

CLICK. CONNECT. COMBAT.



Presented by Paolo PELLEGRINO,
CYBERCRIME OFFICER

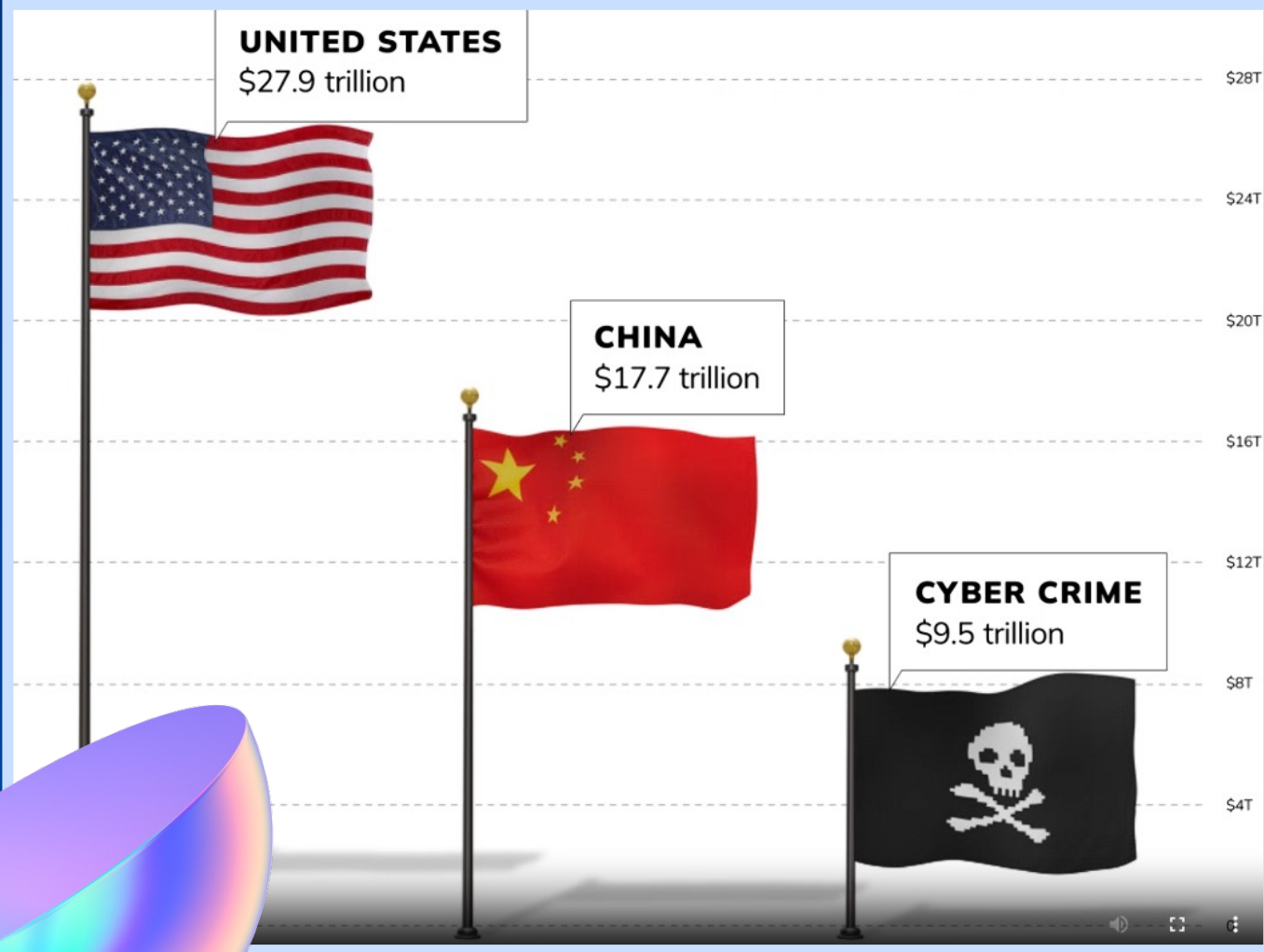


An INTERPOL
Perspective

November 2025

www.interpol.int

THE SCALE OF CYBERCRIME



≥USD 10.5T

GLOBAL CYBERCRIME
ECONOMY (2025)

