INTERPOL's Approach in the Fight Against Cybercrime

Dong-Uk KIM (uKim)

Specialized Officer, GLACY+ Project Manager
Cybercrime Directorate
INTERPOL Global Complex for Innovation

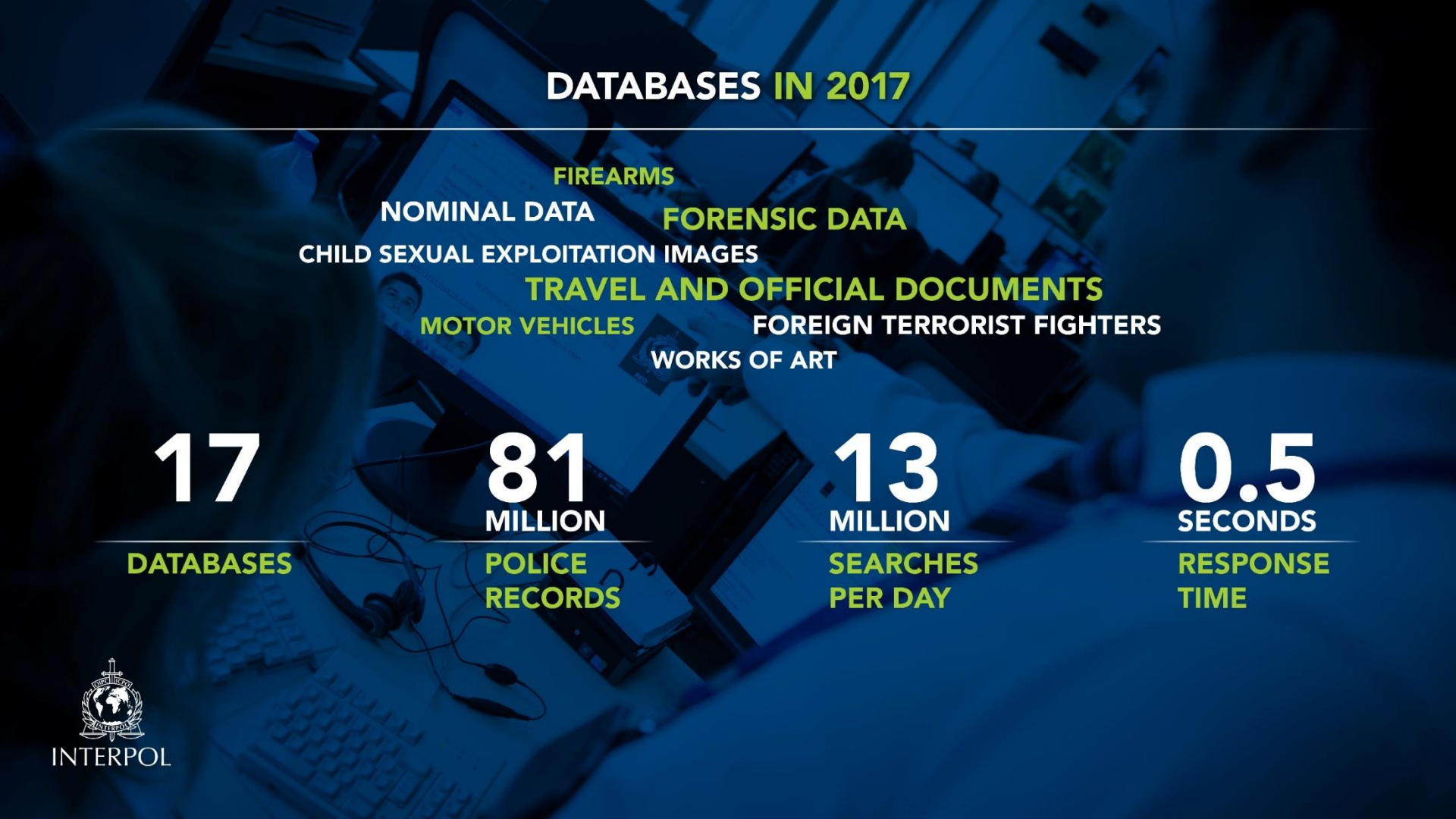
A GLOBAL STRUCTURE

INTERPOL

192 MEMBER COUNTRIES CONNECTED THOUGH A SECURE NETWORK

INTERPOL

Secure Communication System(VPN)


