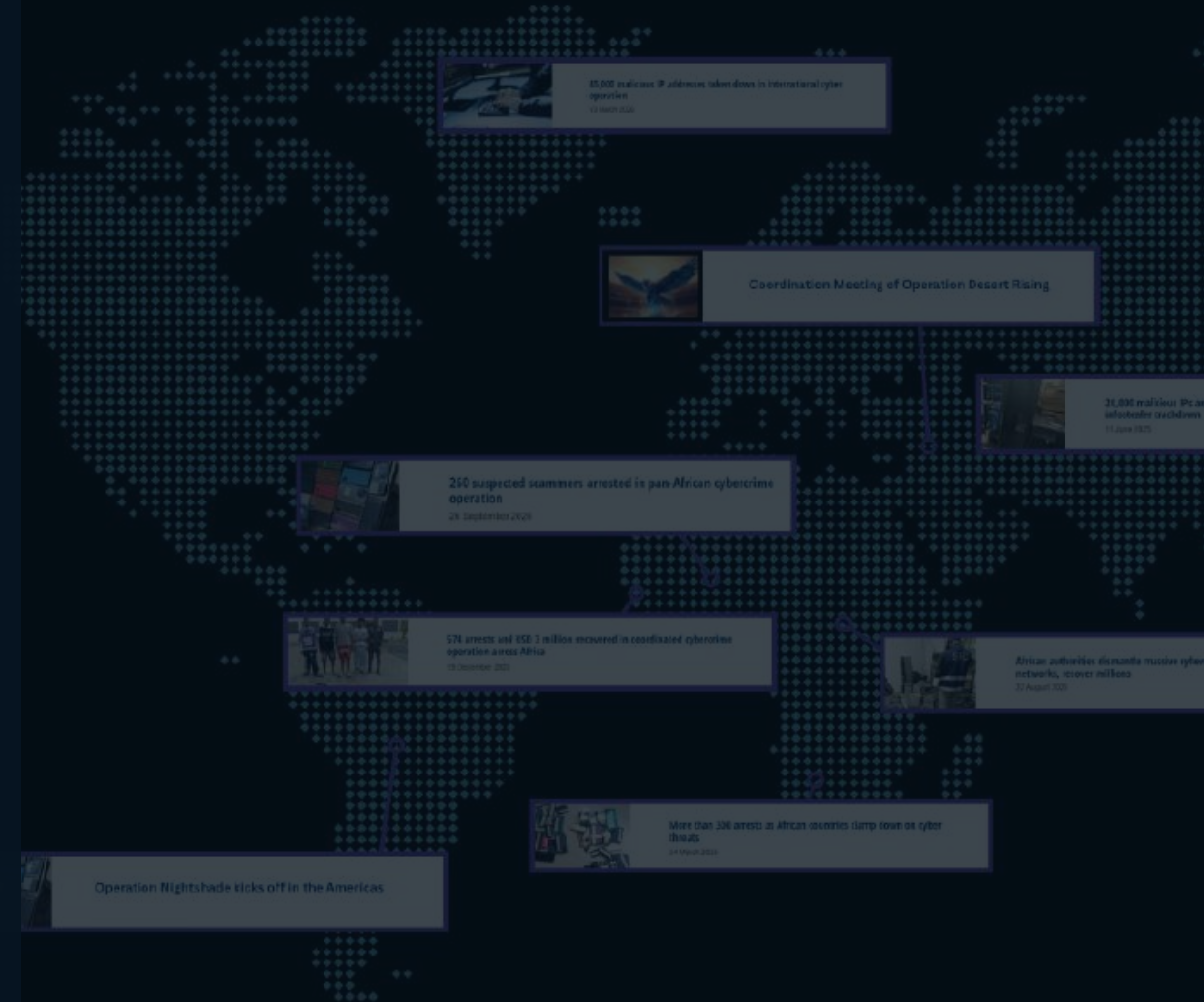


COMBATTING CYBERCRIME TOGETHER: INTERPOL CAPACITIES AND CAPABILITIES

27th AIRLINE INDUSTRY DRUAD SUMMIT
MADRID | 28-30 APRIL 2026

ENRIQUE HERNANDEZ GONZALEZ
Assistant Director Cybercrime Operations,
INTERPOL Cybercrime Directorate

Cyber resilience now depends on connected
enforcement, shared intelligence, and cross-border
action.



