSICAL  
INFORMATION**

**INFORMATION  
SHARING AND  
ANALYSIS**

**THREAT ASSESSMENT  
AND ANALYSIS, TRENDS  
MONITORING**

**ACCESS TO AND  
EXPLOITATION OF RAW  
DIGITAL DATA**

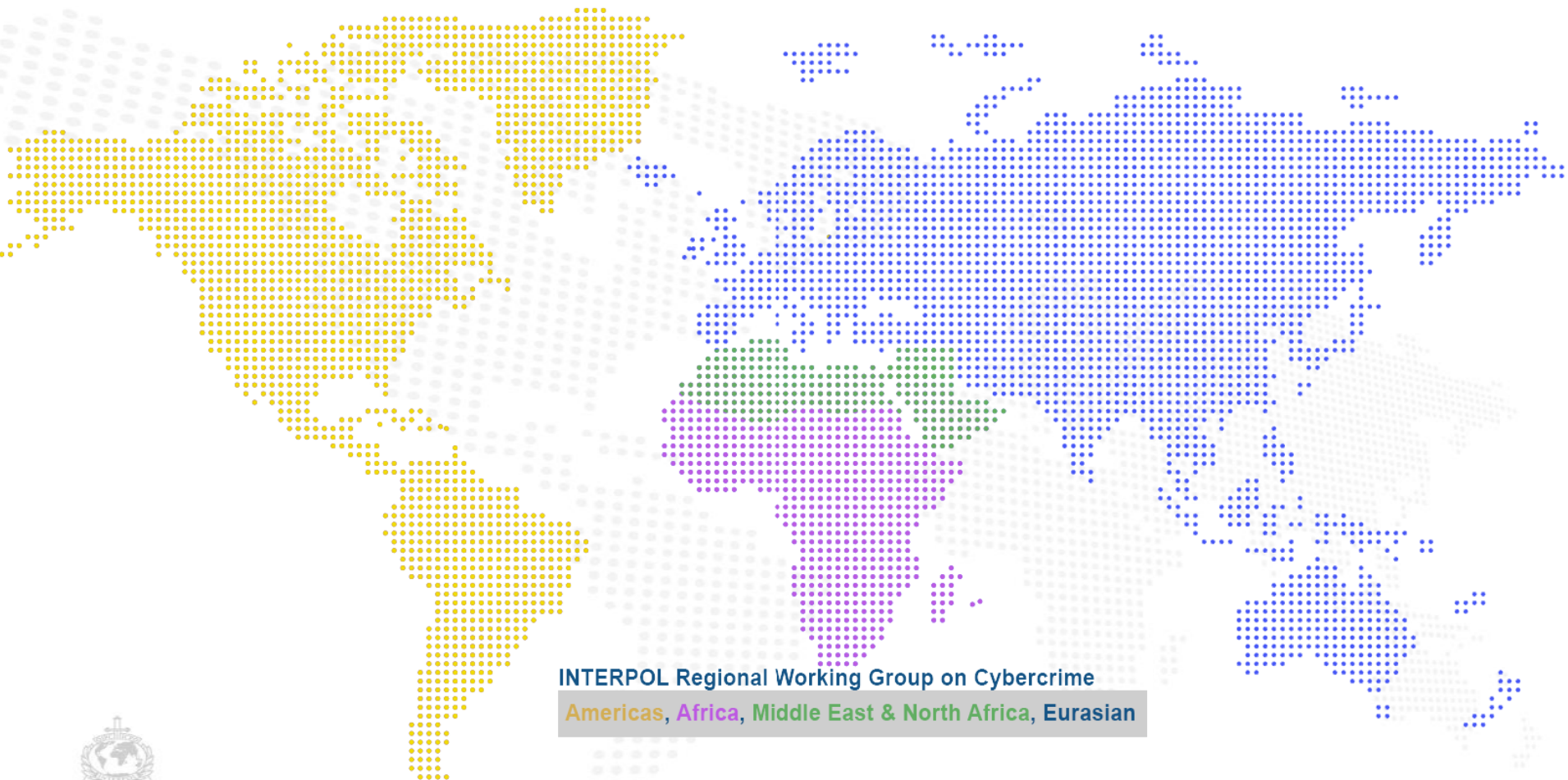
**E-EVIDENCE  
MANAGEMENT  
PROCESS**

**GLOBAL  
COORDINATION IN  
CYBERCRIME  
INVESTIGATIONS**

**CYBER TRAINING**

**DIGITAL FORENSICS**

**2  
GLOBAL  
COORDINATION  
IN CYBERCRIME  
INVESTIGATIONS**



INTERPOL Regional Working Group on Cybercrime  
Americas, Africa, Middle East & North Africa, Eurasian





