INTERPOL

Impact of COVID-19 on Cybercrime and Digital Evidence

Simon HIRRLE

Specialized Officer Cybercrime

Impact of covid-19 on:

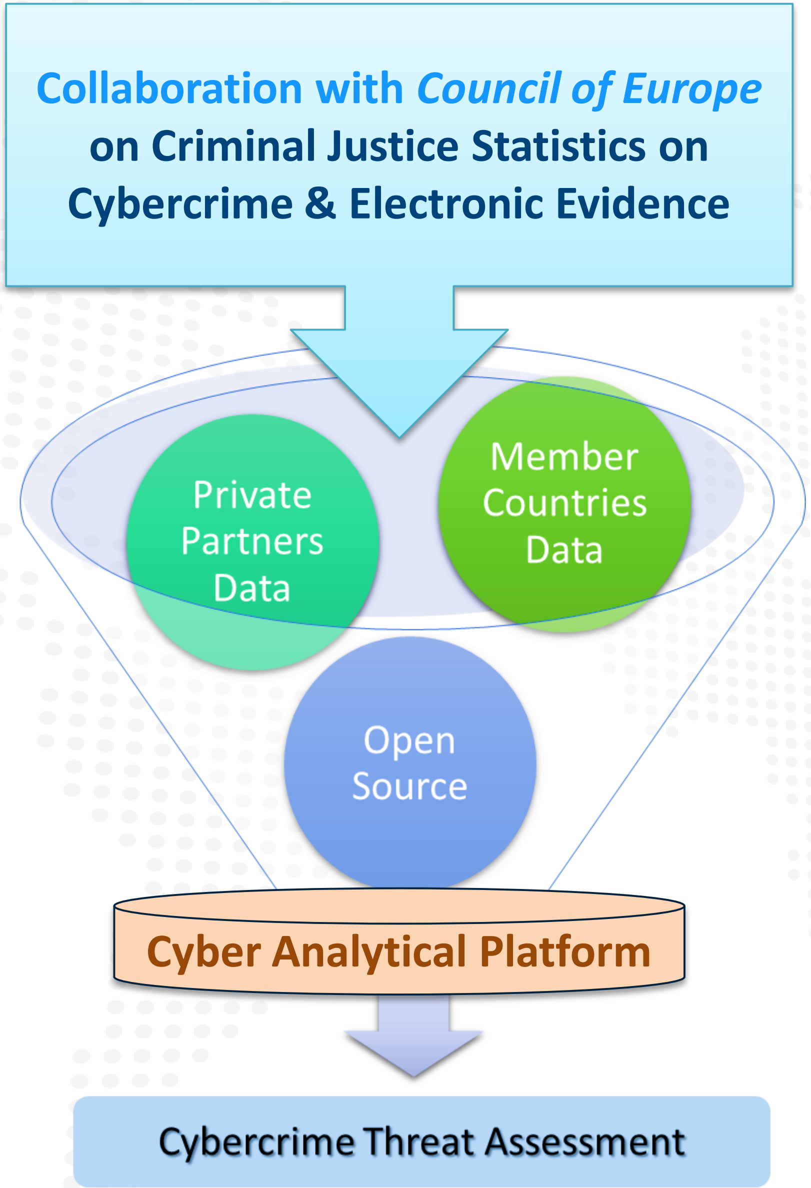
- cyber threats observed
- cybercrime investigations
- cyber capacity building