DATABASES IN 2017
FIREARMS
NOMINAL DATA
FORENSIC DATA
CHILD SEXUAL EXPLOITATION IMAGES
TRAVEL AND OFFICIAL DOCUMENTS
MOTOR VEHICLES
FOREIGN TERRORIST FIGHTERS
WORKS OF ART
17
DATABASES
81
MILLION
POLICE RECORDS
13
MILLION
SEARCHES PER DAY
0.5
SECONDS
RESPONSE TIME
INTERPOL

INTERPOL Global Complex for Innovation

CYBERCRIME DIRECTORATE

Digital Crime Investigative Support (DIS)

Coordinating and facilitating transnational cybercrime investigations and operations which involve intelligence sharing and providing guidance on best practices in conducting cybercrime investigations.

Cybercrime Training

Providing range of training courses, targeted to the needs of participants, covering topics such as emerging trends in cybercrime, investigation techniques, digital forensics and more

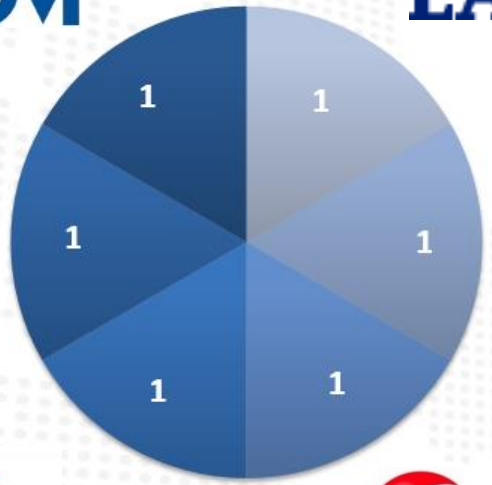
Strategy & Outreach

Bridging the gap between the police and information communication technology communities, bringing them together to fight cybercrime and to prepare for its future developments

Cyber Fusion Centre

A secure and neutral collaboration workspace for law enforcement & industry to share & develop cyber intelligence to tackle cybercrime and cyber-enabled crime

6 Experts working in IGCI



Experts Assignment Agreement

Example of Business Email Compromise

Compromising email via social engineering, phishing
e.g. Keylogger, malware

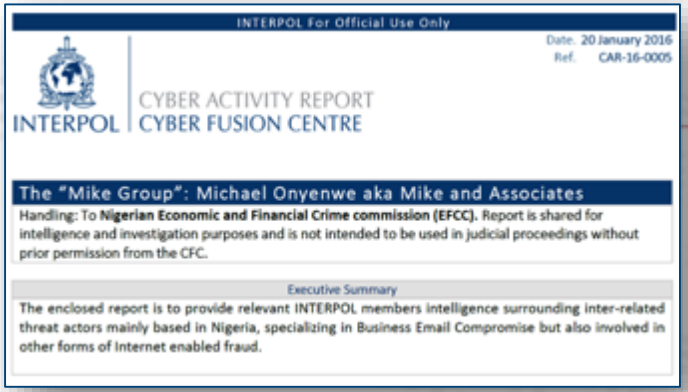
Monitor of email exchange or account takeover
Understanding the business model, activities, relations and etc

Send email to request fund transfer
Via compromised email account or spoof email

Payment transferred
To Criminal's designated account

Money transferred thru network of money mules

A network of criminals orchestrating the scheme



INTERPOL For Official Use Only

Date. 20 January 2016
Ref. CAR-16-0005

INTERPOL | CYBER ACTIVITY REPORT
CYBER FUSION CENTRE

The "Mike Group": Michael Onyenwe aka Mike and Associates

Handling: To **Nigerian Economic and Financial Crime commission (EFCC).** Report is shared for intelligence and investigation purposes and is not intended to be used in judicial proceedings without prior permission from the CFC.

Executive Summary

The enclosed report is to provide relevant INTERPOL members intelligence surrounding inter-related threat actors mainly based in Nigeria, specializing in Business Email Compromise but also involved in other forms of Internet enabled fraud.

Ringleader of global network behind thousands of online scams arrested in Nigeria

The 40-year-old Nigerian national, known as 'Mike', is believed to be behind scams totalling more than USD 60 million involving hundreds of victims worldwide. In one case a target was conned into paying out USD 15.4 million.