# 3

## DIGITAL FORENSICS

**B** Provide digital forensic on-site assistance

**C**

Provide guidance on using digital forensic tools and equipment

**A**  
Develop and provide specific training courses

**D** Contribute to international standards issuance







# 4 CYBER TRAINING

# • INTERPOL e-learning modules on cybercrime



I-LE@RN HTTPS Portal

Search for



Utilisateur USRGSLLISUN

EN

Session : 1 - HTTPS - Crime Areas

Management

Courses

Results

Email

Community

Help

Training course

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



INTE



INTERPOL

C  
INVESTI  
FOR EI

## MALWARE ANALYSIS TRAINING

MANILA, PHILIPPINES  
24-28 APRIL

HC  
28 NOVEM

SUPPORTED BY:



[WWW.INTERPOL.INT](http://WWW.INTERPOL.INT)



# • Training on Darknet and Cryptocurrencies



## INTERPOL TRAINING ON DARKNET AND CRYPTOCURRENCIES

SINGAPORE, 15-19 AUGUST 2016

[WWW.INTERPOL.INT](http://WWW.INTERPOL.INT)

# • 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.




SEE ALSO

✓ [Cybercrime](#)


# National Cyber Review (NCR)

- Assess and learn from different methods of combating cybercrime
- Towards more harmonized global outlook

February 2017



INTERPOL



## National Cyber Review

The Internet has eroded physical borders, providing unprecedented opportunities for countries and individuals. This increasing reliance upon the Internet has also created a large number of vulnerabilities, allowing criminal networks operating anywhere in the world to coordinate complex attacks in a matter of minutes. Cybercrime investigations are different from traditional police investigations, requiring high-level technical expertise and cross-jurisdictional cooperation, which many countries do not yet have the capabilities to conduct alone.

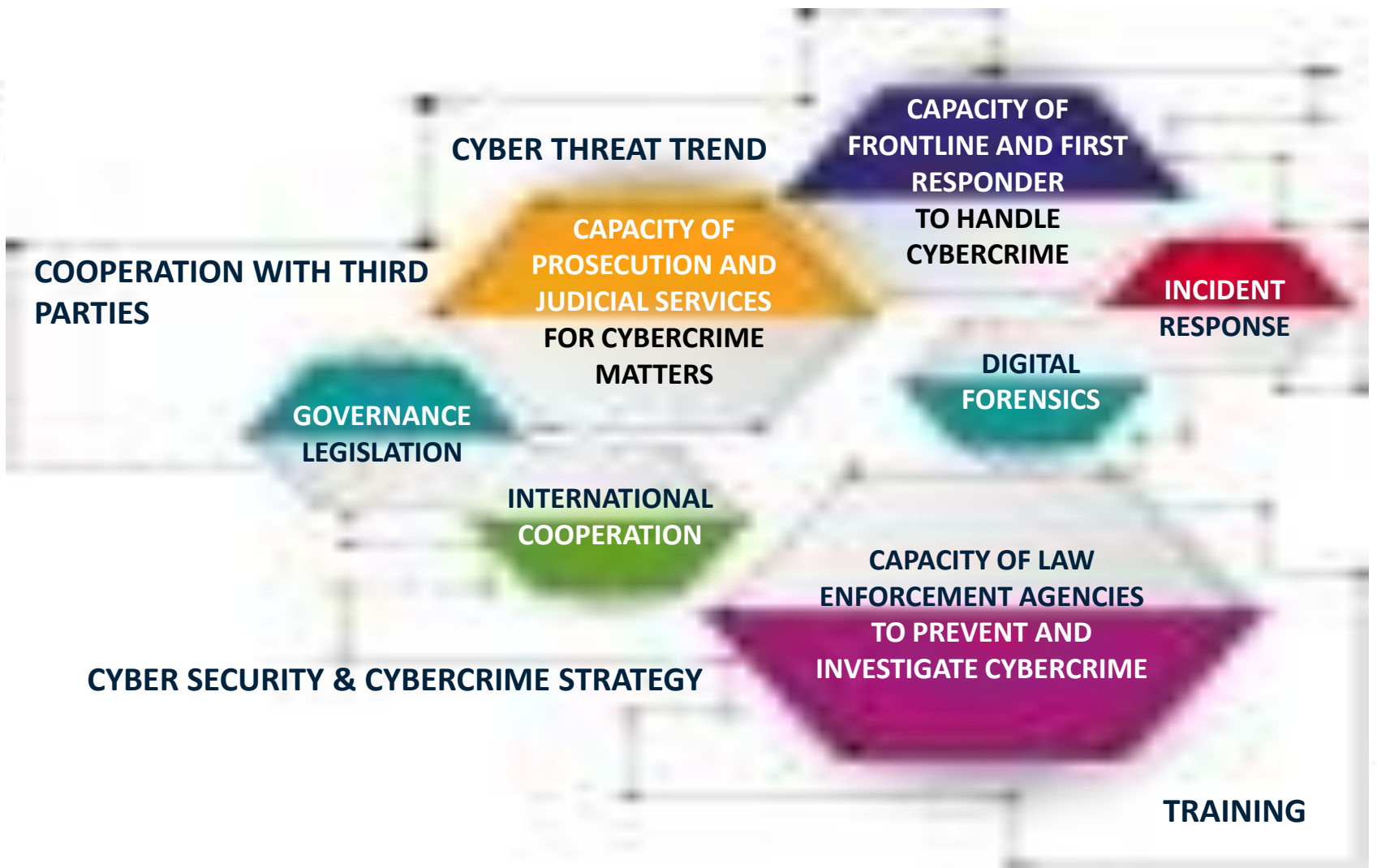
A significant activity for the INTERPOL Global Complex for Innovation (GCI) is therefore to enhance member countries' capability to fight digital crime. Many opportunities exist for INTERPOL to work with partner agencies and organizations to deliver targeted training programmes to member countries.