Cybercrime Threat Assessment

INTERPOL

ASEAN CYBERTHREAT ASSESSMENT 2020

KEY INSIGHTS FROM
THE ASEAN CYBERCRIME OPERATIONS DESK



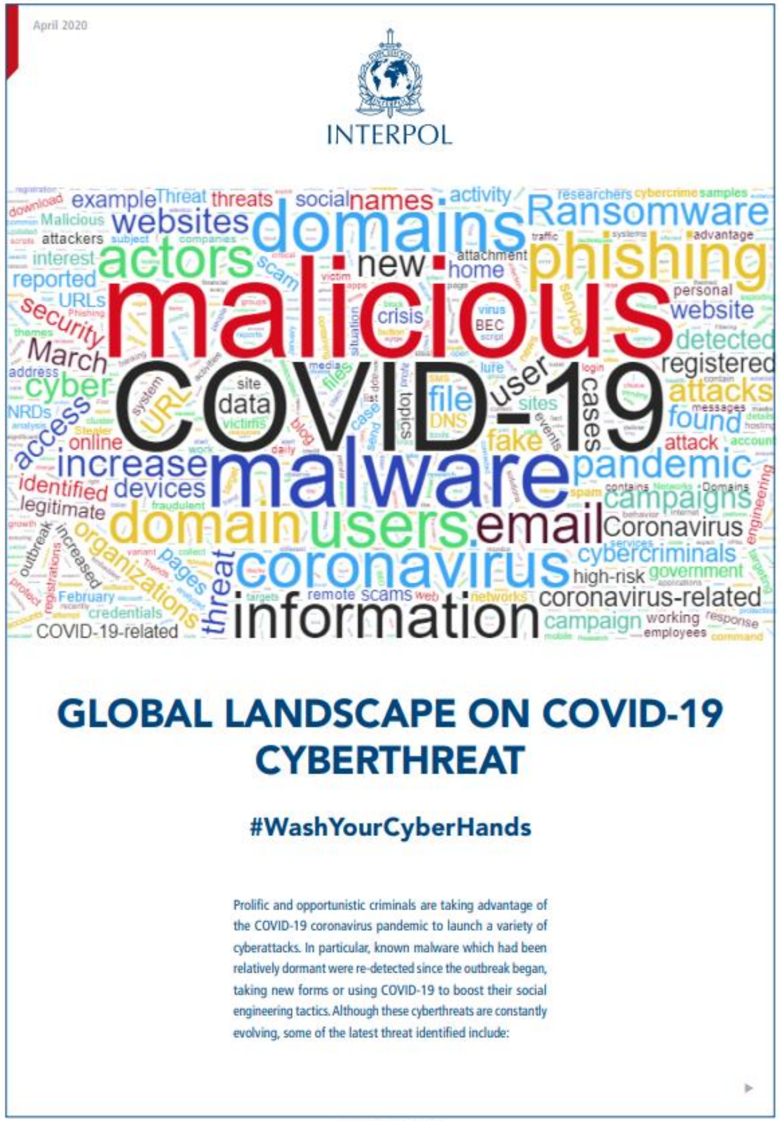
Collaboration with *Council of Europe* on Criminal Justice Statistics on Cybercrime & Electronic Evidence

INTERPOL

CYBERCRIME:
COVID-19 IMPACT

AUGUST 2020

Key COVID-19 Cyberthreats



April 2020

INTERPOL

GLOBAL LANDSCAPE ON COVID-19 CYBERTHREAT

#WashYourCyberHands

Prolific and opportunistic criminals are taking advantage of the COVID-19 coronavirus pandemic to launch a variety of cyberattacks. In particular, known malware which had been relatively dormant were re-detected since the outbreak began, taking new forms or using COVID-19 to boost their social engineering tactics. Although these cyberthreats are constantly evolving, some of the latest threat identified include:

- Malicious Domains
- Disruptive Malware (Ransomware)
- Online Scams and Phishing
- Vulnerability of Remote Workforce
- Misinformation

Related Challenges

‘Cybercrime-as-a-Service’ for easy entry

Targeting healthcare sector & associated supply chains

Online scams & phishing related to vaccine/medication

Remote workforce vulnerabilities

Recommendations

1) Reduce impact of these cyber threats by raising awareness, partnerships and information sharing.

2) Aim for pre-exploit disruption of ransomware and its ecosystem through global law enforcement actions both reactively and proactively.

3) Provide in-event emergency support against cyber attacks with the use of INTERPOL's global network and capabilities.

4) Ensure post-event support following cyber attacks to increase resilience, agility and responsiveness.

Impact of covid-19 on:

- cyber threats observed
- cybercrime investigations
  - – case study Southeast Asia: get creative to further cybercrime investigations that are impeded by COVID-19 related challenges, e.g. travel restrictions
- cyber capacity building
  - – in-person vs. online live vs. online pre-recorded: benefits, limitations, challenges

