INTERPOL

INTERPOL GLOBAL CYBERCRIME CONFERENCE 2023

"CREATING COMMUNITIES TO PROTECT COMMUNITIES"

Outcome Report

TABLE OF CONTENTS

OVERVIEW

Introduction

Today, the world is more digitally connected than ever before. Criminals take advantage of this online transformation to target weaknesses in online systems, networks and infrastructure, causing significant economic and social impact on governments, businesses and individuals worldwide. Phishing, ransomware and data breaches are just a few examples of current cyberthreats, while new types of cybercrime are emerging all the time. Cybercriminals are increasingly agile and organized – exploiting new technologies, tailoring their attacks and cooperating in new ways.

In the face of this evolving threat landscape and the need for greater global connectivity, the INTERPOL Global Cybercrime Programme convened **the first in-person INTERPOL Global Cybercrime Conference** from 15 to 17 October in Singapore, to bring together leaders from law enforcement, the private sector, international organizations and academia. This is in line with the mandate of the INTERPOL Global Cybercrime Programme: **"Reducing the global impact of cybercrime and protecting communities for a safer world."** The timing of the meeting was particularly opportune, as INTERPOL marked the hundred years of its existence in 2023.

INTERPOL would like to take this opportunity to thank each and every organization and individual involved in the 2023 INTERPOL Global Cybercrime Conference. Your contribution was essential to making this conference one of the largest and most successful conferences on Cybercrime.

Overview of the 2023 edition

The first in-person **INTERPOL Global Cybercrime Conference (IGCC)** was organized by the INTERPOL Cybercrime Directorate from 15 to 17 October 2023 at the INTERPOL Global Complex for Innovation (IGCI) in Singapore.

Under the theme of **"Creating communities to protect communities"**, the conference brought together more than 130 leaders from law enforcement, international organizations, academia and the private sector, representing over 50 countries and all INTERPOL regions. Over the course of three days, participants were able to hear from more than 30 speakers presenting case studies, sharing best practices, debating through panel discussions and exploring areas for synergies and collaboration. In addition, the conference provided participants the opportunity to network and exchange with peers from across countries and sectors, in line with the IGCC theme of creating communities to protect communities.

Geographical distribution of participants to the 2023 INTERPOL Global Cybercrime Conference (IGCC).

Kicking off on 15 October 2023, the IGCC featured **the first of its kind INTERPOL Women in Cyber workshop**. The session brought featured distinguished speakers from across cyber, including:

- **Dr. Monisha OBEROI** (ISA Security Services Lead / APAC Security Services Sales Lead, IBM Security Services),
- **Ms. Corien VERMAAK** (Director of Cybersecurity, Cisco Australia and New Zealand),
- **Ms. Isabella WILKINSON** (Research Associate, International Security Programme at the Royal Institute of International Affairs – Chatham House),
- **Dr. Nnenna IFEANYI-AJUFO** (Vice-Chairperson of the African Union Cyber Security Experts Group and Chair of the Cybercrime Working Group of the Global Forum on Cyber Expertise),
- **Ms. Beatriz SILVEIRA** (Former INTERPOL Cybercrime Intelligence Officer),

- **Ms. Lauren MISSLER** (Regional Specialized Officer, Cybercrime Directorate, INTERPOL),
- **Ms. LEE Pei Ling** (Head of Cyber Strategy and Capabilities Development, INTERPOL) and
- **Ms. Cristiana NADOR** (Policy Analyst, Cybercrime Directorate, INTERPOL).

Speakers shared their experiences and discussed with participants different avenues to advance gender inclusivity in cyber law enforcement. A separate report on the event has been prepared by the INTERPOL Cybercrime Directorate, please contact cyberconf@interpol.int for more information.

Speakers and participants of the first ever INTERPOL Women in Cyber Workshop.

Simultaneously, on 15 October, **Mr. Carlos ALVAREZ** delivered a workshop on behalf of **the Internet Corporation for Assigned Names and Numbers (ICANN)**. Mr. Alvarez, who serves not only as the ICANN Director Trust and Public Safety Engagement but also as a Member of the Board of Director of the Forum of Incident Response and Security Teams (FIRST), explained **the Domain Name System (DNS)** and its importance for cybercrime investigations, providing participants with examples of concrete tools and investigative methods.

The main conference of the 2023 IGCC took place on 16 October. **Mr. Stephen KAVANAGH, INTERPOL Executive Director of Police Services**, welcomed participants, noting that close international collaboration using INTERPOL channels is essential to counter the highly organized, interconnected and sophisticated networks behind cybercrime (*please refer to p.8 for the full speech*). **Her Excellency Minister Josephine TEO, Singapore's Minister for Communications and Information and Second Minister for Home Affairs**, then delivered a keynote speech, during which she exhorted participants to collectively take action as a global community to better protect our people (*please see p. 11 for the full speech*).

The rest of the main conference comprised of **four blocks, moderated by Mr. Craig JONES, INTERPOL Director for Cybercrime**, and featuring a combination of presentations, case studies, and panel discussions with experts from law enforcement, government, international organizations, the private sector and academia from all over the world. The topics of the four blocks were determined in line with **the INTERPOL Global Cybercrime Strategy 2022 – 2025**: **(i) Prevention**, **(ii) Detection, (iii) Investigation**, and **(iv) Disruption**.

The **INTERPOL Global Cybercrime Strategy 2022 - 2025** is available online here: t.ly/VsZHi

Key points and takeaways of the four blocks are presented in detail in this report. In addition, the presentation materials will be made available through the INTERPOL Cybercrime Knowledge Exchange (CKE), the Organization's secure information sharing platform. Should you require access to the CKE, please contact us via email at **cyber.support@interpol.int**.

The last day of the conference, taking place on 17 October, consisted of two concurrent tracks. **The first track consisted of a Law Enforcement Open Forum**. It opened with an overview of **the INTERPOL Global Cybercrime Programme**, its key capabilities and ongoing activities, delivered by different members of the team. This was followed by a panel discussion entitled "Capacity Building for Countering and Combating Cybercrime in the Global South: Best Practices from the Stakeholder Community", featuring as speakers **Mr. Christopher PAINTER** (President of the Global Forum on Cyber Expertise (GFCE) Foundation Board), **Dr. Nnenna IFEANYI-AJUFO** (Vice-Chairperson of the African Union Cyber Security Experts Group and Chair of the Cybercrime Working Group of the GFCE), **Mr. Allan S. CABANLONG** (GFCE Regional Director for Southeast Asia), and **Mr Orhan OSMANI** (Head Acting Interim Cybersecurity Division at the Telecommunication Development Bureau, International Telecommunications Union). The panel was followed by an open session dedicated to the sharing of best practices and success stories from different INTERPOL member countries. There was then an interactive discussion between law enforcement representatives and staff from the INTERPOL Global Cybercrime Programme.

Meanwhile, **Track 2, dubbed the "technical track"**, provided participants with live demonstrations and expert presentations. **Ms. Vesta MATVEEVA** (Head of High-Tech Crime Investigation Department, APAC, Group-IB) delivered hands-on practical exercises and demonstrations on investigating and combating phishing threats. This was followed by a presentation on the APNIC Community Honeynet Project by **Mr. Jamie GILLESPIE** (Senior Internet Security Specialist, Asia Pacific Network Information Centre - APNIC), who focused on the technical aspects of the project and on how law enforcement could benefit and contribute to the project. Participants then heard from **Mr. Vitaly KAMLUK** (Principal Security Researcher, Kaspersky) on the rising threat of self-spreadable malware, and from Bi.Zone representatives **Mr. Gennady GRIGORIEV** (Head, Emerging Threats Search and Analysis Department) and **Mr. Ilya TITOV** (Analyst, Emerging Threats Search and Analysis Department) on Hook malware, an Android malware expanding in Asia and the Middle East. Next, **Mr. Krassimir T. TZVETANOV** (Graduate Research Assistant, Purdue University) spoke about OpSec for investigators, covering different browser and infrastructure fingerprinting techniques, browser hooking, instant messaging programs, email security and tracking.

Finally, **Mr. Bernado PILLOT, Assistant Director in charge of INTERPOL Cybercrime Operations**, closed day 3 of the conference, bringing to an end the first in person INTERPOL Global Cybercrime Conference. Participants then had the option to attend **the Singapore International Cyber Week (SICW)**, the most established cybersecurity conference and exhibition in the Asia-Pacific region, which was taking place from 17 to 19 October.

H.E. Josephine Teo, Singapore's Minister for Communications and Information and Second Minister for Home Affairs, with (left of picture) Stephen Kavanagh, INTERPOL Executive Director of Police Services, and Craig Jones, INTERPOL Director of Cybercrime.

KEY TAKEAWAYS OF THE MAIN CONFERENCE

Welcome remarks & keynote speech

WELCOME REMARKS & KEYNOTE SPEECH

Welcome remarks by Mr. Stephen KAVANAGH, INTERPOL Executive Director of Police Services

Your Excellency, Ms. Josephine Teo, Minister for Communications and Information & Second Minister for Home Affairs,

Dear Delegates, Colleagues and Friends,

Ladies and Gentlemen,

Good morning and a warm welcome to the first in-person INTERPOL Global Cybercrime Conference, here at the INTERPOL Global Complex for Innovation that has been our home, housing our Cybercrime Programme, since 2014.