≥USD 20M

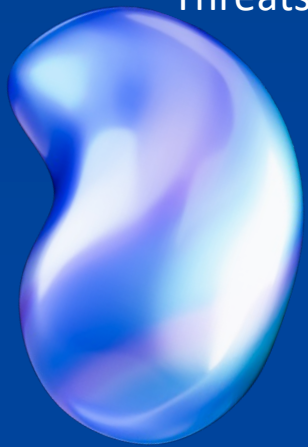
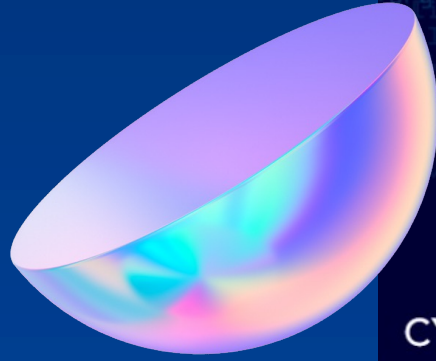
LOSS RATE PER MINUTE (2025)

≥USD 23T

PROJECTED BY 2027
(+142%)

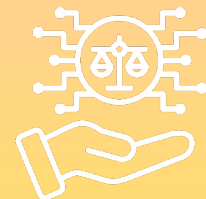
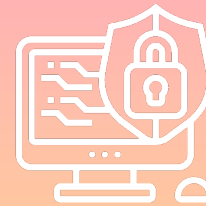
INTRODUCTION TO INTERPOL CYBER THREAT ASSESSMENTS

- Crime Statistics and Trends
- Insights on Asia and Pacific Cyberthreat Trends
- Proactive Actions against Evolving Cyber Threats



KEY CYBERTHREATS & TRENDS

Online scams continue to be the most prolific threat across the region.



- Access to online scam tools is being democratized, as the number of 'Scams-as-a-Service' (SaaS) continue to rise.
- Phishing is the main technique used for initial access in these scams.
- Phishing emails targeting APC are likely to rise in 2024 and 2025 as generative Artificial Intelligence (AI) is integrated into the SaaS platforms.

ONLINE SCAMS

Three major categories.



1. Investment scams

- Impersonation scams
- BEC
- Romance scams
- Job scams
- E-commerce scams,
- Cryptocurrency scams
- Malware-enabled scams



2. Social Media

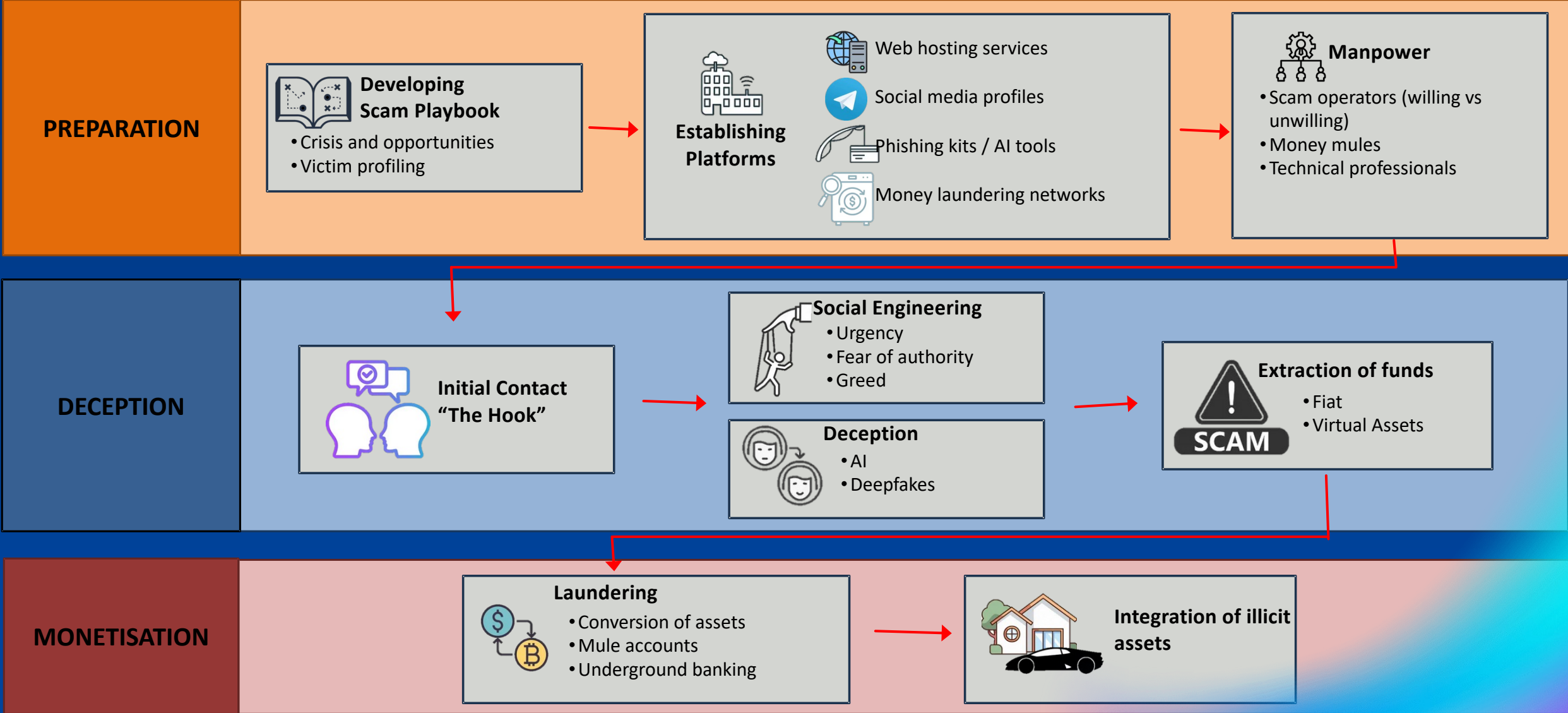
- Messaging Platforms
- Phone calls
- Online Shopping Platforms
- Online Advertisements