INTERPOL

International Cooperation on Cybercrime and Digital Evidence

Simon HIRRLE

Specialized Officer Cybercrime

International Cooperation on Cybercrime and Digital Evidence

- INTERPOL
- Challenges
- Avenues

Partnerships and International Cooperation

Project Gateway

CISCO

SHADOWSERVER

FORTINET

BT

GROUP iB

BI.ZONE

TREND MICRO

BANCO DO BRASIL

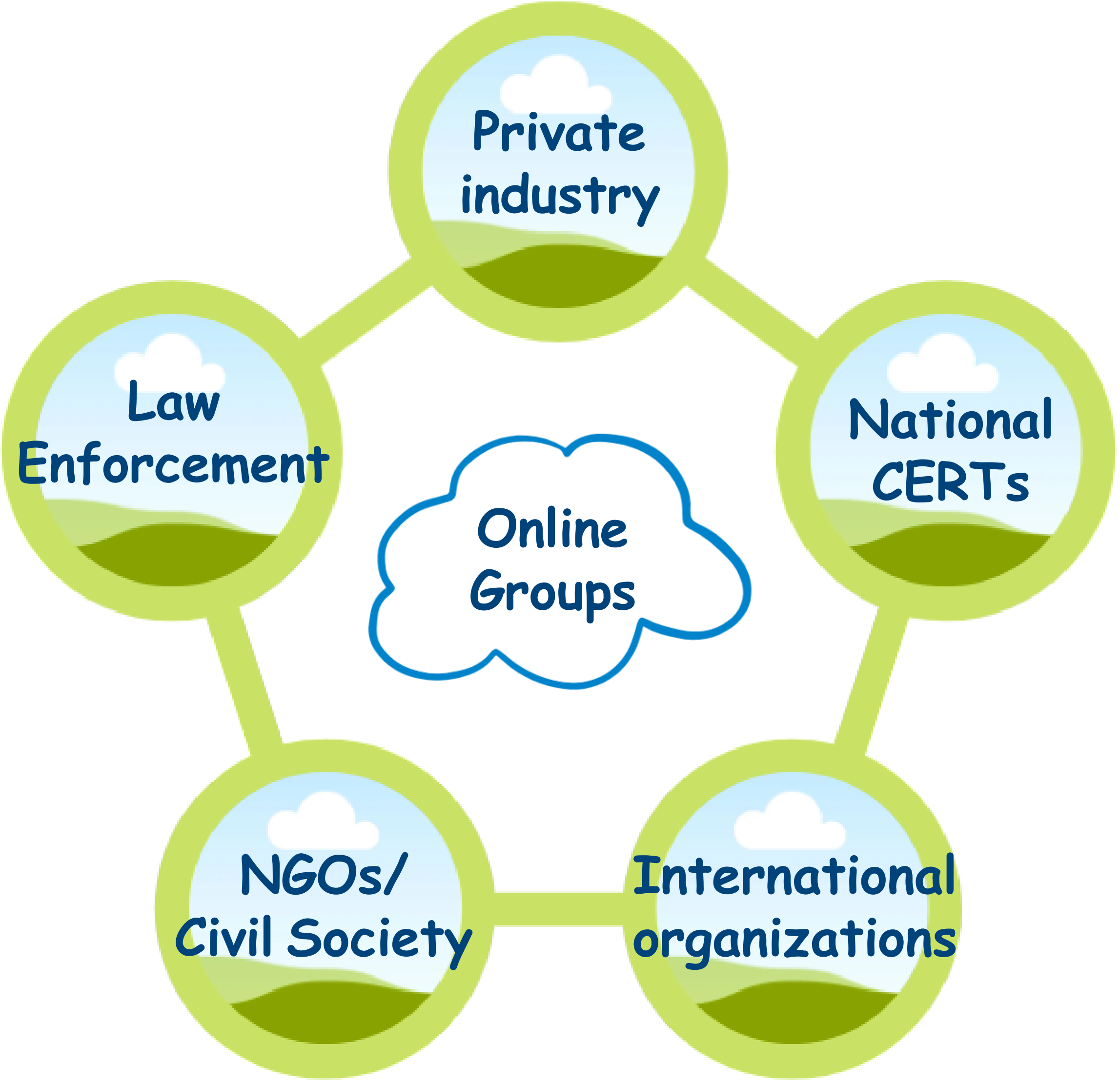
Scitum

paloalto NETWORKS

KASPERSKY lab

LAC

CyberDefense NEC



Private industry

National CERTs

International organizations

NGOs/ Civil Society

Law Enforcement

Online Groups

- **INTERPOL**
- **Challenges**
  - no data available (encryption or no log keeping or no retention)
  - no data obtainable (no cooperation and can’t compel)
  - lack of legal framework (laws, agreements)
  - incorrect data requests, ignorance (LEA portal, LE use unofficial email accounts, unfamiliarity with other channels, e.g. police-to-police)
- **Avenues**

- **INTERPOL**
- **Challenges**
- **Avenues:**
  - + **Intergovernmental Collaboration** (MLA, 24/7 networks, GPEN)
  - + **Public-Private Partnerships** (CyberSec, telco's, fin. services)
  - + **Partnerships with multinational organisations**

    (CoE, INTERPOL, UNODC, ITU, World Bank - ASEAN, ASEANAPOL, African Union, OAS, ECO)

International Cooperation on Cybercrime and Digital Evidence

International cooperation as a puzzle – you are but one piece, i.e. one source of information, most of the information is held by other organizations → put in place the appropriate instruments so you have access to this information.