A GLOBAL STRUCTURE



196 MEMBER COUNTRIES CONNECTED THROUGH A SECURE NETWORK



INTERPOL

FOUR GLOBAL PROGRAMMES



**COUNTER-
TERRORISM**



CYBERCRIME



**ORGANIZED
AND EMERGING
CRIME**



**FINANCIAL
CRIME AND ANTI-
CORRUPTION**



INTERPOL

THE DIGITAL ENVIRONMENT WE POLICE TODAY (CYBERSPACE)

What is the “cyberspace” ?

Cyberspace = all the networks, systems, devices, data and services connected by the Internet

- It is built on real infrastructure: servers, routers, cables, data centres, satellites, phones and IoT devices

Digital activity ignores borders:

- Criminals can act across countries in seconds
- **Most public services depend on digital systems:**
Banking, government, health, transport and communication



Cybercrime is not a parallel universe. It is simply a **crime in a digitally extended society**. The “**cyber layer**” amplifies reach, anonymity, speed, and scale, but the harm remains real.

THE GLOBAL CYBERCRIME PICTURE IN 2025

International Keynote



Global cybercrime risks in 2025

Ransomware remains the top global cyber threat

- 45% of organisations identify ransomware as their highest cyber risk

Cyber-enabled fraud is the second major threat

- Includes phishing, BEC, vishing and online payment fraud
- 20% of organizations report it as their top concern

Identity theft is now the leading personal cyber risk

- Sharp increase from 2024 to 2025, affecting individuals, families and national ID systems

Overall rise in exposure

- 72% of organisations report increased cyber risks in the past year



(Sources: WEF Global Cybersecurity Outlook 2025,)

THE CHALLENGE

Cybercrime has industrialised.

It now operates as a scalable global criminal economy.

Service-based

Structured criminal services lower the barrier to entry.

Adaptive

Attacks are tailored to sectors, communities and behaviours.

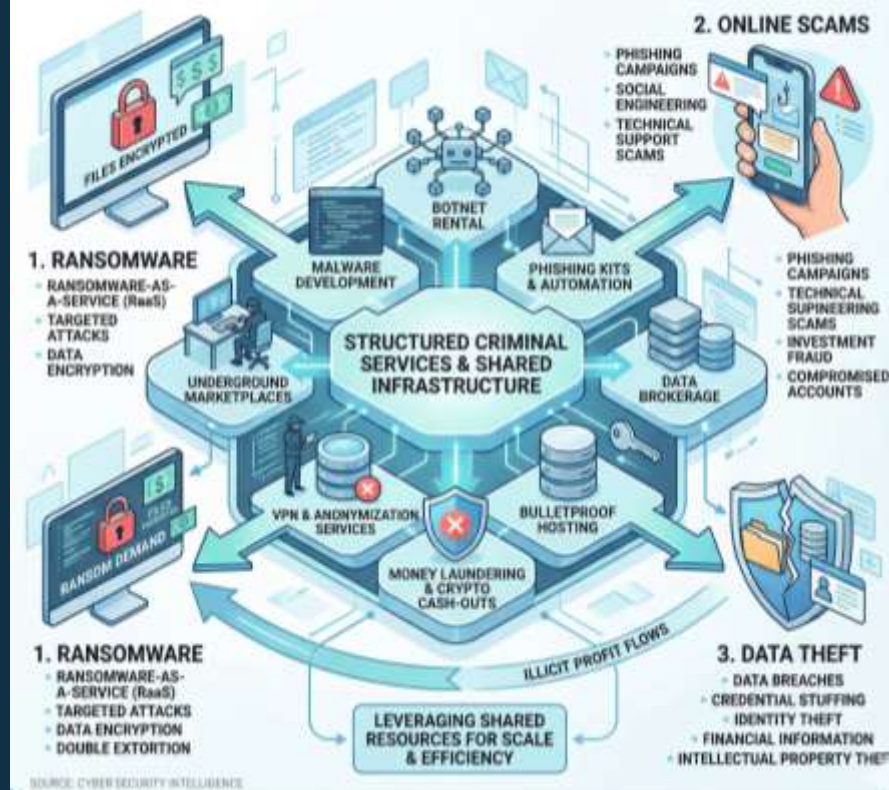
Transnational

Infrastructure and actors operate across borders.