In addition, a broad range of other intergovernmental organizations are also involved in delivering cybercrime investigation and digital forensics training.

Combating cybercrimes, which are multi-jurisdictional in nature, requires a high degree of interoperability amongst different jurisdictions. However, vast differences in operational capabilities, legal systems, rules and procedures pose challenges to efforts to combat cybercrime. To address these concerns, INTERPOL has created the National Cyber Review (NCR) tool to assess and learn from the different methods of combating cybercrime and ultimately move towards a more harmonized global outlook.

LEADING POLICE INNOVATION

# Assessment Areas





**Identify specific training needs**

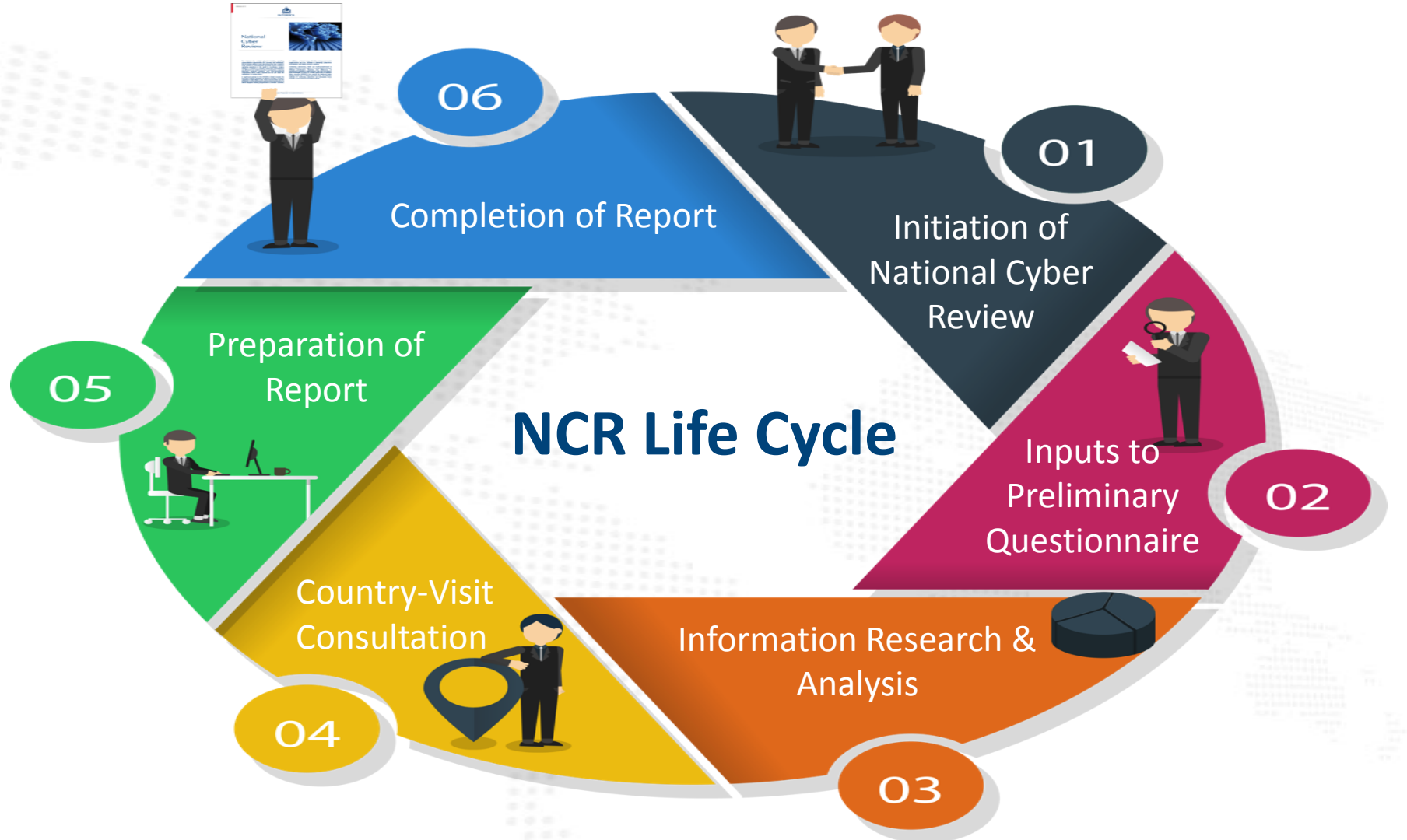
**Assist in setting up cybercrime investigation  
or digital forensics**