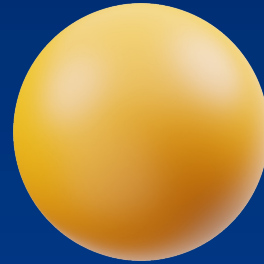
3. Scam-as-a-Service

- Artificial Intelligence in online scams

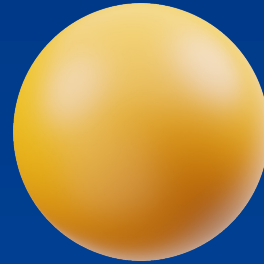
LIFECYCLE OF SCAMS



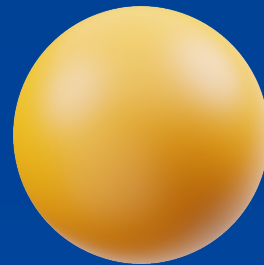
INTERPOL CYBERCRIME DIRECTORATE



**CYBERCRIME STRATEGY
& CAPACITY BUILDING**

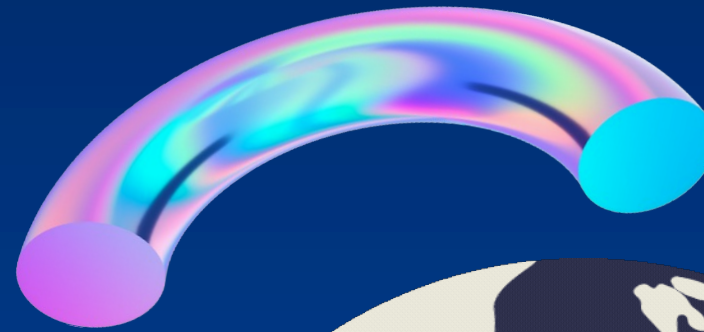


**CYBERCRIME
INTELLIGENCE**



**CYBERCRIME
OPERATIONS**

GLOBAL PRESENCE. REGIONAL ACTION.



ASPJOC aims to strengthen the capability of Asian and South Pacific (ASP) national law enforcement agencies to prevent, detect, investigate, and disrupt cybercrime by:

- Gathering and analyzing information on cybercriminal activity;
- Promoting cooperation and good practices amongst Asia and South Pacific member countries;
- Facilitating and carrying out intelligence-led, coordinated action against cybercrime.