Ransomware, online scams and data theft increasingly share infrastructure, tooling and distribution channels—allowing attacks to scale rapidly.

Reality: cybercrime is an ecosystem, not a loose collection of incidents.

THE CYBERCRIME-AS-A-SERVICE (CaaS) ECOSYSTEM



ACCELERATION

AI is amplifying cybercrime.

It increases speed, lowers cost, and improves deception.

01

Accelerated threats

New cyber-enabled crime models and a lower barrier to entry for malicious actors.

02

Enhanced deception

More convincing phishing, real-time impersonation, deepfakes and voice cloning.

03

System strengthening

Criminal systems become faster, more flexible and harder to detect.

AI misuse is rapidly emerging as a primary challenge for the wider cybersecurity community.

THE TRANSNATIONAL THREAT OF CYBERCRIME



Global Financial Comparison (Trillions USD)

UNITED STATES

\$27.9 trillion

CHINA

\$17.7 trillion

CYBERCRIME

\$10.5 trillion

Global cybercrime economy in 2025:

≥USD 10.5T

Loss rate per minute (2025):

≥USD 20M

... and projected growth by 2027:

≥USD 23T (+142%)

A three-part operating model.

Intelligence, capability building, and coordinated operations reinforce each other.

01

Actionable intelligence

02

Capability building and strategy development

03

Coordinated operations



Cybercrime requires a multi-faceted approach.