**Understand the strength and weakness, as well as  
identify gaps**

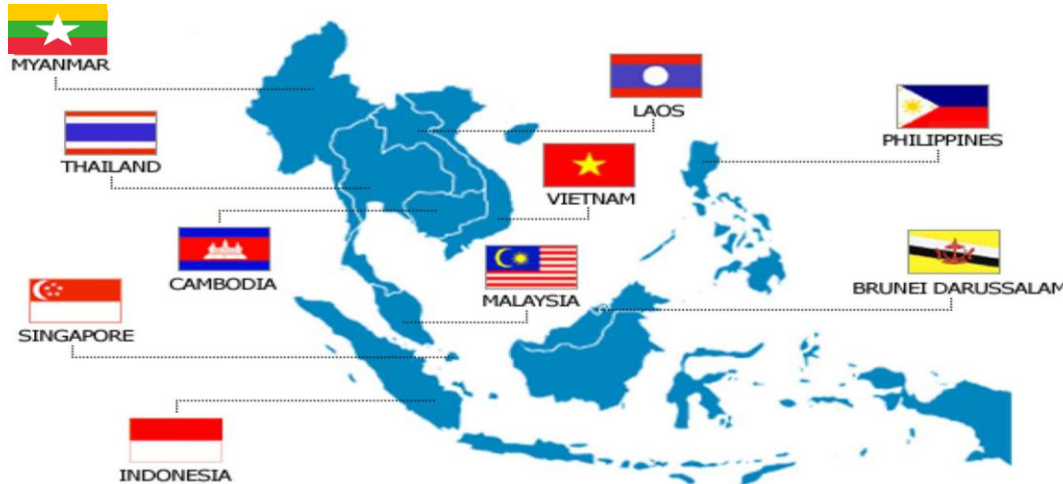
**Observations and recommendations for enhancing existing  
institutional, operational, legal and technical framework**

**DESIRED  
OUTCOMES**





# 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

Affaires mondiales  
Canada

# Cybercrime Capacity in Latin America and the Caribbean



THE CARIBBEAN: ANTIGUA & BARBUDA, ARUBA,  
BAHAMAS, BARBADOS, CUBA, CURACAO,  
DOMINICAN REPUBLIC, DOMINICA, GRENADA,  
HAITI, JAMAICA, SINT MAARTEN, ST KITTS & NEVIS,  
ST LUCIA, ST VINCENT & THE GRENADINES,  
TRINIDAD & TOBAGO, TURKS & CAICOS

**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: 

Global Affairs  
Canada

Affaires mondiales  
Canada

# 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**

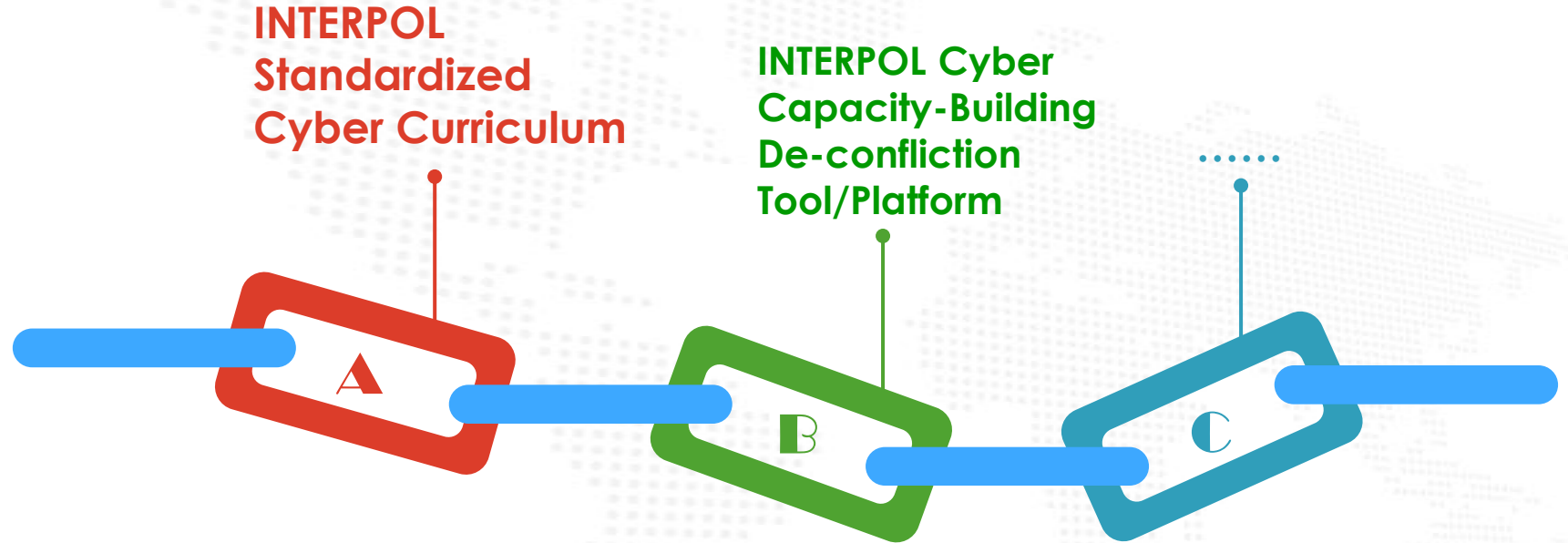
**Beneficiary agencies:** Law enforcement officer responsible for cybercrime and electronic evidence in beneficiary countries in Africa, Asia/Pacific, Caribbean and Latin America region.

Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe

# The Way Forward



- **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**



**CERTIFIED**



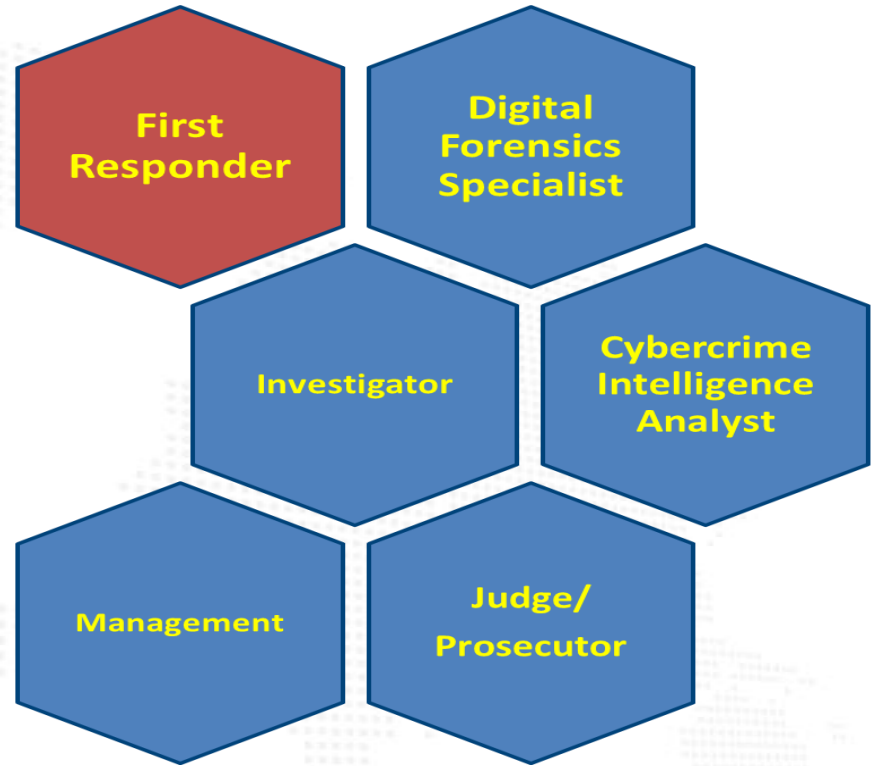
INTERPOL



- **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

First  
Responder

Digital  