Yes – you heard it correctly. This is our first face-to-face conference dedicated to coordinating and enhancing our joint global efforts in countering and combating cybercrime.

As we come together today, we are not just attending an event; we are also celebrating a significant moment in INTERPOL's 100-year journey. This conference symbolizes a fresh start and our dedication to a new century of collaboration.

Allow me to start with some of my own observations.

While traveling from Lyon to Singapore, I was reflecting about the complex nature of cybercrime.

This insidious threat often slips through our understanding. But why? Because it leaves no broken windows, no bullet cases, no bruises on its victims.

Yet, its effects are profound, far-reaching, and pervasive.
Misunderstood, cybercrime is frequently reduced to stereotypes: a lone hacker wearing a hoody in his parents' basement.

The reality? You are the experts. You know and understand that the world of cybercrime consists of criminal networks that operate at both volume and scale. They are highly organized, interconnected, and generating revenue figures that many legitimate businesses could only dream of. In other words: they are everywhere; they are very powerful and motivated by financial gain.

Let me present to you a recent case study that shows how deep and interconnected cybercrime has become: the so-called '16Shop' platform. This 'phishing-as-a-service' scheme was not run by some solitary misfit but was an internationally coordinated operation that spanned across continents. Criminals behind it were advertising and selling 'phishing kits' tailored to well-known brands such as Apple, PayPal, American Express, Amazon, and many more.

These 'phishing kits' then enabled affiliates to exploit Internet users, where victims were sent deceptive emails containing pdf files or links. When accessed, these links led to sites cunningly designed to collect the victims' credit card or personal details. In their wake, at least 70,000 innocent users from 43 countries fell victim, inadvertently divulging personal information. I am talking about email accounts and passwords, ID cards, credit cards, telephone numbers and much more.

This data was stolen and, in turn, resulted in financial losses, identity theft, data breaches, operational disruptions, and undoubtedly, psychological and emotional distress, leaving a very long shadow of consequences resulting from just a few clicks.

This is where INTERPOL's extensive collaboration with law enforcement agencies as well as public and private sectors plays such a crucial role. I would cite just this one example – there are many more I could give. INTERPOL worked closely with Indonesia, Japan, the United States, as well as members of our consortium of tech giants, to ensure the successful takedown of the '16Shop' platform and the apprehension of its operators. This operation spanned from the beginning of 2021 and closed only a few months ago, with the final arrest in August 2023.

This speaks to all, of our persistence - our commitment – our dedication as a community. To prevent, detect, investigate, and disrupt cybercrime in collaboration. I know that representatives from these countries and our Gateway partners such as Group-IB; Palo Alto; and Trend Micro are present here today. Thank you for trusting us in that investigation and many more.

Dear Colleagues, to achieve the profound impact that we have showcased, we need to create a resilient and robust cyber security architecture, that can adapt and respond to the continuously evolving criminal threat landscape.

We are both the architects and

the answer to this need. This is why the theme of this event is: “Creating Communities to Protect Communities”. Communities amongst countries. Communities with relevant organizations. Communities between public and private sector.

This Conference is a symbol of our commitment to inclusivity and integration, representing INTERPOL strategic values moving us towards creating and constructing these vital communities.
Through each session, we are not just going to discuss the threat and the related challenges; we are seeking to better understand the cyber ecosystem, by defining our individual and collective roles and responsibilities; and making ourselves accountable for reducing the global impact of cybercrime and protecting communities for a safer world.

In line with that, we will wrap up the INTERPOL Global Cybercrime Conference with a concise report highlighting best practices and recommendations. This report, which will be shared with you all, will serve as an integral part for planning and executing the future activities of all our offices.

In conclusion, I would like to take a moment to express our gratitude to Singapore. When this building opened its doors the first time, back in September 2014, our then previous Secretary General defined this event “a milestone in the history of international law enforcement”.

Almost ten years later, we all walked through those open doors once more today, into this building that stands as a testament not just to INTERPOL's leadership in navigating the rapidly changing landscape of crime; but also, to the continued trust and support of the Singaporean authorities and all of our 195 member countries that you represent. With this in mind, I feel honored to hand over the floor to Minister, Ms. Josephine Teo.

Colleagues, thank you all for being here today. And a special thank you to the Cyber Directorate team for organizing all of this.

And please remember: in a world where the nature of crime is ever-changing, it is through our collective resilience that we pave the way for a safer world.

Keynote Speech by Mrs. Josephine TEO, Minister for Communications and Information and Second Minister for Home Affairs

Mr. Stephen Kavanagh, Executive Director of Police Services, INTERPOL

Distinguished guests,

Colleagues and friends,

1. Good morning. I am very pleased to be able to address you at this important conference.

Growing Prevalence of Cybercrime

2. Director Kavanagh has given a passionate speech. You can feel his energy and resolve. I think it is indeed these two key attributes that we will need to bring to the fight against cybercrime.

3. In the 2022 INTERPOL Global Crime Trend Report, cybercrime is listed as one of the five crime types that continue to pose a serious threat to governments, businesses and people.

4. Digital connectivity has made it easier for people to reach each other. Unfortunately, it is also making it easier for criminals to reach their victims. Criminals are finding it highly lucrative to exploit new technologies to commit cybercrime, particularly scams, whilst hiding or masking their identities.

5. A study by the Global Anti Scam Alliance found that around US$55 billion was lost to scams worldwide in 2021. I think you and I know that this is likely an underreported figure, because many victims of scams choose not to report their losses. The reasons are well articulated by Stephen. Sometimes, there is a certain amount of embarrassment, and sometimes there are conflict situations that have arisen at home as a result of such scams having been carried out. And so, the individuals prefer not to have to deal with it. The total number of scams reported was 293 million. Again, my own sense is that this is still an underestimate. These are still, nonetheless, staggering numbers.

6. Likewise, scams have become a key concern for Singapore.

(a) Last year, there were about 32,000 cases reported; S$660 million were lost to scams.

(b) In the first half of this year alone, the total amount lost declined marginally.

However, the number of scam cases increased sharply by more than 60%. What this tells us is that the average amount lost by each victim has fallen. But until the cases are significantly reduced, there are still too many distressed victims.

7. The Singapore Police Force has been working closely with other government agencies and private sector organizations to combat scams.

8. In 2019, the Police set up the Anti-Scam Centre, or ASC, to enable the swift interdiction of criminal proceeds. To date, the ASC has frozen more than 49,000 bank accounts and recovered more than S$360 million.

9. In 2022, the Police set up the Anti-Scam Command (ASCom) to consolidate and optimize resources as well as expertise to tackle scams. The command comprises the ASC and the Anti-Scam investigation branches and oversees the Scam Strike Teams situated within each of the seven Police Land Divisions. This enables swifter and well-coordinated actions.

(a) The ASCom partners more than 90 institutions including local and foreign banks to fight scams.

(b) Today, six banks have deployed their staff in ASCom to facilitate real-time coordination with the Police to trace the flow of funds and freeze suspicious bank accounts.

Importance of International Cooperation

10. However, due to the transnational nature of many of these scams being carried out, tackling them effectively requires countries to work closely together.

11. Singapore certainly does so with our foreign partners and international organizations such as INTERPOL to share information and conduct investigations and joint operations targeting scam syndicates. These efforts have led to successful crackdowns on scam syndicates in the Southeast Asia region. For example:

(a) Singapore took part in INTERPOL's Operation "Killer Bee", which involved 11 countries, and led to the arrest of three suspects of malware cyber fraud in May 2022.

(b) Singapore also took part in INTERPOL's Operation HAECHI, from 2020 to 2022, which involved 30 countries, and led to the arrests of more than 2,000 suspects and the recovery of about US$240 million linked to cyber-enabled financial crimes and money laundering.

12. The success of these operations demonstrates the importance of international cooperation in fighting cybercrime.

Improve Asset Recovery

13. One important area that deserves attention is asset recovery. The United Nations Office on Drugs and Crime estimates that the global asset recovery rate is less than 1%. Now, this means that perpetrators have been able to keep 99% or more of their criminal proceeds. This is a "return on investment"; an ROI legitimate businesses can only dream about. No corporate CEO will dare to come anywhere close to suggesting to their shareholders that they will have these kinds of return on investment.

14. But, because these criminal proceeds are often extracted from the system through cross-border transfers, unfortunately for victims, the cross-border asset recovery is very unlikely to bear fruit. Funds can be transferred across jurisdictions very quickly, often before the crime is even reported. Law enforcement agencies must react even more quickly and cooperate closely with our counterparts to stop the fund transfer. However, jurisdictions have different standards and processes on tracing fund flows and freezing of funds. It's no wonder that these syndicates have decided to exploit this weakness.