INTERPOL

Preparing criminal justice authorities to respond to future crises

Simon HIRRLE

Specialized Officer Cybercrime

Preparing criminal justice authorities to respond to future crises

Preparation is key. You may not be able to stop new (cyber)threats from affecting you, BUT in preparing, you

- may be able to **limit damage** and
- increase **cyber resilience** = **recover** from a cyber incident **more quickly**

Preparation needs to cover all relevant stakeholders and angles:

- **Collaboration** > intra- and intergovernmental, PPP, multinational org's (as discussed)
- **Create Awareness**
- **Sharpen Strategies & Processes** > GLACY+ & INTERPOL guides etc.
- **Capacity Building** > GLACY+, INTERPOL, UNODC, CEPOL (and many more)

Preparing criminal justice authorities to respond to future crises

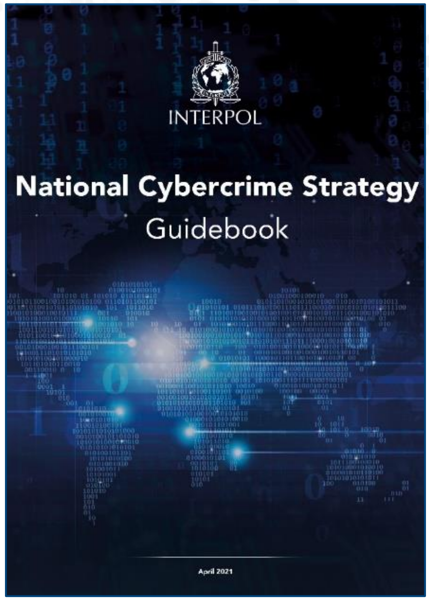
- Create Awareness

https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-launches-awareness-campaign-on-COVID-19-cyberthreats

design awareness campaigns with the cyber **threat** and **target group** in mind