Forensics  
Specialist

Investigator

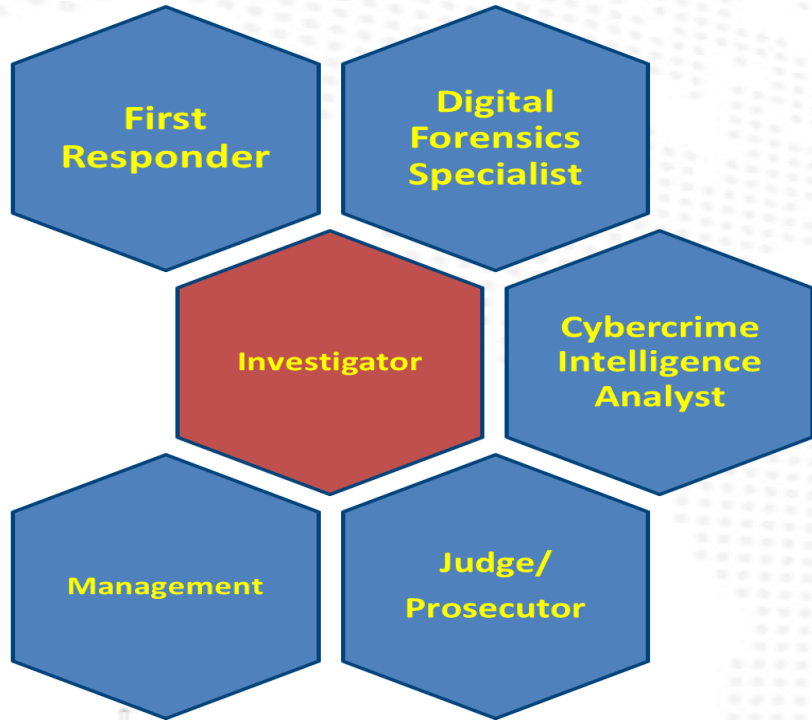
Cybercrime  
Intelligence  
Analyst

Management

Judge/  
Prosecutor



INTERPOL

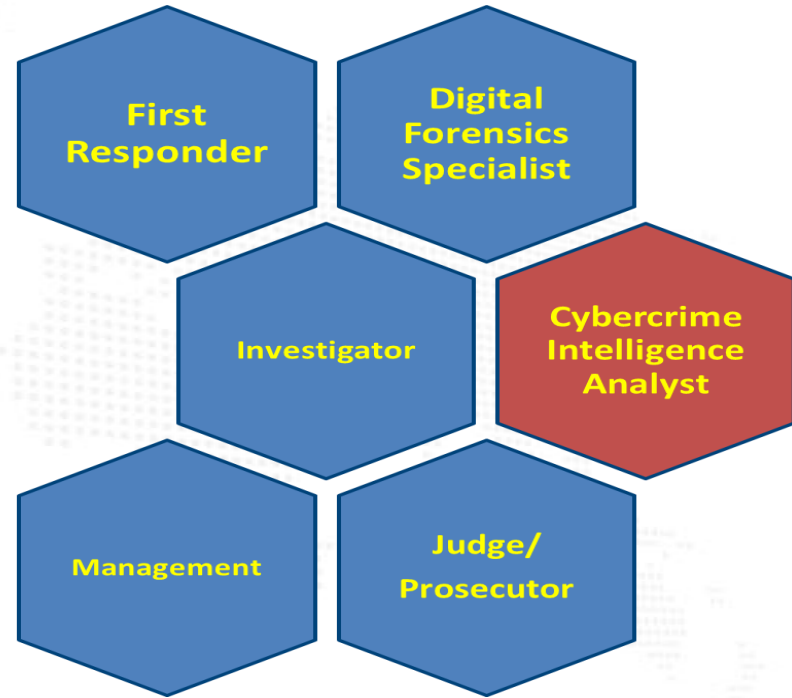


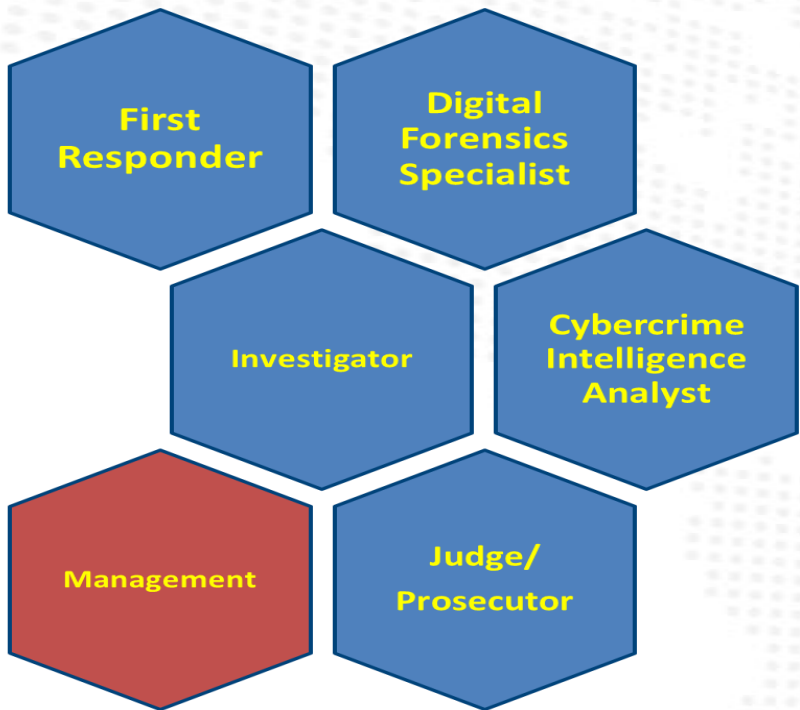
- **Police Officers in various operational units**