15. To overcome these challenges, we need a major mindset shift. We have to prioritize asset recovery in order to deter the criminals. As long as criminals get to retain most of their ill-gotten gains, I think it is very difficult to persuade them to stop. They won't decide that there are other more productive ventures unless we are able to show them that this is not something that will bear too much fruit for them. We must therefore strengthen our work in global asset recovery by cooperating more closely with one another.

(a) We must all have the domestic legal frameworks to enable quick freezing and confiscation of criminal proceeds.

(b) We must adopt tools to enhance our ability to seize and confiscate illegal proceeds.

(c) We also need to strengthen our global law enforcement community – one of the most important features of today's conference and collaborate more closely on a global scale.

16. For instance, the Financial Action Task Force (FATF), under Singapore's presidency, has partnered INTERPOL to initiate the FATF-INTERPOL Roundtable Engagement on Asset Recovery (FIRE) last year. This is summarized as the FIRE initiative.

(a) Last month, around 200 experts in financial crime came together at the second FIRE event to discuss how we can overcome global challenges in asset recovery through their panel discussions and sharing of real-life case studies.

(b) Such platforms provide opportunities for the international community to come together to discuss and find solutions to address challenges faced in asset freezing, seizure and confiscation.

(c) Singapore is also working with INTERPOL and Egmont Group at the FATF to co-lead a project to counter the illicit funding of cyber-enabled fraud. This project will provide a comprehensive picture of the risk landscape and share the best practices on national and international responses. We urge countries to review the report when it is published and consider implementing the recommendations.

17. We need to continue these important discussions and collaboration by leveraging bilateral, regional and international platforms such as INTERPOL to improve information sharing and exchange best practices.

Conclusion

18. On this note, let me reinforce once again, the theme of today's conference being "Creating Communities to Protect Communities". Indeed, we need the global community to work closer together to fight cybercrime effectively and protect our people from cybercriminals. Let us take the necessary actions as a community so that we can better protect our communities.

19. I wish you all a fruitful conference today. Thank you.

H.E. Josephine Teo, Singapore's Minister for Communications and Information and Second Minister for Home Affairs and Stephen Kavanagh, INTERPOL Executive Director of Police Services.

KEY TAKEAWAYS OF THE MAIN CONFERENCE

Block 1: Prevention

BLOCK 1: PREVENTION

Introduction

The strategies for preventing cybercrime encompass a diverse range of approaches. These include enhancing collaboration among law enforcement agencies, and/or relevant stakeholders like cybersecurity agencies and the private sector; increasing the capacity of domestic criminal justice systems through legislative measures and technical support; establishing standards for products to prioritize security by design or offering bug bounty programmes to identify vulnerabilities promoting public awareness, cyber hygiene, and education; or addressing the socio-economic factors contributing to cybercrime to prevent offenses and/or facilitate the reintegration of offenders.

What these preventive measures have in common is that they require the active involvement of multiple stakeholders – in other words, they require building communities. Accordingly, in the 1st Block of the IGCC, participants were exposed to best practices in creating communities to strengthen prevention against cybercrime. This included presentations by three speakers, each showcasing different cybercrime preventive measures, as well as how they approached the challenge of building communities to protect communities to successfully implement these measures:

Mr. Cyrus VANCE Jr., Global Chair of the Cybersecurity Practice, Baker & McKenzie.

Ms. Floor JANSEN, Deputy Department Head, Dutch National High Tech Crime Unit, Netherlands Police.

Mr. Andrew GOULD, Detective Chief Superintendent, City of London Police – National Cybercrime Programme Lead for National Police Chiefs' Council, United Kingdom

Prevention, cyber resilience and response – experiences from co-founding the New York City Critical Infrastructure Task Force

During his time as Manhattan District Attorney, Mr. Vance Jr. contributed to the launch of **the New York City (NYC) Cyber Critical Services and Infrastructure (CCSI) Project,** a new citywide initiative aimed at coordinating digital law enforcement efforts. This was the focus of his presentation, entitled "Prevention, cyber resilience and response – experiences from co-founding the New York City Critical Infrastructure Task Force."

- In November 2017, **the Manhattan District Attorney's Office, the New York Police Department (NYPD), the New York City Cyber Command, and the Global Cyber Alliance** (an international nonprofit) convened members of New York City's local cyber community. This gathering followed several high-profile cyber-attacks against the critical infrastructure of cities around the United States, which had caused significant financial loss and harm to communities.
- A major realization that emerged from the meeting was the lack of dialogue and information exchange across different sectors about cybersecurity, especially at the local level. In turn, this fragmentation created blind spots and risked leaving the whole city ecosystem vulnerable to attacks.
- In response, the Manhattan District Attorney's Office, NYPD, the New York City Cyber Command, and the Global Cyber Alliance established a formal partnership known as the NYC Cyber Critical Services and Infrastructure (CCSI) Project. This citywide initiative aimed to enhance cyber prevention efforts and build a ring of steel around the city's critical services and infrastructure – including emergency services, water systems, energy producers, and other critical services.
- To protect New York City's infrastructure from cyber-attacks, the CCSI brought together **local cybersecurity experts from across 17 industry sectors**. Efforts were focused around three main themes: (1) regularly receiving and sharing cyber intelligence across sectors at the municipal level; (2) training together to develop a coordinated response to major cyber incidents, including through tabletop exercises; and (3) establishing the United States' first municipal "cybersecurity defense centre", with a physical presence in lower Manhattan.
- While the CCSI project was initially developed discreetly, in 2019 the initiative became public, expanding their community by inviting more local experts to join the initiative to share cyber threat intelligence and develop a coordinated, city-wide response to cyber-attacks. **To date, CCSI includes more than 280 professionals from public organizations and private companies**.

- In closing, it was emphasized that **cybersecurity needs to be a shared responsibility.** The CCSI project was compared to the olden days when people would come together to pass buckets of water to put out fires. Today, we need "cyber fire brigades" that provide a coordinated response to major cyber-attacks, passing along intelligence (instead of water). This should be done at different levels: there is no path forward unless entities at the national and local level develop their own strategies to prevent and remediate attacks as a community.

The International Cyber Offender Prevention Network (InterCOP)

Ms. Floor Jansen presented on **the International Cyber Offender Prevention Network (InterCOP)**, challenging common understandings of who should be included in the communities that protects communities. Her presentation also included a video on behalf of the Danish police about the “Danish Online Patrol”.

- Preventing cybercrime without pursuing offenders is toothless; but pursuing without preventing is endless. Recognizing that we cannot simply arrest ourselves out of cybercrime, in recent years law enforcement agencies around the world have been experimenting with different preventive measures.
- For example, in 2022 the Danish police established **the Danish Police Online Patrol.** The aim of this special online unit is to strengthen the digital presence of the Danish police, "patrolling" on social media and gaming platforms to prevent inappropriate behavior and crime, and to enable citizens to engage with digital police officers online - just like they would on the street. This initiative recognizes that communities, and especially children and young people, are spending an increasing amount of time in the cyber realm, and therefore that the police cannot afford not to be online. In short: the Danish police is online because everyone is online.

The Danish police have created a special online unit called Politiets Online Patrulje (Police Online Patrol). Image source: https://mezha.media/en/2022/12/19/the-danish-police-created-the-police-online-patrol-which-plays-games-with-young-people/

- Meanwhile, **the Netherlands Police** is adopting a holistic approach to the prevention of cybercrime, which can be summarized through 4 "D"s: **deter, divert, degrade and disrupt.**
  - *Deter*: create public awareness, increase perception of risk, highlight legal and life implications.
  - *Divert:* highlight positive alternatives, preserve and gain talent, stimulate informed choices.
  - *Degrade*: devalue reputation of profiles, products and platforms used by serious offenders.
  - *Disrupt*: disrupt criminal markets, means and methods, combine lower-level arrests with off and online prevention, create barriers to entry.
- One aspect of this holistic approach is **cyber offender prevention (COP)**. In The Netherlands, it has been observed that compared to offline offenders, many cyber offenders tend to be relatively young, may not realize the full implications of their criminal behaviour, and usually only encounter corrective measures well into their cybercriminal career. Recognizing cyber offender prevention as an effective and necessary part of the response to cyber criminality, the Dutch Police has set up **a specialized Cyber Offender Prevention team** (as part of its National High Tech Crime Unit). This team has launched several campaigns to inform young people about the illegality of certain of forms of cyber behaviour - and the consequences that might ensue. It may also conduct cease and desist visits offline. The team works with a range of partners from the public and private sector to divert at risk youth or those who already crossed the line to legitimate cybersecurity organizations, allowing them to use their cyber skillsets in more socially productive ways. Examples include initiatives such as re: B00TCMP and Hack Right.
- To harness international cooperation and maximize the impact of its work on cyber offender prevention, in 2023 the Netherlands established **the International Cyber Offender Prevention network (InterCOP)**, with funding provided by the European Commission. Now featuring 26 countries, the InterCOP network aims to connect international law enforcement agencies to share expertise and best practices on cyber offender prevention and jointly develop, carry out and evaluate related interventions. Some recent successes include the development of **the CyberChoice Brand** by **the United Kingdom National Crime Agency (NCA)** and the establishment of an **"International Cyber Offender Prevention Day" on 15 June.** Ultimately, InterCOP aims to create a community featuring not just law enforcement but also stakeholders from the public and private sector to guide young cyberskilled individuals and build a safer online world for all.