Preparing criminal justice authorities to respond to future crises

- **Sharpen Strategies and Processes**



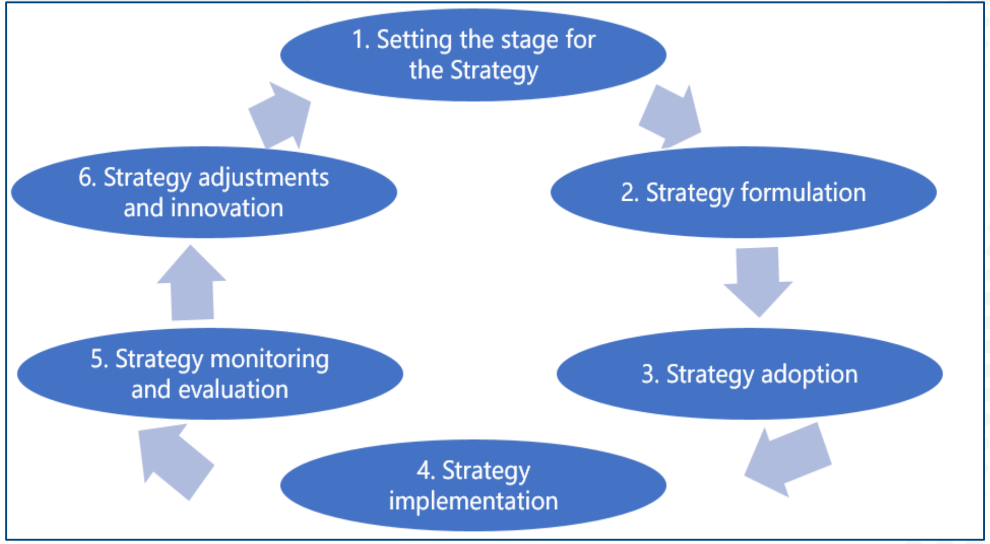
INTERPOL

National Cybercrime Strategy

Guidebook

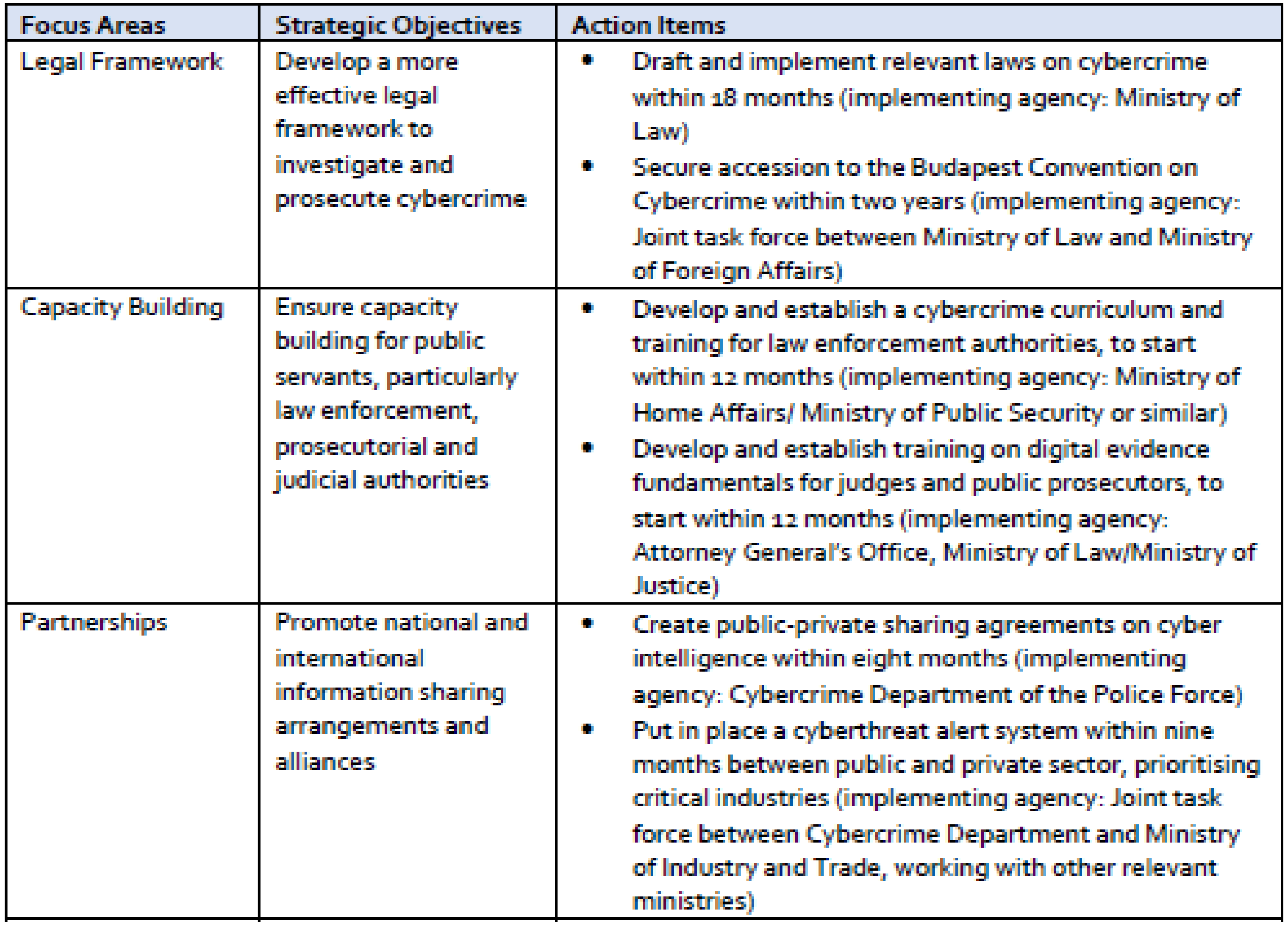
April 2021

Strategy Life Cycle:



1. Setting the stage for the Strategy
2. Strategy formulation
3. Strategy adoption
4. Strategy implementation
5. Strategy monitoring and evaluation
6. Strategy adjustments and innovation

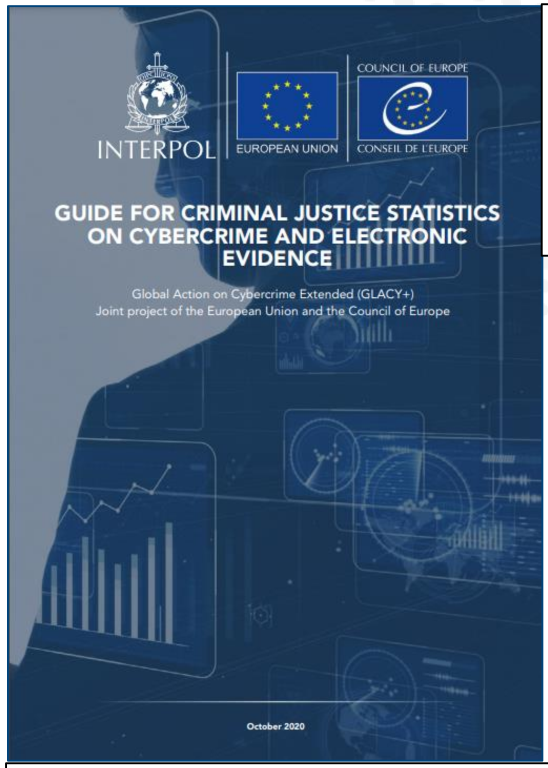
Sample Summary Table:



Focus Areas	Strategic Objectives	Action Items
Legal Framework	Develop a more effective legal framework to investigate and prosecute cybercrime	• Draft and implement relevant laws on cybercrime within 18 months (implementing agency: Ministry of Law) • Secure accession to the Budapest Convention on Cybercrime within two years (implementing agency: Joint task force between Ministry of Law and Ministry of Foreign Affairs)
Capacity Building	Ensure capacity building for public servants, particularly law enforcement, prosecutorial and judicial authorities	• Develop and establish a cybercrime curriculum and training for law enforcement authorities, to start within 12 months (implementing agency: Ministry of Home Affairs/ Ministry of Public Security or similar) • Develop and establish training on digital evidence fundamentals for judges and public prosecutors, to start within 12 months (implementing agency: Attorney General's Office, Ministry of Law/Ministry of Justice)
Partnerships	Promote national and international information sharing arrangements and alliances	• Create public-private sharing agreements on cyber intelligence within eight months (implementing agency: Cybercrime Department of the Police Force) • Put in place a cyberthreat alert system within nine months between public and private sector, prioritising critical industries (implementing agency: Joint task force between Cybercrime Department and Ministry of Industry and Trade, working with other relevant ministries)

Preparing criminal justice authorities to respond to future crises

- **Sharpen Strategies and Processes**



INTERPOL | EUROPEAN UNION | COUNCIL OF EUROPE CONSEIL DE L'EUROPE

GUIDE FOR CRIMINAL JUSTICE STATISTICS ON CYBERCRIME AND ELECTRONIC EVIDENCE

Global Action on Cybercrime Extended (GLACY+)
Joint project of the European Union and the Council of Europe

October 2020

https://www.**interpol**.int/en/Crimes/Cybercrime/Cyber-capabilities-development/**Glacy**

GLACY+ Project

- Guide for criminal justice statistics on cybercrime and electronic evidence
- Law enforcement training strategy

INTERPOL Digital Forensics Laboratory (DFL)

- Global guidelines for Digital Forensics First Responders by INTERPOL Innovation Centre – Digital Forensics Laboratory (IC-DFL)
- Global guidelines for Digital Forensics Laboratories (IC-DFL)
- Framework for responding to a Drone Incident (IC-DFL)
- ....

INTERPOL

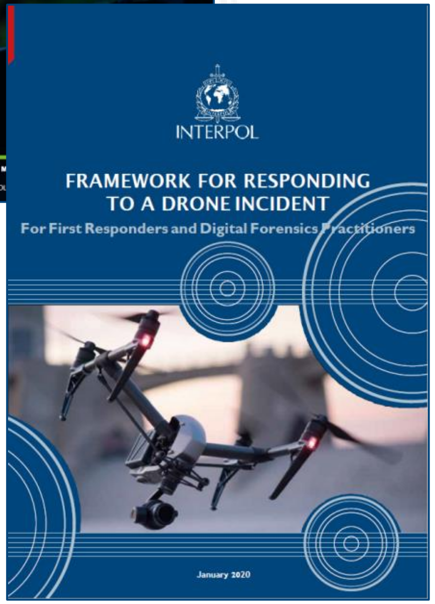
GLOBAL GUIDELINES FOR DIGITAL FORENSICS LABORATORIES

May 2019

INTERPOL

GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS

Best practices for search and seizure of electronic and digital evidence



INTERPOL

FRAMEWORK FOR RESPONDING TO A DRONE INCIDENT

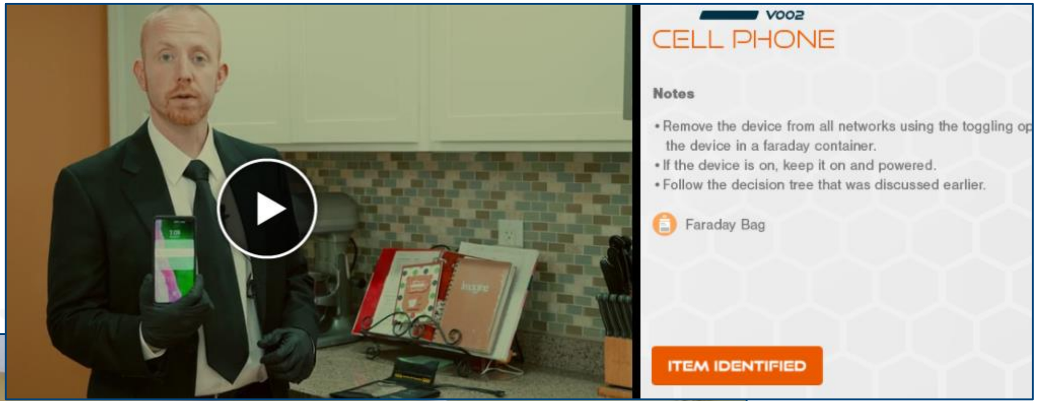
For First Responders and Digital Forensics Practitioners

January 2020

Preparing criminal justice authorities to respond to future crises

- **Capacity Building**

KICKOFF AND DRAFTING WORKSHOP ON STRATEGY DEVELOPMENT GUIDEBOOK
ASEAN CYBER CAPACITY DEVELOPMENT PROJECT PHASE 2
Cybercrime or C