- 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



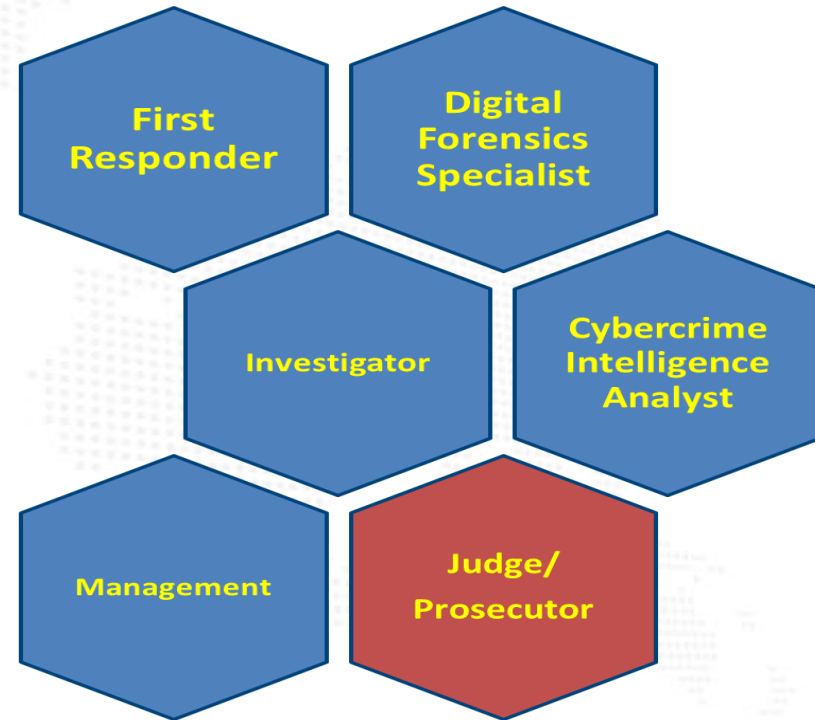


- **Management**

- Profound knowledge of cybercrime
- Advanced knowledge of legal and jurisdiction issues
- Effective relationship management in international cooperation

- **Judge/Prosecutor**

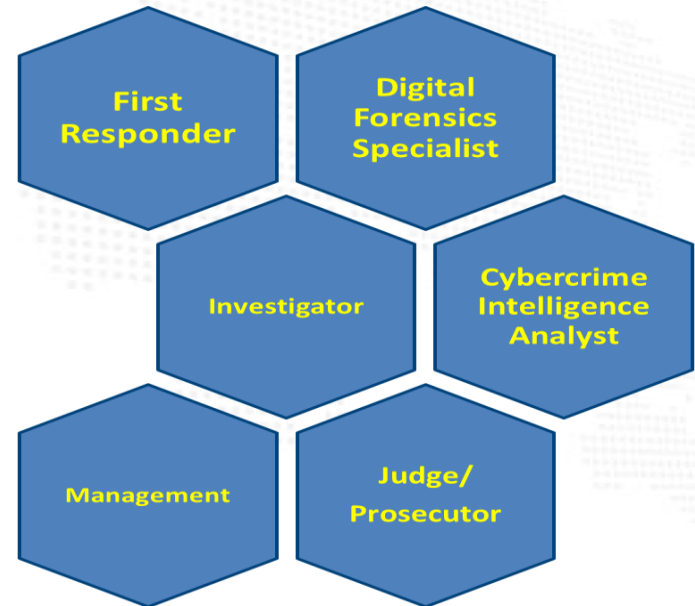
- High level cybercrime awareness
- Knowledge of legal and jurisdiction issues
- Knowledge of the institutional framework for international cooperation



	TRAINING				AWARENESS		
	1 Response Track	2 Digital Forensics Track	3 Investigative Skills Track	4 Intelligence Track	5 Management Track	6 Judiciary Track	
Fundamentals	General Cybercrime Awareness	Introductory Forensic IT	General Cybercrime Awareness and types of crimes	General Cybercrime Awareness	General Cybercrime Awareness and types of crimes	General Cybercrime Awareness and types of crimes	INTERPOL Certified Specialist
	Crime Scene Attendance	Core Mobile Phone Forensics	Network Investigations Fundamentals	Strategic and operational crime analysis	Cybercrime legal issues	Cybercrime legal issues	
	Understanding Digital Evidence	Basic Commercial Tools Training	Internet Investigation Fundamentals		Managing a Cybercrime/Digital Forensics Unit	Network Investigations Fundamentals	
		Windows Forensics(NTFS)	Cybercrime legal issues		Network Investigations Fundamentals		
Intermediate	Cyber legislation concepts	Live Data Forensics	Internet investigations	Analytical and visualisation tools	Managing a Cybercrime/Digital Forensics Unit	Internet investigations	
	Risks of cyber investigations	Intermediate Network Forensics	Network Investigations	Network Investigations Fundamentals	Managing an international cyber investigation	Network Investigations	
		Intermediate Mobile Phone Forensics	Linux as an Investigative Tool, part 1	Social media and Open Source Intelligence (OSINT)	Internet investigations	Social media and Open Source Intelligence (OSINT)	
		Linux as an Investigative Tool, part 2	Social media and Open Source Intelligence (OSINT)	Big data management and analysis	Network Investigations		
Advanced		Introduction to Malware Analysis					
	Jurisdiction specific SOP	Forensic Scripting	Linux as an Investigative Tool, part 2	Databases and data mining	Social media and Open Source Intelligence (OSINT)		
	Awareness on new trends in technology	Advanced Malware Analysis	Deep web and Virtual Currencies - Doarklis				
		Cloud forensics	Wireless LAN & VOIP Investigations				
		Cryptocurrencies forensics	DNS abuse and criminal use of DNS				
		IOT devices					
		Advanced Mobile Forensic Techniques: JTAG and Chip-off Forensics					
	Decryption						
	Audio/Video Forensics						