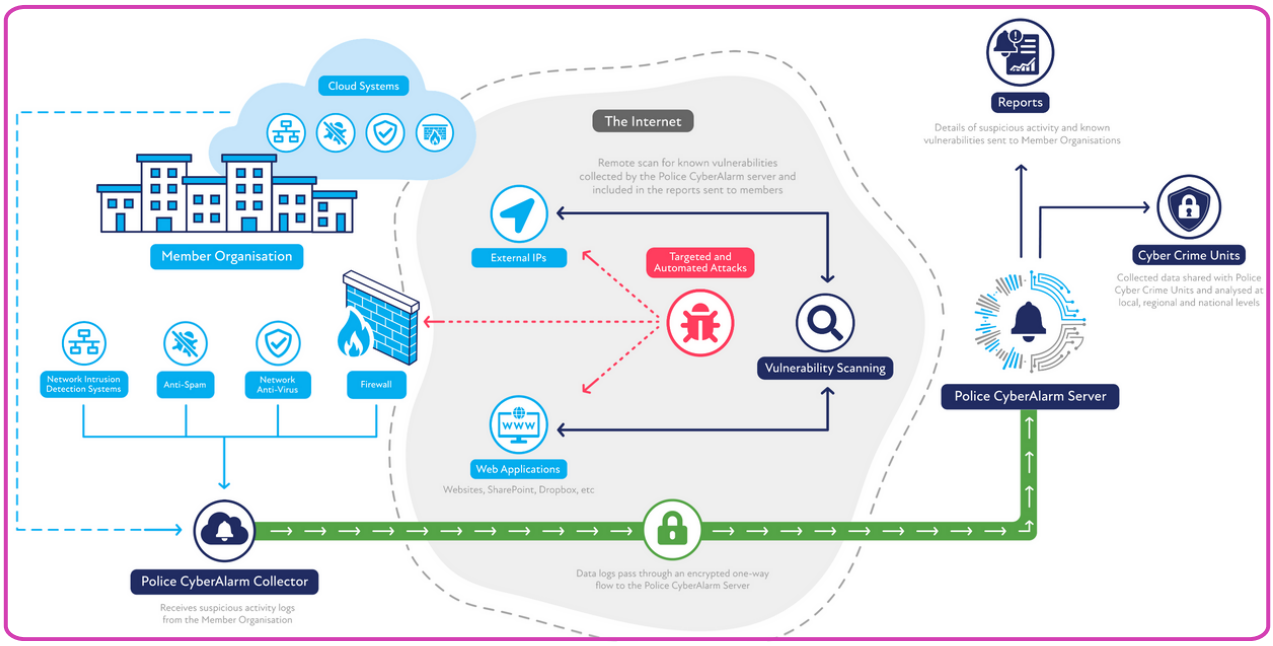
For more information on **the International Cyber Offender Prevention network (InterCOP)**, please see:

https://www.politie.nl/en/information/what-does-the-the-international-cyber-offender-prevention-network-intercop-do.html

Law Enforcement in the United Kingdom - Protecting Small and Medium Sized Organizations from Cybercrime Through Innovation

In his presentation, **Mr. Andrew Gould** explained some of the innovative preventative measures which the UK police has deployed to protect small and medium sized organizations from cybercrime.

- In the United Kingdom, the police have developed the **"Police CyberAlarm"** with funding from the Home Office. This free tool empowers small and medium organizations to detect, monitor and report the suspicious cyber activity they face, by monitoring the logs of traffic seen by a member's connection to the internet.



Visual representation of how the UK's Police CyberAlarm works.
Image source: https://cyberalarm.police.uk/police-cyber-alarm/how-it-works/

- By voluntarily joining Police CyberAlarm, organizations receive regular reports of suspicious activity, and are able to conduct vulnerability assessments by scanning their business website and external IP addresses for known vulnerabilities and gain access to intelligence on the latest cyber threats.
- In turn, the information provided by members of Police CyberAlarm enable the

UK police to proactively and more comprehensively develop a picture of the cyber threat landscape, informing cyber defence strategy and collecting evidence that can be used in the identification, pursuit and prosecution of criminals.

- **To date, over 8000 members have joined the Police CyberAlarm**, fostering a UK wide cyber defence network that shares collected data with law enforcement for analysis at local, regional and national levels to identify trends, react to emerging threats and identify, pursue and prosecute cyber criminals.
- Over a billion suspicious events have been identified since the launch of Police CyberAlarm. Demonstrating the effectiveness of the tool, of the 2,100 critical/high vulnerabilities detected in 2022, 60% were fixed by members within a month.

For more information on Police CyberAlarm, please visit:
www.cyberalarm.police.uk

- **The National Cyber Resilience Centre Group (NCRCG)** is another strong example of "creating communities to protect communities", as it entails a strategic collaboration between the police, government, private sector and academia to help strengthen cyber resilience across the nation's small and medium-sized enterprise (SME) community, in support of the government's National Cyber Strategy.
- Funded by the United Kingdom Home Office, policing and private sector partners, the NCRCG provides a platform to coordinate defence against cybercrime. For example, through "Cyber PATH", the NCRCG has created a talent pipeline from academia to policing, to equip select students with hands on working experience.
- The national reach of the NCRCG is supported by **nine regional Cyber Resilience Centres (CRCs)** spread across England and Wales, whose mission is to provide affordable, high-quality cyber resilience services to smaller organizations in their locality. Such services could include security awareness training, internal or remote vulnerability assessment, security policy review, partner resource support, etc.
- In addition, companies like KPMG, CGI, NatWest, Chainanalysis, The Very Group, Siemens, SANS, Microsoft, Mastercard act as national ambassadors to amplify the work of NCRCG.

UK police to proactively and more comprehensively develop a picture of the cyber threat landscape, informing cyber defence strategy and collecting evidence that can be used in the identification, pursuit and prosecution of criminals.

- **To date, over 8000 members have joined the Police CyberAlarm**, fostering a UK wide cyber defence network that shares collected data with law enforcement for analysis at local, regional and national levels to identify trends, react to emerging threats and identify, pursue and prosecute cyber criminals.
- Over a billion suspicious events have been identified since the launch of Police CyberAlarm. Demonstrating the effectiveness of the tool, of the 2,100 critical/high vulnerabilities detected in 2022, 60% were fixed by members within a month.

For more information on Police CyberAlarm, please visit:
www.cyberalarm.police.uk

- **The National Cyber Resilience Centre Group (NCRCG)** is another strong example of "creating communities to protect communities", as it entails a strategic collaboration between the police, government, private sector and academia to help strengthen cyber resilience across the nation's small and medium-sized enterprise (SME) community, in support of the government's National Cyber Strategy.
- Funded by the United Kingdom Home Office, policing and private sector partners, the NCRCG provides a platform to coordinate defence against cybercrime. For example, through "Cyber PATH", the NCRCG has created a talent pipeline from academia to policing, to equip select students with hands on working experience.
- The national reach of the NCRCG is supported by **nine regional Cyber Resilience Centres (CRCs)** spread across England and Wales, whose mission is to provide affordable, high-quality cyber resilience services to smaller organizations in their locality. Such services could include security awareness training, internal or remote vulnerability assessment, security policy review, partner resource support, etc.
- In addition, companies like KPMG, CGI, NatWest, Chainanalysis, The Very Group, Siemens, SANS, Microsoft, Mastercard act as national ambassadors to amplify the work of NCRCG.

KEY TAKEAWAYS

1. PREVENTIVE MEASURES ARE KEY TO REDUCE THE GLOBAL IMPACT OF CYBERCRIME.

- Addressing cybercrime requires a holistic approach, taking into account not only technical cybersecurity measures, but also coordination across sectors and at the local, national and international levels.
- It is important to aim to intervene at an early stage, promote out of the box thinking and develop proactive, innovative solutions that can complement investigations and disruption, including in terms of cyber offender prevention.
- *The prevention of cybercrime can not only protect communities but also enables key operational outcomes*. For example, by proactively monitoring suspicious activity and vulnerabilities through the Police CyberAlarm, the UK police have been able to identify locally based IP addresses which are causing malicious activity and deal with them accordingly.

2. EFFECTIVE CYBER PREVENTION REQUIRES LAW ENFORCEMENT TO CREATE DIVERSE COMMUNITIES, INVOLVING A RANGE OF PUBLIC AND PRIVATE PARTNERS.

- All three presentations drove home the fact that although law enforcement has a key role to play in prevention, it cannot do it alone. We need to work together with a wide range of stakeholders – other public entities, the private sector, the general public and even potential offenders! Only by creating such communities can we build societies that are resilient to cybercrime.
- **Cybersecurity is a shared responsibility.** The only way to prevent the harm of cybercrime is for different sectors to collaborate and share intelligence on threats and vulnerabilities. Person-to-person, sector-to-sector, real-time cyber collaboration is as important as the technical challenges in cybersecurity.
- The NYC CCSI initiative stands as an example of what can be achieved when different communities come together, even with little investment (for instance, the CCSI used the NYPD's existing application to share information, while IBM sponsored trainings for members of the community). And even developing cyber offender prevention measures like re:B00TCMP and Hack Right required the Dutch Police to cooperate with private and public partners such as municipalities, the Probation Service, Child Care Services, the Public Prosecution Service, etc.