GLOBAL SUPPORT MODEL

Global Reach, Regional Approach

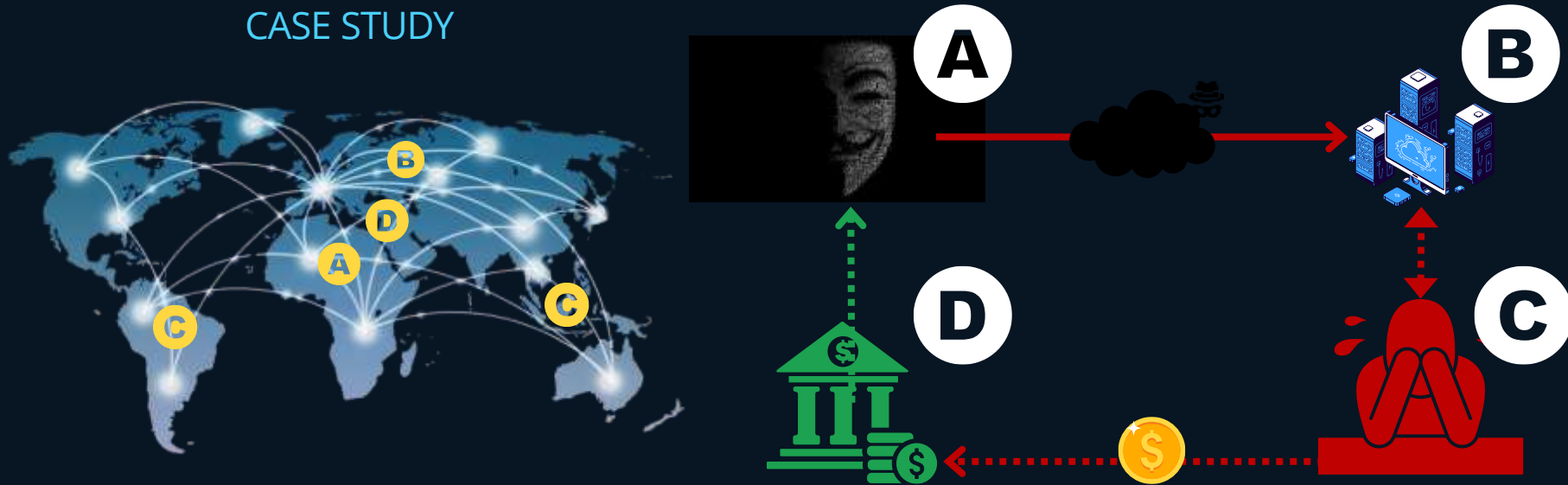


Regional Operations Desks

-  Africa
-  Asia & South Pacific
-  Americas
-  Middle East
-  Europe

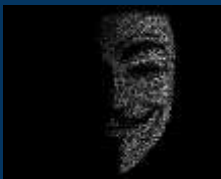
THE COMPLEXITY OF CYBERCRIME

CASE STUDY



A

Threat Actors



B

Attack Infrastructure



C

Victims



D

Financial Network



Operational Capabilities

Supporting ongoing operations

- Identifying trends
- Facilitating communication
- Providing support

Leading Global Operations

- Facilitating information and intelligence sharing
- Facilitating operational action



Raising Awareness

- Running global awareness campaigns
- Campaigning across social media

Capacity Building

- Sharing tools and best practices
- Running global exercises

OPERATIONAL IMPACT

Cross-border operations produce measurable outcomes.

Operation Synergia III shows the scale and coordination required.

18 Jul 2025 – 31 Jan 2026

72

countries & territories

- 94 arrests
- 110 suspects under investigation
- 45,000+ malicious IPs and servers disrupted
- 212 electronic devices seized

Success comes from shared visibility, joint targeting and synchronized action.



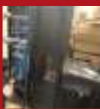
CHECK OUR PRESS RELEASE!



INTERPOL cyber operation takes down 22,000 malicious IP addresses
19 November 2024



Coordination Meeting of Operation Desert Rising



29,000 malicious IPs and domains taken down in INTERPOL infostealer crackdown
11 June 2025



260 suspected scammers arrested in pan-African cybercrime operation
20 September 2025



INTERPOL event shares tips for staying safe online
12 August 2025



African authorities dismantle massive cybercrime and fraud networks, recover millions
22 August 2025



More than 300 arrests as African countries clamp down on cyber threats
24 March 2025



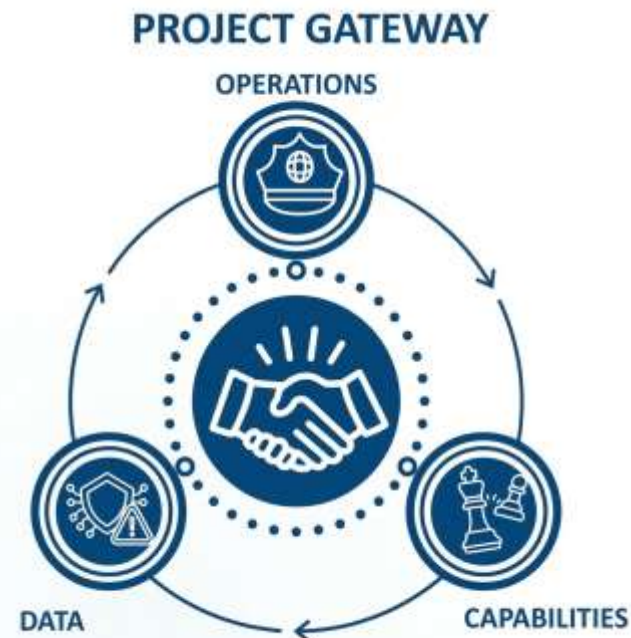
Operation Nightshade kicks off in the Americas

PUBLIC-PRIVATE PARTNERSHIP

Operational speed improves when intelligence flows both ways.

Project Gateway bridges visibility and enforcement.

- Connects cybersecurity firms, financial institutions and tech partners.
- Transforms private-sector insight into swift operational action.
- Analyses infrastructure intelligence to produce actionable leads.
- Coordinates a faster, more targeted international response.



We do not compete against each other. We compete against cybercrime.