Charges including hacking, conspiracy and obtaining money under false pretences.

Business Email Compromised

targeted businesses were payment diversion fraud – where a supplier's email would be compromised and fake messages would then be sent to the buyer with instructions for payment to a bank account under the criminal's control – and 'CEO fraud'.

INTERPOL

THE ANATOMY OF BUSINESS EMAIL COMPROMISE

3 TOXIC INGREDIENTS

Low cost!
Low risk!
High rate of return!

= **Millions in illegal profits**

Hacking

An email account is compromised through malware, employee intrusion, etc.

Social engineering fraud

The victim is manipulated into providing information or funds.

Money laundering

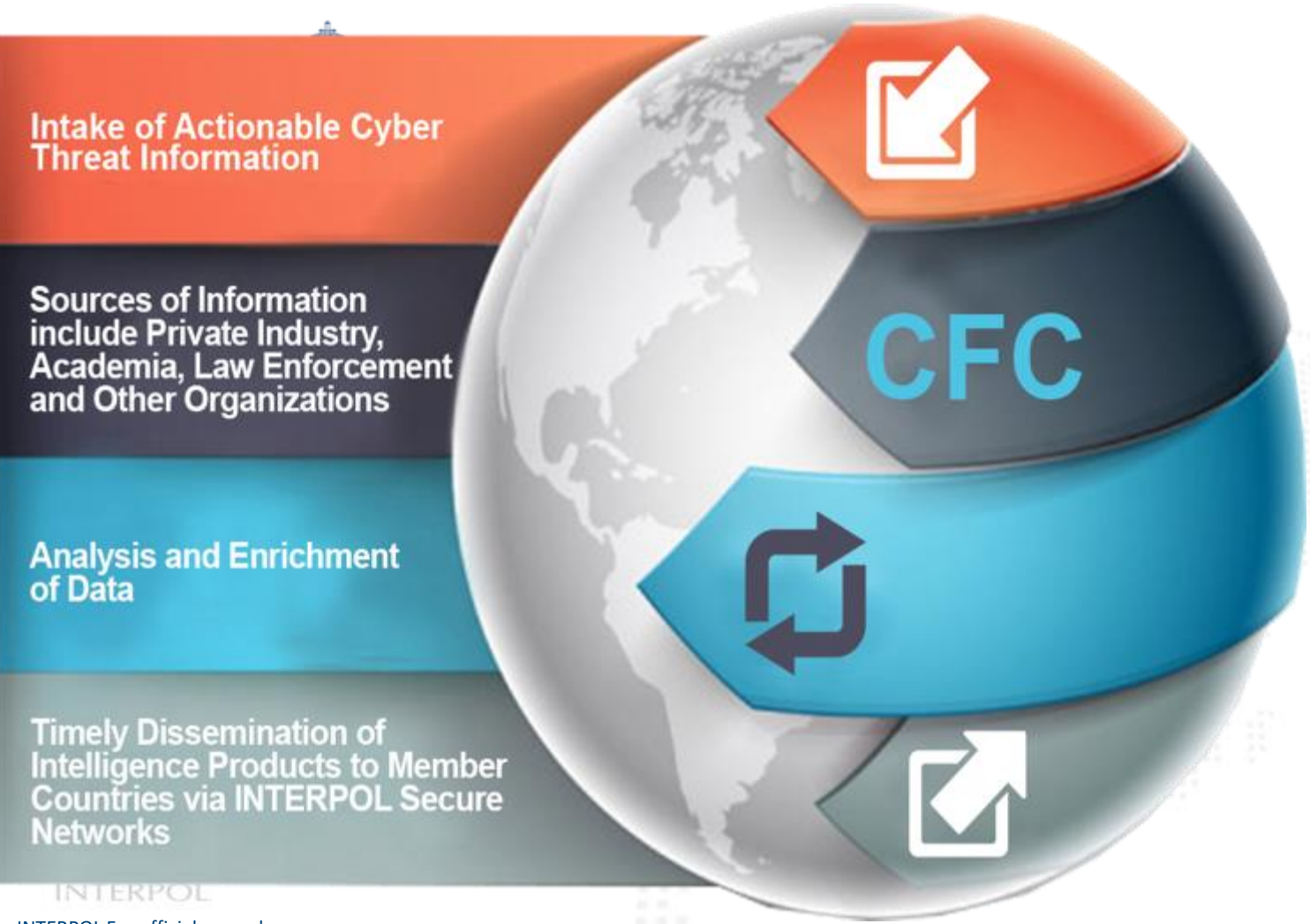
Multiple transfers are made involving foreign banks/ institutions