- A service-oriented approach can serve as a strong foundation to create communities that protect communities, as with the UK Police CyberAlarm tool.

3. JUST LIKE NO COUNTRY CAN FIGHT CYBERCRIME ON ITS OWN, NO COUNTRY CAN PREVENT CYBERCRIME ON ITS OWN.

- International cooperation is key to maximize the effectiveness of prevention initiatives such as cyber offender preventive measures.
- As the example of InterCOP demonstrates, international cooperation can allow law enforcement agencies to exchange best practices on cybercrime prevention and jointly develop, carry out, evaluate or amplify related interventions.

ACTIONS FOR INTERPOL

- INTERPOL will continue to facilitate the exchange of best practices on cybercrime prevention.
- Member countries are invited to share successful preventive measures with the INTERPOL. Please contact cyberconf@interpol.int if you would be interested in presenting these measures during future conferences.
- INTERPOL will host the 3rd InterCOP conference in 2024 to enable the exchange of innovative approaches on cybercrime prevention at the international level.

KEY TAKEAWAYS OF THE MAIN CONFERENCE

Block 2: Detection

BLOCK 2: DETECTION

Introduction

Effective cybercrime detection involves a diverse array of strategies but typically requires fostering synergies among law enforcement, cybersecurity experts, and private sector stakeholders. In the second block of the IGCC, participants delved into the best practices for forming collaborative networks specifically tailored to enhance the detection and response to cybercrime incidents.

The block first included presentations from three speakers, each showcasing different cybercrime detection measures, as well as how they approached the challenge of building communities to protect communities to successfully implement them:

Mr. Ted Hyunmin SUH, Director of Business Centre, S2W.

Mr. Stewart GARRICK, Law Enforcement Liaison and Operations Manager, Shadowserver.

Mr. Carlos ALVAREZ, Member of Board of Directors, Forum of Incident Response and Security Teams (FIRST).

Following these three presentations, the final item under Detection was a panel discussion on the topic of "Cybercrime Atlas - Public-Private Partnerships for Detection of Cybercrime", with contributions from:

Mr. Derek MANKY, Chief Security Strategist and VP Global Threat Intelligence, Fortinet.

Mr. Ivo PEIXINHO, Head of Cybercrime Threat Response, INTERPOL.

Ms. Jacky FOX, Senior Managing Director and Europe Lead, Accenture Security.

Introducing DarkBERT: S2W's AI model for combatting cybercrimes at scale in the dark web

S2W is a data intelligence company that focuses on cyber threat intelligence, brand/digital abuse, and blockchain. The firm aims to make the world safer by using technology for justice, offering services such as Threat Intelligence, Digital Abuse Intelligence, and Virtual Asset Intelligence. During the IGCC, an S2W representative presented one of the latest products of the company: **DarkBERT**.

- **DarkBERT is an innovative language model,** designed specifically for understanding the complex linguistic landscape of the Dark Web. This AI model is based on the RoBERTa architecture [1] and has been pretrained on a substantial corpus of Dark Web data, around 5.83 GB of raw text and 5.20 GB of preprocessed text, which was collected over 15 days.
- To ensure ethical standards during the creation of DarkBERT, S2W undertook a meticulous data collection process. Developers gathered data from public repositories and performed rigorous filtering to remove duplicates, balance categories, and eliminate pages with low information density. Within this context, sensitive information was masked or removed entirely from the text corpus before feeding it to the language model.
- In terms of performance, DarkBERT can be used for **Dark Web page classification, ransomware leak site detection, noteworthy thread detection, and threat keyword inference.** DarkBERT excels particularly in understanding the language of hacking forums and ransomware leak sites, offering an effective tool for cybersecurity and CTI applications.
- The dataset used to fine-tune DarkBERT for Dark Web tasks, like the DUTA and CoDA datasets, contained various categories of web pages, including those related to hacking, drugs, financial information, and other illegal activities. Researchers focused on tasks that could potentially cause widespread damage, emphasizing the need for accurate detection of malicious activities.
- One of the unique capabilities of DarkBERT is its fill-mask function, which allows it to predict semantically related keywords in the context of the Dark Web. This function proved effective in identifying keywords associated with threats and drug sales, distinguishing DarkBERT's nuanced understanding of Dark Web language from other models.

[1] In 2018 Google AI released a self-supervised learning model called BERT for learning language representations. Then in 2019, a robustly optimized approach was introduced, called RoBERTa (Robustly Optimized BERT-Pretraining Approach), for pretraining natural language processing (NLP) systems that improve on Bidirectional Encoder Representations from Transformers RoBERTa is a reimplementation of BERT with some modifications to the key hyperparameters and tiny embedding tweaks, along with a setup for RoBERTa pre-trained models.

Shadowserver: expanding global coverage, expanding law enforcement support

The Shadowserver Foundation, established in 2004, is a non-profit organization focused on enhancing internet security through the collection and analysis of data on malicious internet activities such as malware, botnets, and computer fraud. Shadowserver scans 3.7 billion IPv4 addresses 148 times per day, with 381 million hosts responding, making it a comprehensive effort to monitor every device connected to the internet. It manages 4-5 million IP addresses sinkhole per day across 400 different malware families and operates 2750 class C networks hosting honeypots and spampots:

- In their data center, Shadowserver runs 1,115,000 unique malware samples through sandboxes daily and has accumulated over 1.8 billion[M1] [LA2] samples in its malware repository. The organization stores 12 petabytes of malware and threat intelligence, growing at a rate of more than 1 petabyte per year. Additionally, it has indexed and made searchable 70 billion SSL certificates.
- Shadowserver's efforts extend to repackaging this information into free reports sent to 7,000 network owners and 201 National CSIRTs in 175 countries and territories. They also provide significant behind-the-scenes support for law enforcement operations, offering visibility of criminal infrastructure and advice on building cases.
- Their website offers a dashboard (dashboard.shadowserver.org) as a free resource to understand the data Shadowserver holds. Notable case studies include the Progress MOVEit CVE-2023-34362, where they created a honeypot profile, identified over 5000 entities looking for an exploit, and added device detection to their daily scanning.
- Another notable case is the Foundation's support to the FBI during the Qakbot Takedown. Special reports produced by Shadowserver were used to disseminate information about historic infections and compromised addresses, helping to identify over 700,000 infected addresses, some of which dated back to mid-June 2019.

Building bridges: ICANN, the incident response community and law enforcement

During the IGCC, Mr. Carlos Alvarez presented on **the Internet Corporation for Assigned Names and Numbers (ICANN),** an American multistakeholder group which plays an important role in maintaining the stability and security of the internet. ICANN's work is fundamental in the management of the global Domain Name System (DNS). It oversees policy development for the internationalization of the DNS, the introduction of new generic top-level domains (TLDs), and the operation of root name servers. In addition to managing the DNS, ICANN is in charge of the Internet Protocol address spaces for IPv4 and IPv6 and assigns address blocks to regional Internet registries. It also maintains registries of Internet Protocol identifiers.

- A key aspect of ICANN's role is performing the technical maintenance work of the Central Internet Address pools and DNS root zone registries. This is part of its function under the Internet Assigned Numbers Authority (IANA) contract. The stewardship contract between ICANN and the National Telecommunications and Information Administration (NTIA) of the United States Department of Commerce, which formalized this role, ended on October 1, 2016, transitioning the functions to the global multistakeholder community.
- ICANN's primary principles revolve around ensuring the operational stability of the Internet, promoting competition, achieving broad representation of the global Internet community, and developing policies through bottom-up, consensus-based processes. Its motto, "One World. One Internet," reflects its commitment to these principles.

Participants were also provided with an overview of **the Forum of Incident Response and Security Teams (FIRST)**, its role and how it can support law enforcement against cybercrime:

- Meanwhile, **the Forum of Incident Response and Security Teams (FIRST)** brings together incident responders such as CERTs, CSIRTs, and PSIRTs. Established in 1990, FIRST enables incident responders to collaborate, develop a shared understanding of security problems, and work in an environment conducive to their roles. FIRST aims to unite incident response and security teams from every country to ensure a safe internet for all, with a membership of 688 teams and over 5,000 responders in 106 countries.
- FIRST supports the building of cybersecurity communities, helps CSIRTs gain maturity, and provides a roadmap and guide for expanding capabilities. It delivers training in partnership with others and at events, convenes Special

Interest Groups around topics of common interest, and shares its vision of a strong incident response community with partners globally.