V002

CELL PHONE

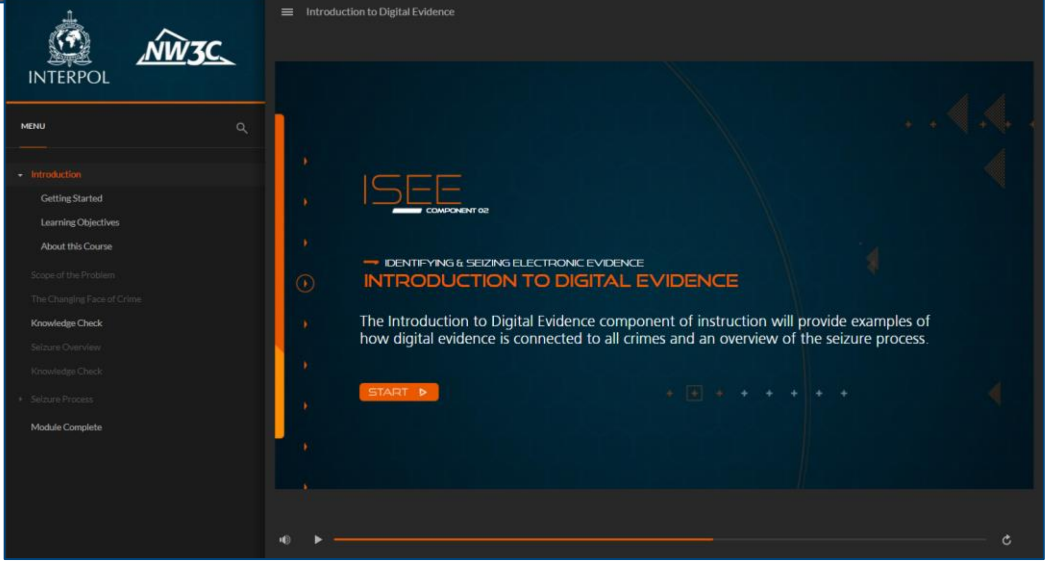
Notes

- Remove the device from all networks using the toggling op
  the device in a faraday container.
- If the device is on, keep it on and powered.
- Follow the decision tree that was discussed earlier.

Faraday Bag

ITEM IDENTIFIED

21 ITEMS FOUND



INTERPOL NW3C

Introduction to Digital Evidence

MENU

- Introduction
  - Getting Started
  - Learning Objectives
  - About this Course
- Scope of the Problem
- The Changing Face of Crime
- Knowledge Check
- Seizure Overview
- Knowledge Check
- Seizure Process
- Module Complete

ISEE COMPONENT 02

IDENTIFYING & SEIZING ELECTRONIC EVIDENCE

INTRODUCTION TO DIGITAL EVIDENCE

The Introduction to Digital Evidence component of instruction will provide examples of how digital evidence is connected to all crimes and an overview of the seizure process.

START ▶

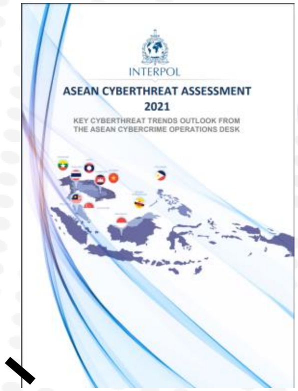
INTERPOL

Proposals for further action and capacity building

Simon HIRRLE

Specialized Officer Cybercrime

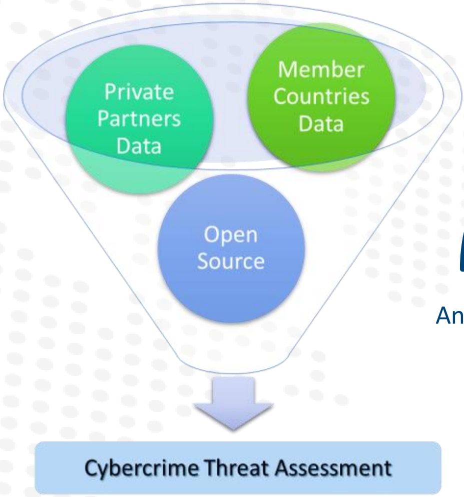
Proposals for further action and capacity building