CYBERCRIME THREAT INTELLIGENCE



OPERATING MODEL



**AGGREGATED
DATA SETS**



**DATA
TRANSFORMATION**



DATA ANALYSIS



**GLOBAL ACTIONABLE
INTELLIGENCE**



INTERNAL TOOLS AND PLATFORMS



MEMBER COUNTRY DATA



PRIVATE PARTNER DATA

KEY PRODUCTS



Cyber Activity Report



Threat Assessment Report



Cyber Threat Alert



**Prevention and Disruption
Strategies**



**Intelligence Opportunities for
Operations**

The email address for the Cyber Fusion Centre (CFC) is: cfc@interpol.int

Key products - CARs

INTERPOL FOR OFFICIAL USE ONLY



INTERPOL

CYBER ACTIVITY REPORT

CYBER FUSION CENTRE

+

<Date>

<Identifier number>

HANDLING CONDITIONS: TO NCB <OFFICE> AND APPROPRIATE LAW ENFORCEMENT AGENCIES IN <COUNTRY>.

This information may be used by domestic law enforcement agencies for further investigation and/or for international police cooperation purposes. It may only be used for intelligence and lead purposes and should not be construed as being a document of evidential value or for use in judicial proceedings. Any decision on action to be taken based on this information is within the discretion and responsibility of the appropriate law enforcement authorities and should be done in accordance with the applicable national law and international obligations of the country concerned.