- FIRST aspires to unite incident response and security teams from every country to ensure a safe internet for all. This global coordination is essential to ensure that incident responders around the world can communicate effectively and understand each other's intents and methods. FIRST has a widespread reach, with a membership of 688 teams consisting of over 5,000 incident responders in 106 countries.
- To build cybersecurity communities, FIRST supports CSIRTs in gaining maturity and liaising with relevant stakeholders. It maintains a CSIRT and PSIRT Services Framework, which details services typically offered by CSIRTs and provides a roadmap and guide for expanding their capabilities. FIRST also develops training materials for individual services, which are Creative Commons licensed and available for free. Additionally, FIRST delivers training through partnerships and at various events, utilizing a roster of trainer-practitioners.
- FIRST organizes Special Interest Groups (SIGs) to convene members around topics of common interest, often with a formal charter, timeline, and deliverables. These SIGs include various working groups and standards groups focused on different aspects of cybersecurity, such as academic security, automation, big data, cyber threat intelligence, DNS abuse, and vulnerability coordination. They also have discussion groups on topics like metrics and industrial control systems (ICS).

PANEL DISCUSSION: The Cybercrime Atlas Initiative and the potential of Public Private Partnerships for the Detection of Cybercrime

The final segment of block two featured a prime example of building communities to enhance the detection of cybercrime: **the Cybercrime Atlas initiative.** This initiative was introduced through **the World Economic Forum** in June 2022, with the primary objective of mapping and documenting the activities of cybercriminals, establishing a comprehensive database that can be harnessed by global law enforcement agencies to disrupt cybercrime networks. The Atlas initiative plays a crucial role in bridging the gap between different sectors involved in cybercrime detection as it acts as a centralized platform, gathering and disseminating information, and streamlining the process of identifying and addressing cyber threats. Main takeaways of the discussions included:

- **An emphasis on the need for a holistic approach in dealing with cybercrime**. This approach should involve **not only technological solutions but also policy**

changes and strategic collaborations. Atlas hopes to serve as a catalyst in this in this process, facilitating dialogue and action across different domains.

- **A major focus of the initiative is on building a trust-based environment.** Trust is seen as the cornerstone for effective collaboration among law enforcement, the private sector, and other relevant entities. The Atlas initiative is designed to foster this trust by providing a reliable and transparent mechanism for sharing information and resources.
- The panel also highlighted **the importance of open-source intelligence as a foundational tool.** By leveraging publicly available data, the Atlas aims to create a comprehensive understanding of the cybercrime landscape, which is crucial for proactive detection and prevention measures.
- The panel touched on **the challenges and opportunities in prioritizing efforts against cybercrime**. With the vast array of potential threats, the Atlas aims to identify and focus on key areas that require immediate attention, thereby optimizing resource allocation and response strategies.
- In discussing the future direction and sustainability of the initiative, it was noted that **ongoing engagement and participation from all sectors are essential**. The Atlas is envisioned as a dynamic platform that evolves with the changing landscape of cyber threats, requiring continuous input and collaboration from its stakeholders.
- Lastly, the panel underscored **the significance of having a unified platform** like the Atlas. It was recognized as a vital step towards not just reacting to cyber threats, but **proactively shaping a more secure cyber environment** through collective effort and shared expertise.

During the panel, several practical examples of the implementation of the Atlas initiative were mentioned, for instance in relation to **the INTERPOL-led operation called Africa Cyber Surge** – and how this is supporting the creation of a learning and forward-looking aspect of multi-stakeholders collaboration. **Within this context, INTERPOL was highlighted as a point of contact for law enforcement to engage with the Cybercrime Atlas initiative.**

KEY TAKEAWAYS

1. COMMUNITIES ARE CRUCIAL TO EFFECTIVELY DETECT CYBER THREATS.

- Effective cybercrime detection relies heavily on the formation of collaboration networks, or so-called "communities". These networks encompass law enforcement, cybersecurity experts, private sector stakeholders, and other relevant entities.
- Networks can only work in a trust-based environment and via trust-enabler organizations and initiatives that represent a neutral ground for collaboration amongst stakeholders that might have different interests at stake.
- The same networks need to be and remain agile and flexible to be able to effectively detect changing landscape of cyber threats.

2. PRIORITIZATION AND ALIGNMENT ARE KEY.

- Identifying and focusing on key areas of cyber threats is necessary for optimizing resource allocation and response strategies. This prioritization helps in effectively detecting the most pressing cybercrime challenges.
- Efforts in cybercrime detection should aim for global reach and inclusivity, ensuring that diverse perspectives and capabilities are incorporated – and should refrain from repeating instruments and procedures that are already in place.

3. IN A RAPIDLY EVOLVING LANDSCAPE, TECHNOLOGY CAN GIVE AN EDGE TO DETECTION.

- The use of advanced technologies, particularly those capable of analyzing complex data sets like those found in the Dark Web, is vital as these technologies help in identifying and classifying cyber threats.
- A thorough and wide-ranging approach to internet monitoring is essential. This includes scanning a vast range of IP addresses and analyzing malware samples to gain a comprehensive understanding of the cyber threat landscape.
- Leveraging publicly available data, or open-source intelligence, should not underestimated as it can contribute to creating a detailed understanding of the cybercrime landscape.

ACTIONS FOR INTERPOL

- INTERPOL will continue to act as a neutral interlocker between the public and private sectors, initiating and strengthening cooperation to ensure a more accurate and efficient sharing of information and intelligence and drive the proactive detection of cybercrime worldwide.
- INTERPOL will pursue its collaboration with initiatives such as the Cybercrime Atlas and work closely with relevant stakeholders, through joint activities, strategic alignment and policy formulation to enhance the global detection of cybercrime.
- INTERPOL will remain committed to promoting the role of key stakeholders that make the cyberspace a safer place, including those specialized in supporting technological advancement for a facilitated detection of cybercrime.

KEY TAKEAWAYS OF THE MAIN CONFERENCE

Block 3: Investigation

BLOCK 3: INVESTIGATION

Introduction

Successful cybercrime investigations typically involve strong partnerships between law enforcement, cybersecurity professionals, and the private sector. Indeed, unlike traditional crime scenes, cybercrime investigations often lack physical evidence such as blood spots or bullet casings, and there are seldom witnesses to interview. These unique challenges mean that cybercrime investigations often need specialized expertise, advanced techniques, and state-of-the-art tools. Additionally, these investigations frequently cross international borders, involving victims, perpetrators, and infrastructures spread across different countries. This global aspect necessitates a coordinated and collaborative approach to search, seize, and analyze both physical and digital evidence, as well as to execute judicial authorizations like warrants.

To explore the opportunities and challenges that public-private partnerships present in the realm of cybercrime investigations at the national, regional and international level, the third block of the IGCC included presentations by two speakers, each showcasing different cybercrime investigative measures, as well as how they approached the challenge of building communities to protect communities to successfully implement them:

Ms. Suzanne GRIMMER, Senior Manager, TICAT - Incident Management and Operational Support, National Cyber Crime Unit, National Crime Agency, United Kingdom.

Ms. Jacky FOX, Senior Managing Director and Europe Lead, Accenture Security.

Following these two presentations, the final item under block 3 was a panel discussion, on the topic of "Partnership Collaboration in Cybercrime Investigation", with contributions from:

Ms. Vesta MATVEEVA, Head of High-Tech Crime Investigation Department, APAC, Group-IB.

Ms. Lauren MISSLER, Regional Specialized Officer, African Joint Operation against Cybercrime (AFJOC), INTERPOL.

Ms. Beatriz SILVEIRA, Former INTERPOL Cybercrime Intelligence Officer.

How the United Kingdom's National Crime Agency (NCA) triages, coordinates and tasks cyber incidents – Impacting investigation, data mitigation risks and of course the victim.

A representative from **the United Kingdom (UK)'s National Crime Agency (NCA)** delivered a presentation on the comprehensive strategies and methodologies used by the country's **National Cyber Crime Unit (NCCU)** and its associated networks in managing cyber incidents. The presentation outlined the NCCU's approach, which encompasses four critical strategies: **Pursue, Prepare, Prevent, and Protect**. This comprehensive approach involves proactive and reactive investigations, technology and skills development, disrupting potential cybercriminal activities, and mitigating cyber threats at scale.

- Central to the NCCU's operation is **the Triage Incident Coordination and Tasking (TICAT) system**, which serves as the primary entry point into the NCCU and the Regional Organized Crime Unit network. TICAT's primary objectives include minimizing the impact of severe cyber incidents on the UK and its citizens, providing effective support for victims, identifying perpetrators for criminal justice outcomes, and issuing protect notifications to prevent future cybercrimes.
- Handling a high volume of cyber incidents and intelligence reports monthly, **TICAT's efficiency hinges on its partnerships with agencies such as the National Fraud Intelligence Bureau (NFIB) and the National Cyber Security Centre (NCSC)**. These collaborations are vital to managing demand, through joint triage.
- In its pursuit strategy, TICAT assesses threat, harm, and risk, offers victim support, focuses on data mitigation, and aims to maximize viable lines of enquiry. It also plays a crucial role in sharing intelligence and leading the UK's response to cyber threats. Meanwhile, in its protect strategy, TICAT deals with sensitive and fast-time intelligence, deconflicts and assesses threats, and provides urgent outreach and support to victims. This includes advising on how to protect companies, reporting unauthorized access, and capturing evidence.
- The presentation concluded by highlighting **the real-world impact of cyber incidents,** noting significant risks to councils, the education sector, small and medium businesses, charities, and the legal sector. The compromise of personal identifiable information can lead to a range of further criminal activities, thereby underscoring the duty to protect communities from such threats.