Intelligence Package Lifecycle

- Multiple partners cooperate to identify threat
  - LE, public, private partnership, INTERPOL as facilitator
- Information produced as Cyber Activity Report (CAR)
  - description of criminal activities in the member countries
  - Information delivered via confidential channel (i24/7)
- Actions vary by recipient authority's legislations and practices
  - Case / evidence to be built by receiving authorities
  - Authenticity of the intelligence should be validated
  - LE capacity matters, INTERPOL may facilitate

Cyber Fusion Centre

Single point of gateway for global cyber related information and intelligence


Intake of Actionable Cyber Threat Information
Sources of Information include Private Industry, Academia, Law Enforcement and Other Organizations
Analysis and Enrichment of Data
Timely Dissemination of Intelligence Products to Member Countries via INTERPOL Secure Networks
CFC

Cyber Surge Operations
Timeline

ASEAN

2016

EURASIAN WG — 15-17 JUN

Planning Meeting — 24 AUG

Gathering Intel

2017

Training — 9-13 Jan

Final Preparatory Meeting — 8 – 10 FEB

Week-Long-Operation — 13-17 FEB

Conclusion — 17 MAR

Americas

2017

Training — 6-31 MAR

Americas WG — 5-7 APR

Planning Meeting — 29 MAY

Gathering Intel

Week-Long-Operation — 30 Aug -1 SEP

Conclusion — 17 NOV

INTERPOL

Cyber Surge Ops

- **Step 1. Planning Meeting**
  - Background and concept shared. Rountable country briefing
  - Presentations on Malicious Website, Malware Tracing etc.
- **Step 2. Investigation Training**
  - IP Address, DNS Abuse, Open Source & SNS Investigation,
  - Preserving Online Materials, Practical Exercises
- **Step 3. Final Prep and Operation**
  - Designate coordinators
  - Distribute intelligence packages (CARs)

- **The CARs are related to:**
  - Website defacements and related activities
  - Malicious domains and Phishing websites
  - Marketplaces/forums and suspected criminal actors
  - C2 infrastructure and related malware families
  - Underground cybercriminal services linked to buying/selling in each country
- **CFC worked with 6 private partners to produce CARs.**
- **More input from police authorities of ASEAN +3 countries**

Surge Operations Result

- Prosecution of cyber criminals
- Quarantine of C2 servers, phishing sites, dark market
- Learning, capacity building, deconfliction
- International cooperation enhanced

Challenges of Police Intelligence

- **Public-Private Partnership is crucial for producing actions**
  - Information at hands of / in better sight of private partners
  - Matching LE's cyber intelligence capability required
- **Intelligence may save time, but can't be used directly**
  - LE need to have capacity to build cases using the provided intel
  - LE need to have capacity to verify – intel maybe incorrect
- **Cooperation between police and prosecution required**
  - Effective SOP to handle police intelligence should be developed
  - Acting on, provision of intelligence should not be discouraged

GLACY+ Project @ INTERPOL

- Country Assessment – initial and final
- Organizational development of cyber & digital forensic units (advise)
- Cybercrime training strategy development (advise)
- Trainings on:
  - Technical course (ECTEG)
  - Instructor Development Course (ToT)
  - Data Protection and Rule of Law
- International Meetings
  - Regional Operational WG
  - Joint MLA training

GLACY+
@INTERPOL

Cyber Fusion Center, Training Team, Regional Bureaus, and other INTERPOL resources

24/7 Point of Contact for Cybercrime, National Central Bureaus (NCBs)

Regional Working Group on Cybercrime for Heads of Units (America, Africa, Eurasian, Middle-East & North Africa)

Largest international police organization

Investigative and Operational Support on Transnational Cybercrime

نشكركم جزيل الشكر على انتباهكم

Thank You-Merci-Gracias

d.kim@interpol.int

INTERPOL