REPORT TITLE

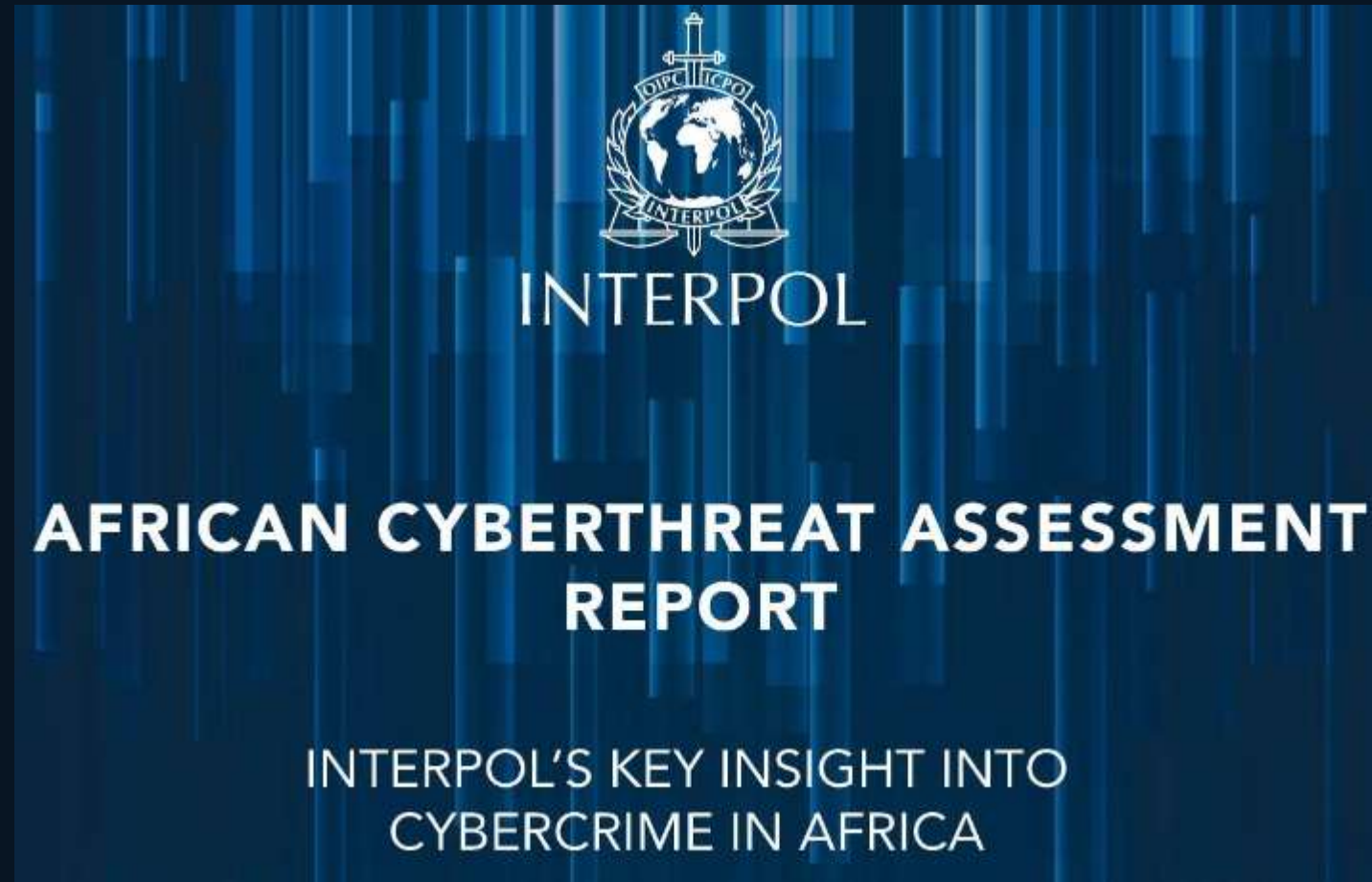
EXECUTIVE SUMMARY

ANALYSIS AND FINDINGS

RECOMMENDATIONS

Key products – Threat Assessments

International Keynote



Key products – Purple Notices

International Keynote

REQUEST FOR PUBLICATION OF A PURPLE NOTICE

Control No.: For General Secretariat use

Requested by: Name of the requesting member country (or General Secretariat unit) and other member countries

File No.: For General Secretariat use

Date of publication: Click here to enter a date

Last update on: Click here to enter a date



MODUS OPERANDI

Type(s) of offence: Conti Ransomware deployment against critical infrastructure and organisations globally.

Date of offence: Ongoing

Place of offence: Global

Country of offence: Global

Data source(s): Data Supplied by INTERPOL's Cybercrime Directorate private partners, internal threat analysis generated by INTERPOL's Cyber Threat response Team, threat alerts put out by Member Countries¹ and Open Source reports of attacks globally.

BEYOND OPERATIONS

Sustained resilience requires networks, expertise and new initiatives.

INTERPOL is expanding both community and capability.



History

Established in 2014; re-launched in March 2025; last in-person event: February 2026 in Hong Kong.



Numbers

182 specialized law enforcement officers from 82 countries.



Sectors

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



Fighting cybercrime means exchanging cyber expertise and innovation solutions.

BEYOND OPERATIONS

Sustained resilience requires investments.

INTERPOL is expanding both community and capability.



PROJECT STARDUST

Today, many cybercriminals exploit specialized services to conduct criminal activity on a global scale. This requires utilizing infrastructure rental services, data marketplaces selling personally identifiable information, and phishing operations and selling cybercrime-as-a-service. These services allow criminals to amplify the scope and impact of their operations. INTERPOL's Project Stardust equips law enforcement to fight against the industrialization of cybercrime.

What is the Industrialization of Cybercrime?	Examples of Exploited Key Services
In many countries today, INTERPOL's data shows that a cybercrime law represents a substantial proportion of all reported offenses – often exceeding 50%.	Service-based providers' architecture across different parts of the globe allows crime actors to have a global reach. Key services include: - Infrastructure Providers and Cloud-based Data-Flow Networks - Subdomain Hosting services Infrastructure - Phishing as a Service (PhaaS) and Phishing Kits - Crashers, Botnets and Malware-as-a-Service - Malware-as-a-Service (MaaS) - Cloud-based and Remote Access and Control Services - Malware-as-a-Service (MaaS) and Malware-as-a-Service (MaaS) - Malware-as-a-Service (MaaS) and Malware-as-a-Service (MaaS)
A key driver of this growth is the industrialization of cybercrime . This involves the commodification and subsequent sale of services, resulting in a growing underground economy of specialized services.	Exploiting the impact of such services, in the U.S. the FBI has reported that the average cost of a cybercrime attack is now \$10,000, up from \$1,000 just a few years ago.

Without global coordination, these threats will escalate, impacting individuals, businesses, and governments worldwide.