Accenture Security: A private sector's perspective on the Irish Healthcare System Cyberattack

A representative from Accenture presented a private sector perspective and an in-depth analysis of **the Conti Ransomware attack on the Health Service Executive (HSE) in Ireland.** The presentation detailed the timeline and impact of the attack, emphasizing the challenges and responses during the incident.

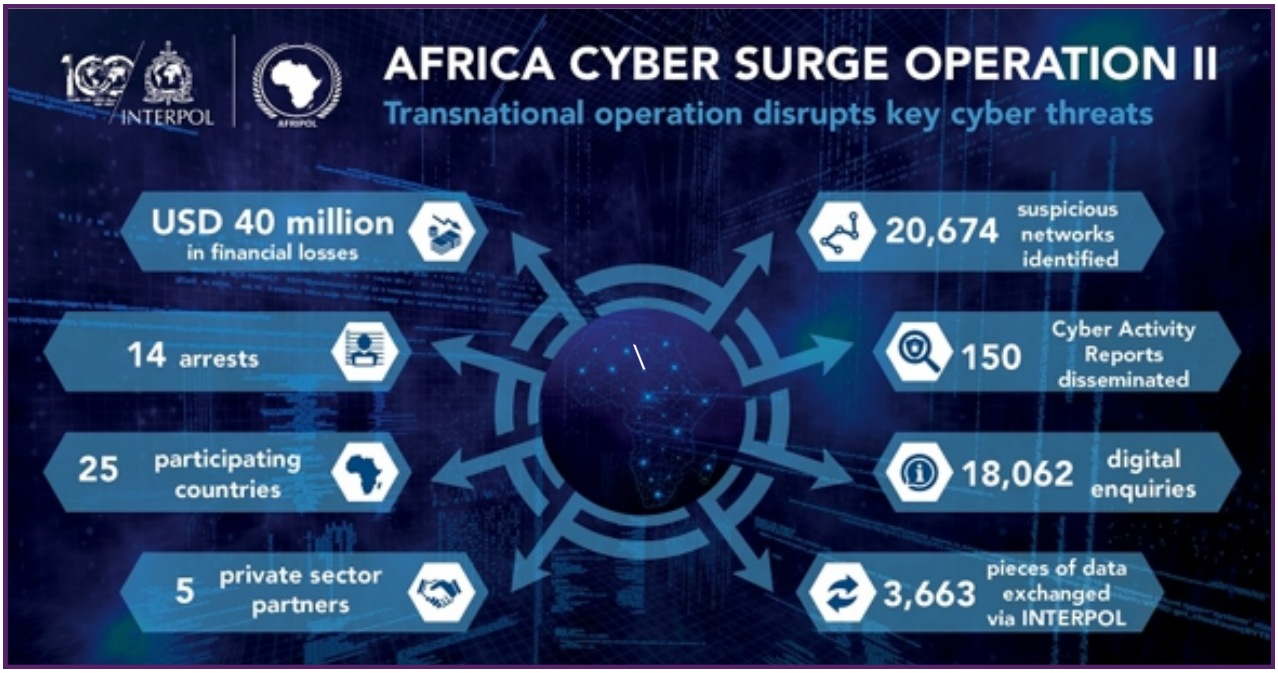
- The Conti malware, first identified in December 2019, is a C++ written ransomware primarily targeting local file encryption. The malware, linked to the group Wizard Spider, has targeted key industries including finance, health, manufacturing, and technology.
- The timeline of the HSE attack began on 18 March 2021 with the initial infection of Patient Zero's workstation, escalating in May 2021 when the attacker compromised several hospitals and executed the ransomware within the HSE. During this period, various hospitals identified and reported malicious activity, and the HSE's antivirus security provider flagged unhandled threat events.
- As the scale of the attack escalated, the HSE set up a war room on 15 May 2021 and reported the breach to the Data Protection Commission (DPC). They also obtained a court order to restrain the sharing of HSE data.By 24 May, a process for the secure recovery of systems was released. The decryption key was received on 21st May 2021, and the HSE established a Situation Centre in Citywest. By mid-June, nearly half of the servers were decrypted, and more than half of the applications were restored. In a significant development, 100% of the servers were considered decrypted by 21st September 2021, with approximately 99% of applications restored.
- Despite this success, the HSE faced various challenges during the recovery process. This included difficulties in gathering and maintaining up-to-date information about applications, heavy reliance on specific individuals prolonging the recovery timeline, and a lack of clear decision-making authority during the crisis. Additionally, there was insufficient IT support from the Office of the Chief Information Officer (OCIO) and limited ability for the HSE to investigate the attack.
- Several key lessons learned from the incident were shared with participants. Amongst them, the representative highlighted **the importance of understanding the reliance on technology; the need for effective cybersecurity strategy and leadership;** and **having ransomware-specific assessments, simulated attack tests, and robust cybersecurity monitoring and**

response mechanisms. The incident underscored the significant impact of community collaboration in responding to and recovering from cyber-attacks.

PANEL DISCUSSION: Partnership and collaboration in cybercrime investigations

In the panel dedicated to **"Partnership and collaboration in cybercrime investigations"**, experts delved into the intricacies of investigations, with a particular focus on the African region. The rapid growth of internet and mobile banking services in Africa has led to a surge in cyber threats like digital extortion, ransomware, online scams, and business email compromises. The discussion highlighted the challenges and solutions in combatting these cyber threats, **including recent activities coordinated by INTERPOL in the African region**. Key points from the discussion include:

- **The INTERPOL African Joint Operations against Cybercrime (AFJOC)** has seen significant changes in the last two years, particularly in its collaboration and coordination efforts. **The INTERPOL Africa Cyber Surge operations I & II** exemplify this, enhanced collaboration, especially with local CERTs, which resulted in a higher number of infrastructure takedowns.
- Panelists highlighted **the impressive growth of cyber maturity in Africa.** More countries are seeking assistance from INTERPOL, highlighting the importance of continuous needs and capabilities assessments.



- **INTERPOL's private sector partners** like Group-IB played a pivotal role during the second Africa Surge operation, focusing on identifying misconfigurations and threat actors to aid law enforcement. They provided threat intelligence and sped up the investigation process through attribution efforts.
- Relatedly, one panelist shared how the transition from the public to private sector brings a change in perspective regarding cybercrime investigations. In the private sector, the approach is more about bringing different communities together, building trust, and sharing indicators across various sectors. Meanwhile, the private sector can benefit from hiring investigators with law enforcement backgrounds due to their extensive training and established community relations.
- The discussion also touched upon **global policy perspectives on ransom payment** in the context of cyber-attacks, with some emphasizing the importance of not paying ransoms to cybercriminal groups to avoid setting a precedent.
- Panelists also discussed how when data is exfiltrated and published, assessing its sensitivity becomes crucial, especially when it involves legal entities and could pose risks to individuals' lives.
- In closing the panel, INTERPOL re-iterated its commitment to **linking training and capacity-building to operational outcomes.** However, maintaining **sustainability, especially in terms of funding**, were highlighted as enduring challenges.

KEY TAKEAWAYS

1. PARTNERSHIPS ACROSS SECTORS AND BORDERS CAN HELP ADDRESS THE COMPLEX NATURE OF CYBERCRIME INVESTIGATIONS.

- Cybercrime investigations are uniquely challenging due to the absence of physical evidence and witnesses, coupled with the potential for suspects to operate across international borders. This necessitates a range of specialized expertise, advanced investigative techniques, and cutting-edge tools.
- *Effective cyber investigations must involve cross-border collaboration* for the search, seizure, and analysis of both physical and digital evidence, along with the execution of legal authorizations like warrants.
- National strategies are far away from being mere documents. They can empower or limit cyber investigations at the national, regional, and international level. These strategies include the ones to deal with specific circumstances such as ransomware payments.

2. THERE IS A NEED TO TACKLE ENDURING CHALLENGES IN CYBER CAPACITY BUILDING AND FUNDING.

- Cyber capacity building and training remain a top priority at the international level, as many countries are face significant challenges in investigating cybercrime. However, the capacity building and training landscape can sometimes be confusing and scattered, with some public and private entities having similar offers.
- INTERPOL designs its technical assistance and capacity building specifically to address the needs of law enforcement, for instance by linking training activities with operational outcomes.
- Sustaining effective cybercrime investigation initiatives, particularly in terms of funding and capacity building, will likely remain a challenge in the near future, emphasizing the need for ongoing support and resources.

ACTIONS FOR INTERPOL

- INTERPOL will continue to enable international and multistakeholder collaboration, foster information exchange and provide operational support to assist member countries with their cybercrime investigations.

- INTERPOL will pursue its current strategy of linking capacity building and training to operational activities, to ensure that newly acquired knowledge can be beneficial to investigations and eventually lead to the reduction of cybercrime worldwide.