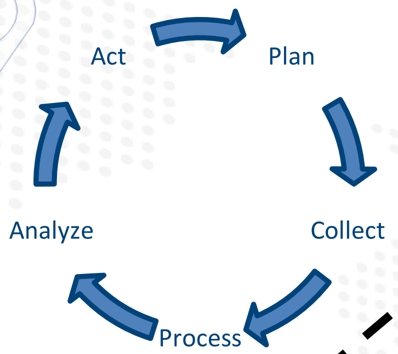


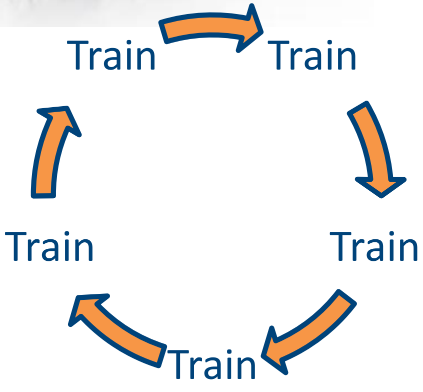
INTERPOL

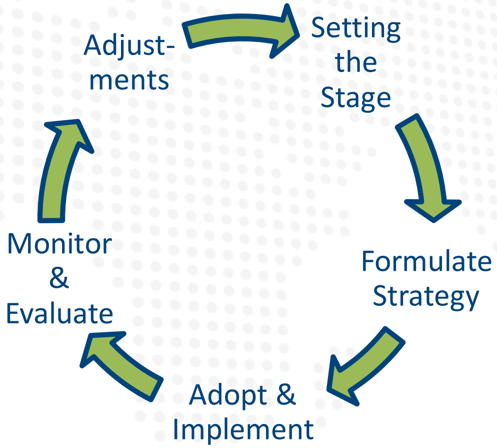
ASEAN CYBERTHREAT ASSESSMENT 2021

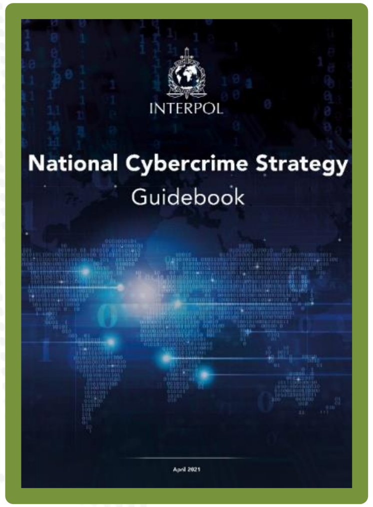
KEY CYBERTHREAT TRENDS OUTLOOK FROM THE ASEAN CYBERCRIME OPERATIONS DESK











INTERPOL

National Cybercrime Strategy Guidebook

April 2021

> Continuous Action <

SUMMARY

Impact of COVID-19 on Cybercrime and Digital Evidence

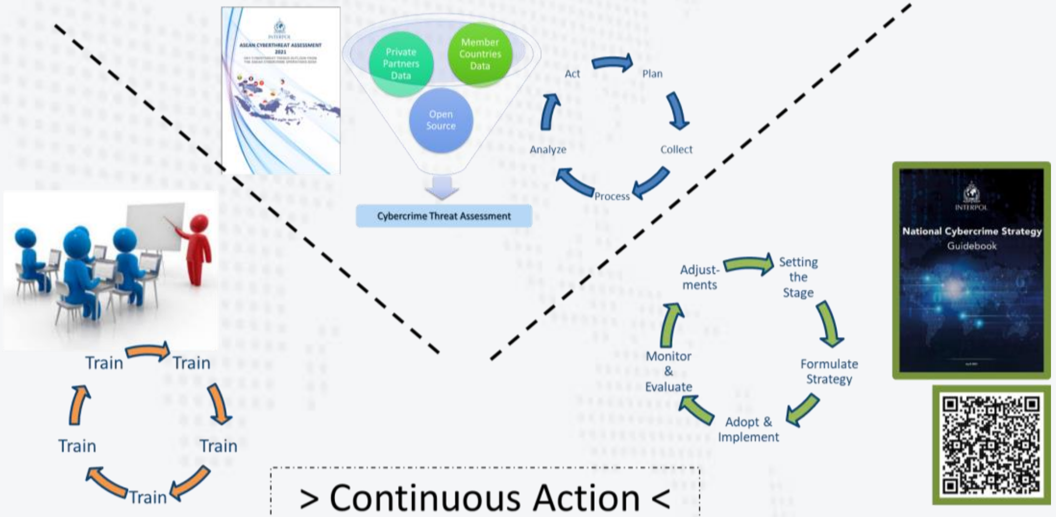
- Malicious Domains
- Disruptive Malware (Ransomware)
- Online Scams and Phishing
- Vulnerability of Remote Workforce
- Misinformation

International Cooperation on Cybercrime and Digital Evidence

Preparing criminal justice authorities to respond to future crises

- **Collaboration** > intragovernmental, intergovernmental, PPP, multinational org's
- **Create Awareness**
- **Sharpen Strategies & Processes** > GLACY+ & INTERPOL guides
- **Capacity Building** > GLACY+, INTERPOL, UNODC, CEPOL (and many more)

Proposals for further action and capacity building



> Continuous Action <

SUMMARY

نشكركم جزيل الشكر على انتباهكم

Thank You-Merci-Gracias

s.hirrle@interpol.int