Foreign, Commonwealth
& Development Office



OPERATIONAL CYCLE



INTELLIGENCE

Enhancing cybercrime intelligence for effective responses

1



AWARENESS

Promoting good cyber hygiene for a safer cyberspace

4

OPERATIONS

Strengthening cooperation for joint operations against cybercrime

2

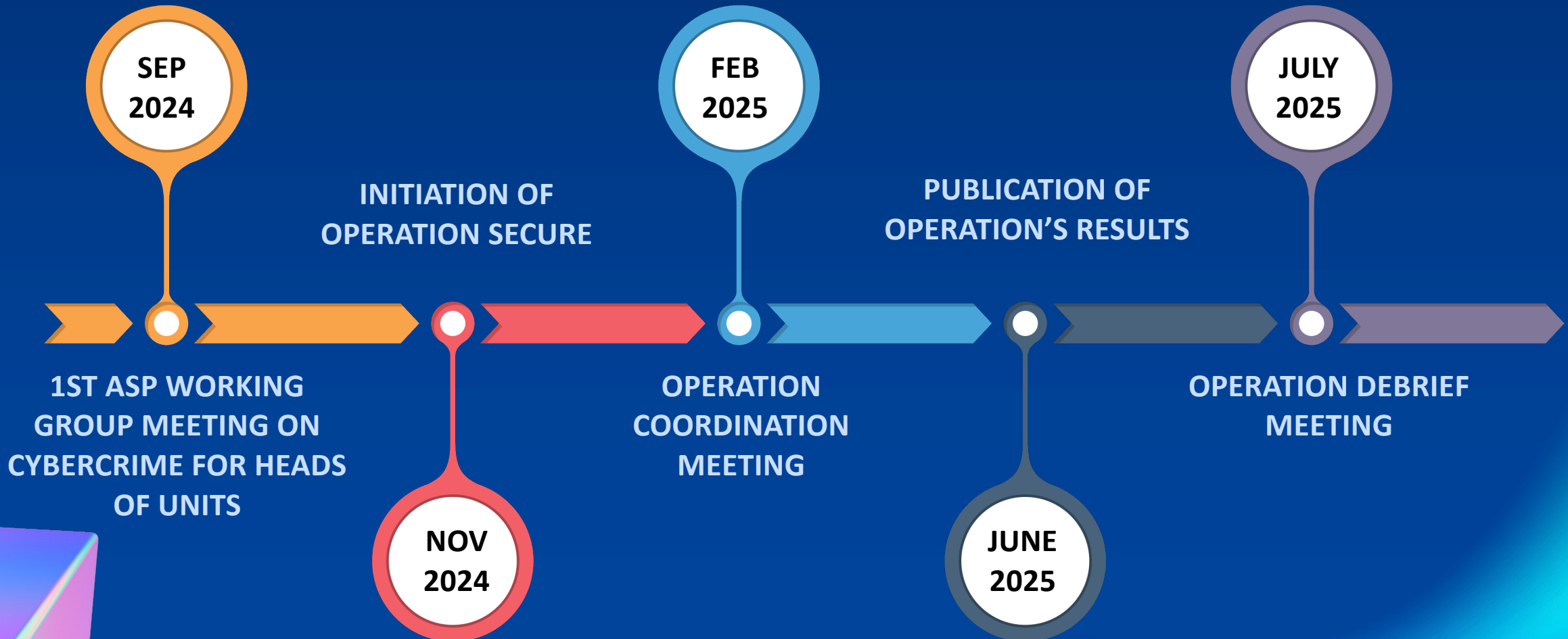


CAPABILITIES

Developing regional capacities and capabilities to combat cybercrime

3

OPERATION SECURE: CASE STUDY



WHAT'S AN INFOSTEALER

MALICIOUS SOFTWARE DESIGNED TO SILENTLY STEAL SENSITIVE INFORMATION FROM INFECTED DEVICES



Credential Theft
→ Scams & Phishing
Data Sale on Dark Web
→ Widespread Abuse

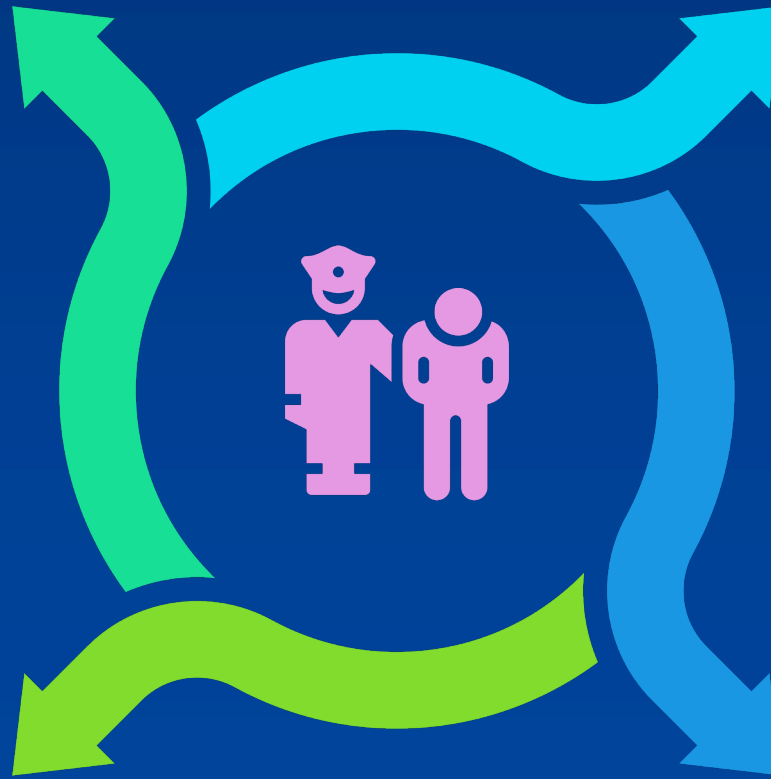


Business Account Access
→ Ransomware Attacks
File Theft
→ Cyber Extortion

OPERATION SECURE: THE CHALLENGES

LIMITED ACCESS
TO INVESTIGATIVE
TOOLS

DELAYS IN CROSS
JURISDICTIONAL
COORDINATION AND
INFORMATION
EXCHANGE



DISPARITIES IN
INVESTIGATIVE
CAPABILITIES

DIFFERING
LEGAL FRAMEWORK

OPERATION SECURE: THE RESULTS



25,917

IPs/domains investigated



20,642

IPs/domains taken down



>100GB

Data seized



31

Cyber Activity Reports produced



41

Servers seized



26

Participating countries



69

Infostealer variants investigated



216,058

Victim notifications



32

Individuals arrested



GATEWAY FRAMEWORK