- **A certification system**
  - INTERPOL Certified Cyber Fundamentals
  - INTERPOL Certified Specialist
    - INTERPOL Certified Expert



- **A Train the Trainer approach**

- Scalable
- Sustainable



Capacity  
builders

Requestors

De-confliction Tool

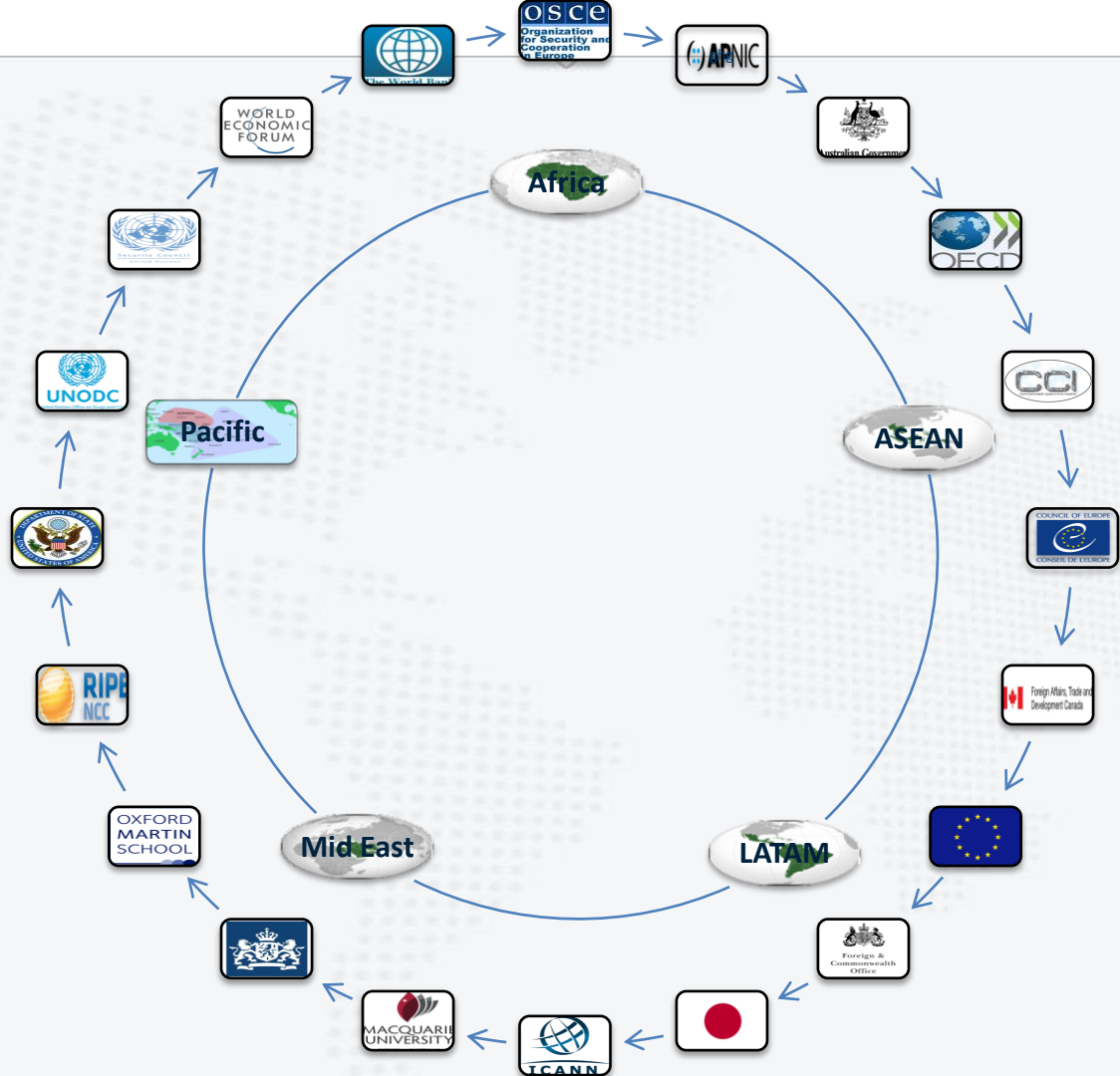
Facilitator

Optimizing resource utilization/prioritization **1**

Coordinate efforts between capacity builders **2**

Window for global cyber capacity building **3**





## 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?



نشكركم جزيل الشكر على انتباهكم  
**Thank You-Merci-Gracias**

[I.sun@Interpol.int](mailto:I.sun@Interpol.int)