THE SOLUTION: PROJECT STARDUST

INTERPOL's Project Stardust will create an ecosystem that hinders the activities of cybercriminals through:

- GLOBAL OPERATIONS**
Coordinate international law enforcement to identify and shut down the infrastructure and identify those administering them and using them to implement cybercriminal activity.
- STRENGTHENING OF PREVENTIVE CAPACITY**
Collaborate with relevant stakeholders to identify and address root causes of non-reported and unreported cyber threats.
- PUBLIC OUTREACH AND RISK COMMUNICATION**
Inform the public and engage with relevant stakeholders to prevent or limit the impact of cyber threats, and limit the damage to victims.
- DEVELOPMENT OF BEST PRACTICES AND A FRAMEWORK FOR COORDINATED ACTION**
Develop a comprehensive framework and a set of best practices that will enable a coordinated and coordinated action against the operators and users of services involved in the industrialization of cybercrime.
- CAPABILITY DEVELOPMENT**
Provide training and capacity building to law enforcement agencies in INTERPOL member countries to successfully investigate and prosecute the threat of the industrialization of cybercrime.



PROJECT ECHO

OPERATIONAL RESPONSE TO ONLINE INTIMATE IMAGE ABUSE AND DIGITAL SEX CRIMES

Current Situation	The Problem In Numbers
Image-based sexual abuse, sexual extortion, and the non-consensual creation or distribution of intimate images represent one of the fastest growing forms of digital sexual crime worldwide. These offenses occur both through traditional digital means and through the criminal misuse of emerging technologies such as artificial intelligence (AI).	- In 2024, the FBI's ICS reported 54,416 instances of sexual abuse and 22,222 instances of sexual extortion, with adult age groups accounting for the majority of cases. - In 2024, the FBI's ICS reported 54,416 instances of sexual abuse and 22,222 instances of sexual extortion, with adult age groups accounting for the majority of cases. - In 2024, the FBI's ICS reported 54,416 instances of sexual abuse and 22,222 instances of sexual extortion, with adult age groups accounting for the majority of cases.
Reproduction, digital sexual abuse, platform, removing, distribution, online forums, and social communication tools, and digital payment systems to target victims, adult users, online commerce, and other operational and psychological harm. In some cases, offenders manipulate digital means to exploit victims, they generally synthesize content using AI tools, and in many instances, they pay or simply use highly visible methods of victimization and abuse.	- Extensive evidence to the FBI's ICS report that 70% of all reported digital sexual abuse are non-consensual intimate images and 70% of all reported digital sexual abuse are non-consensual intimate images and 70% of all reported digital sexual abuse are non-consensual intimate images. - In 2024, the FBI's ICS reported 54,416 instances of sexual abuse and 22,222 instances of sexual extortion, with adult age groups accounting for the majority of cases.

THE SOLUTION: PROJECT ECHO

Project ECHO is built on three mutually reinforcing operational pillars designed to move from intelligence to action, and from action to reassessable enforcement outcomes.

PILLAR 1	PILLAR 2	PILLAR 3
INTELLIGENCE AND THREAT ECOSYSTEM To create targeted intelligence of digital image-based sexual abuse, and other related digital sexual abuse, and other related digital sexual abuse, and other related digital sexual abuse.	OPERATIONAL CAPABILITY AND INVESTIGATIVE EFFECTIVENESS To conduct intelligence into reassessable enforcement outcomes, the pillar strengthens frontline investigative effectiveness through operational response and case-based response to cybercrime, including training, support, and other related digital sexual abuse.	COORDINATED INTERNATIONAL DISRUPTION AND ENFORCEMENT To maximize international enforcement at scale, this pillar drives cross-border investigations and joint operations across the globe, including training, support, and other related digital sexual abuse.