The Gateway Framework is INTERPOL's flagship initiative to connect law enforcement and the private sector in the fight against cybercrime. Adopted by the INTERPOL General Assembly in 2019, it provides a secure, renewable 5-year framework for the exchange of cyber threat intelligence between INTERPOL and trusted partners. The aim is to close the gap between law enforcement and industry so that cyber threats can be identified and disrupted more effectively.

PUBLIC - PRIVATE COOPERATION



**SECURE INTELLIGENCE
EXCHANGE**



**INTEGRATED ANALYSIS
AND DISSEMINATION**



**OPERATIONAL
COLLABORATION**



**FORMAL 5-YEAR DATA
SHARING AGREEMENT**

WHAT IS CYBEREX?



**+180 specialized law enforcement officers
from around the world**



**Experts from academia, industry and the
wider cyber ecosystem**



**Promotes the exchange of cyber expertise
& innovative solutions**



**Established 2014
Re-launched March 2025**

HOW WE WORK: CYBEREX'S STRUCTURE

FOUR THEMATIC PILLARS



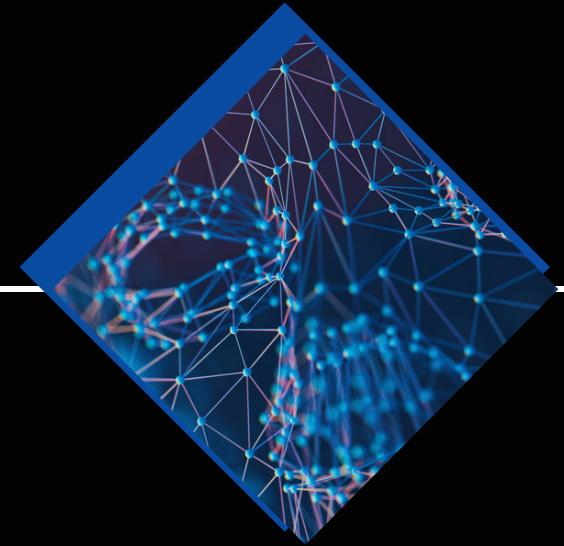
STRATEGY



INVESTIGATIONS



PREVENTION



EMPOWERMENT

GET INVOLVED!

We are looking for:

- 1 Speakers & presenters
- 2 Investigative case studies
- 3 Research & tools

... and more!



If interested, please reach out to: cyberex@interpol.int



نشكركم جزيل الشكر
على انتباهكم

THANK YOU

MERCI

GRACIAS



Presented by Paolo PELLEGRINO,
CYBERCRIME OFFICER
p.pellegrino@interpol.int