PROJECT HARPOON

The Problem	The Problem By The Numbers
Phishing is one of the most common cyber threats to individuals, businesses, and governments. It involves tricking victims into revealing sensitive information, such as login credentials, financial data, or other confidential information. It often involves the use of social engineering, phishing kits, and other tools to trick victims into revealing sensitive information.	- In 2024, the FBI's ICS reported 54,416 instances of phishing, with adult age groups accounting for the majority of cases. - In 2024, the FBI's ICS reported 54,416 instances of phishing, with adult age groups accounting for the majority of cases. - In 2024, the FBI's ICS reported 54,416 instances of phishing, with adult age groups accounting for the majority of cases.
In the past, individual and global threat actors have targeted critical infrastructure, including healthcare, energy, and financial services, and other related digital sexual abuse, and other related digital sexual abuse, and other related digital sexual abuse.	- In 2024, the FBI's ICS reported 54,416 instances of phishing, with adult age groups accounting for the majority of cases. - In 2024, the FBI's ICS reported 54,416 instances of phishing, with adult age groups accounting for the majority of cases. - In 2024, the FBI's ICS reported 54,416 instances of phishing, with adult age groups accounting for the majority of cases.

THE SOLUTION: PROJECT HARPOON

INTERPOL's Project Harpoon will build a proactive, scalable global system to fight phishing through coordinated action by law enforcement, industry, and judicial partners, including the following elements:

- DISRUPTION CELL**
A global network of law enforcement agencies and other stakeholders to identify and disrupt phishing operations.
- INTELLIGENCE INFORMATION**
A global network of law enforcement agencies and other stakeholders to identify and disrupt phishing operations.
- INVESTIGATIVE FRAMEWORK**
A global network of law enforcement agencies and other stakeholders to identify and disrupt phishing operations.
- ANTI-FISHERY TOOLKIT**
A global network of law enforcement agencies and other stakeholders to identify and disrupt phishing operations.
- ALIGNED THREAT RESPONSE**
A global network of law enforcement agencies and other stakeholders to identify and disrupt phishing operations.



PROJECT SYMPHONY

Current Situation	The Problem By The Numbers
Cyberattacks targeting critical infrastructure, including healthcare, energy, and financial services, and other related digital sexual abuse, and other related digital sexual abuse, and other related digital sexual abuse.	- In 2024, the FBI's ICS reported 54,416 instances of cyberattacks, with adult age groups accounting for the majority of cases. - In 2024, the FBI's ICS reported 54,416 instances of cyberattacks, with adult age groups accounting for the majority of cases. - In 2024, the FBI's ICS reported 54,416 instances of cyberattacks, with adult age groups accounting for the majority of cases.
The threat of cyberattacks continues to grow, with the average breach cost rising to \$4.4 million in 2024, up from \$3.9 million in 2023.	- In 2024, the FBI's ICS reported 54,416 instances of cyberattacks, with adult age groups accounting for the majority of cases. - In 2024, the FBI's ICS reported 54,416 instances of cyberattacks, with adult age groups accounting for the majority of cases. - In 2024, the FBI's ICS reported 54,416 instances of cyberattacks, with adult age groups accounting for the majority of cases.

THE SOLUTION: PROJECT SYMPHONY

INTERPOL's Project Symphony will strengthen global defense against cyberthreats to critical infrastructure through:

- ADVANCED TRAINING ECOSYSTEM**
A global network of law enforcement agencies and other stakeholders to identify and disrupt phishing operations.
- CRISIS BUSINESS RESPONSE NETWORK**
A global network of law enforcement agencies and other stakeholders to identify and disrupt phishing operations.
- KNOWLEDGE EXCHANGE PLATFORM**
A global network of law enforcement agencies and other stakeholders to identify and disrupt phishing operations.
- MAJOR EVENT PROTECTION**
A global network of law enforcement agencies and other stakeholders to identify and disrupt phishing operations.
- CAPABILITY DEVELOPMENT**
A global network of law enforcement agencies and other stakeholders to identify and disrupt phishing operations.

Projects empower the INTERPOL Cybercrime Directorate to tackle new national security priorities.



STRONGER TOGETHER

Our response must be equally connected - across borders,
across sectors, and across disciplines.

**WHATEVER COUNTRY THE EVENT IS HOST IN /
COMPANY THAT IS HOSTING US is a critical partner in
this effort.**

Thank you

Enrique HERNANDEZ GONZALEZ
Assistant Director Cybercrime Operations, INTERPOL
Cybercrime Directorate
e.hernandezgonzalez@interpol.int



CHECK OUR WEBSITE!