- INTERPOL will actively engage in various international fora that are leading policy and strategic changes in the realm of cybercrime and cybersecurity, to reflect the global law enforcement perspective and its needs in terms of cybercrime investigations. These fora include, but are not limited to:
  - The United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes; and
  - the Open-ended Intergovernmental Expert Group to Conduct a Comprehensive Study of the Problem of Cybercrime.

KEY TAKEAWAYS OF THE MAIN CONFERENCE

Block 4: Disruption

BLOCK 4: DISRUPTION

Introduction

The aim of criminal investigations is to apprehend suspects and bring them to justice. However, this can sometimes prove to be challenging in the context of cybercrime, as investigations are typically lengthy, and suspects may be located in uncooperative jurisdictions. Thankfully, there is a range of actions that can be taken to disrupt cybercriminals and make a real impact besides only arrests, from seizing websites and taking down malicious infrastructure to developing decryption keys and making them available to victims. Accordingly**, the focus of Block 4, entitled "Disruption", was not only "arrests" or "convictions", but also the various interventions that can be taken to effectively hinder and disrupt criminal activity.** Proactive disruption measures can help prevent further attacks, reduce victimization, and minimize harm. However, once again, law enforcement cannot do it on its own. To effectively disrupt cybercrime, we need to build communities with actors across different sectors and borders.

Block 4 exposed participants to different successful measures aimed at disrupting cybercrime, from effective operations to the disruption of ransomware payments and legislative changes, highlighting the importance of multistakeholder collaboration for these efforts to be successful. The Block featured four speakers:

Mr. Carsten MEYWIRTH, Director of Cybercrime Division, Federal Criminal Police Office (BKA), Germany.

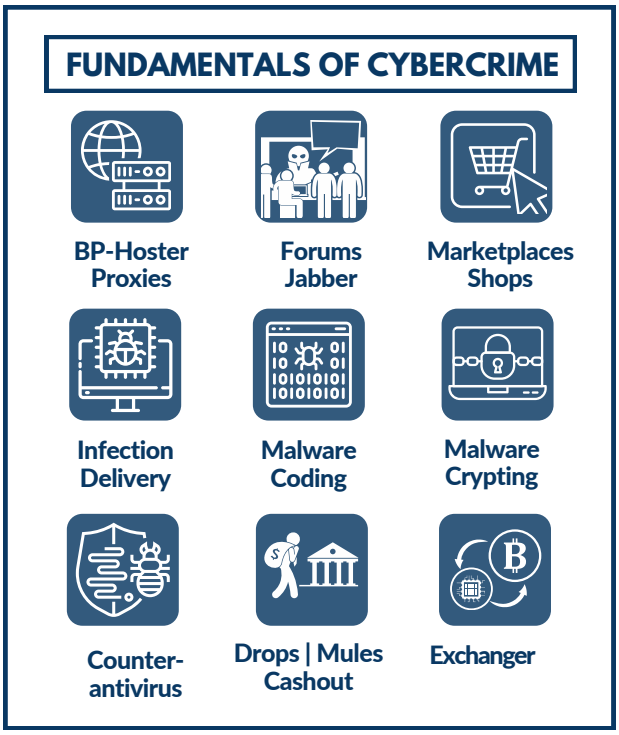
Mr. Enrique HERNANDEZ GONZALEZ, Head of Operations in the INTERPOL Cybercrime Directorate.

Mr. Philip REINER, CEO, Institute for Security and Technology (IST).

Mr. Christopher ONG, Deputy Chief Prosecutor, Attorney-General's Chambers, Singapore.

Counter-cyber operations against high value targets – Situation overview from the German BKA

Block 4 started with a law enforcement perspective in disrupting cybercrime, delivered by a representative from the German Bundeskriminalamt (German Federal Police or BKA for short).



- The presentation emphasized the importance of **understanding the fundamentals of cybercriminal activity** (cf. image on the right) in order to effectively disrupt it.
- Indeed, cybercriminal activities can involve a range of actors that are skilled, organized, worldwide, merciless and connected. Likewise, law enforcement needs to strive to be solution oriented, agile, creative, globally connected and constantly learning.
- In addition, the presentation highlighted four successful disruptions of cybercrime in which the BKA has been involved recently:

EMOTET	• Prime example of "Malware as a Service" • Global computer system infection • Pilot project for Central Investigation & Infrastructure strategy
HYDRA MARKET	• Darknet marketplace for narcotics with the highest revenue • 17 Mio customer and 19.000 accounts • Confiscation of infrastructure located in Germany
CHIPMIXER	• "Mixing-as-a-Service" with the world's highest profit • Securing and changing the cash flow from incriminated wallets • Seizure of the Bitcoins (worth 90 Mio. €)
QAKBOT	• Malicious programme which was designed to deliver other malware to a victims computer (i.e. dropper) • Infrastructure in USA, NI, FR and GER • Destroying the infrastructure of Qakbot

- Reflecting on these successes, it was emphasized that when it comes to cybercrime, l**aw enforcement should not only focus on arrests but also aim to takedown infrastructure and confiscate the proceeds of crime**.
- The presentation also highlighted **the importance of international cooperation in fighting the global scourge of cybercrime**. Law enforcement needs to collaborate with a wide range of law enforcement agencies and IT services at the national and international level.
- Last but not least, there is a need to organize the collection of data, to transform it into action and to share the resulting information with partners.

INTERPOL operational successes against cybercrime

In the next presentation, participants were presented with three recent INTERPOL operational successes in the disruption of cybercrime.

Operation Kingfisher

- One of the most recent operations of INTERPOL in the ASEAN region, Operation Kingfisher targeted the phishing-as-a-service platform known as "16shop". 16shop had sold hacking tools, which are estimated to have contributed to compromising more than 70,000 users in 43 countries.
- During the operation, the arrest of the administrator of 16shop was made possible thanks to the intensive intelligence-sharing between INTERPOL, Indonesia, Japan and the United States, as well as the support of INTERPOL's private sector partners Cyber Defense Institute, Group-IB, Palo Alto, and Trend Micro. This successful disruption highlights the critical importance of international cooperation and public-private partnerships.

To learn more about Operation Kingfisher, please see: https://www.interpol.int/en/News-and-Events/News/2023/Notorious-phishing-platform-shut-down-arrests-in-international-police-operation

Operation GoldDust

- Operation GoldDust was a four-year operation across five continents and 17 jurisdictions which resulted in the disruption of a ransomware cybercrime gang and the arrest of seven suspects believed to have caused billions of dollars of damage.
- INTERPOL, working with Europol, national law enforcement agencies in 17 countries and private sector partners like Trend Micro, S2W, Palo Alto

- Networks, Fortinet, CDI, Kaspersky, assisted countries in mitigating ransomware incidents, developed IOC (Indicator of Compromise), and analyzed malware samples to develop a global threat picture of GandCrab and REvil ransomware families and the suspects behind them. Participating countries involved Australia, Belgium, Canada, France, Germany, The Netherlands, Luxembourg, Norway, Philippines, Poland, Romania, South Korea, Sweden, Switzerland, Kuwait, the United Kingdom and The United States and Ukraine.

To learn more about the operation, please see: https://www.interpol.int/en/News-and-Events/News/2021/Joint-global-ransomware-operation-sees-arrests-and-criminal-network-dismantled

Operation Synergia

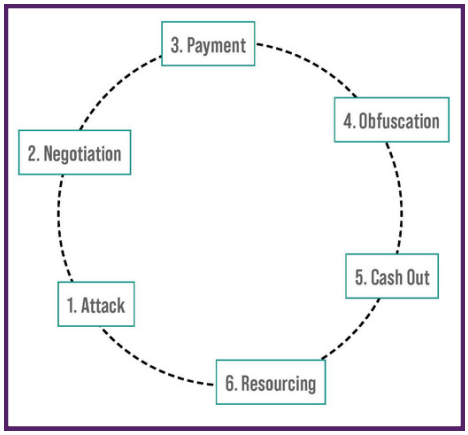
- The ongoing Operation Synergia targets cyberthreats which are high-harm, high-impact, high-volume and high-interest, targeting phishing, ransomware and banking malware infrastructure.
- To date, 53 countries and 4 private sector countries have participated, resulting in 210 cyber activities reports and the identification of over a thousand malicious servers.

Mapping the Ransomware Payment Ecosystem: IST's comprehensive depiction of the process and participants

The next presentation provided participants with a comprehensive walkthrough of the actors, stakeholders, processes, and information required for and produced during the ransomware payment process, based on work conducted by **the Institute for Security and Technology's (IST)** Ransomware Task Force:

- In 2021, the Institute for Security and Technology (IST), a think tank based in the United States, launched **the Ransomware Task Force (RTF)** to bring together over 60 experts from industry, government, law enforcement, civil society and international organizations in countering the threat of ransomware.
- One area of work of the RTF has been to illuminate the ransomware payment ecosystem, as part of IST's efforts to improve the information environment and blunt the ability for criminal and other malign actors to profit from ransomware attacks, and thereby stop engaging in ransomware for profit. The result of this effort was the publication of a report in Fall 2022 entitled **Mapping the Ransomware Payment Ecosystem.**

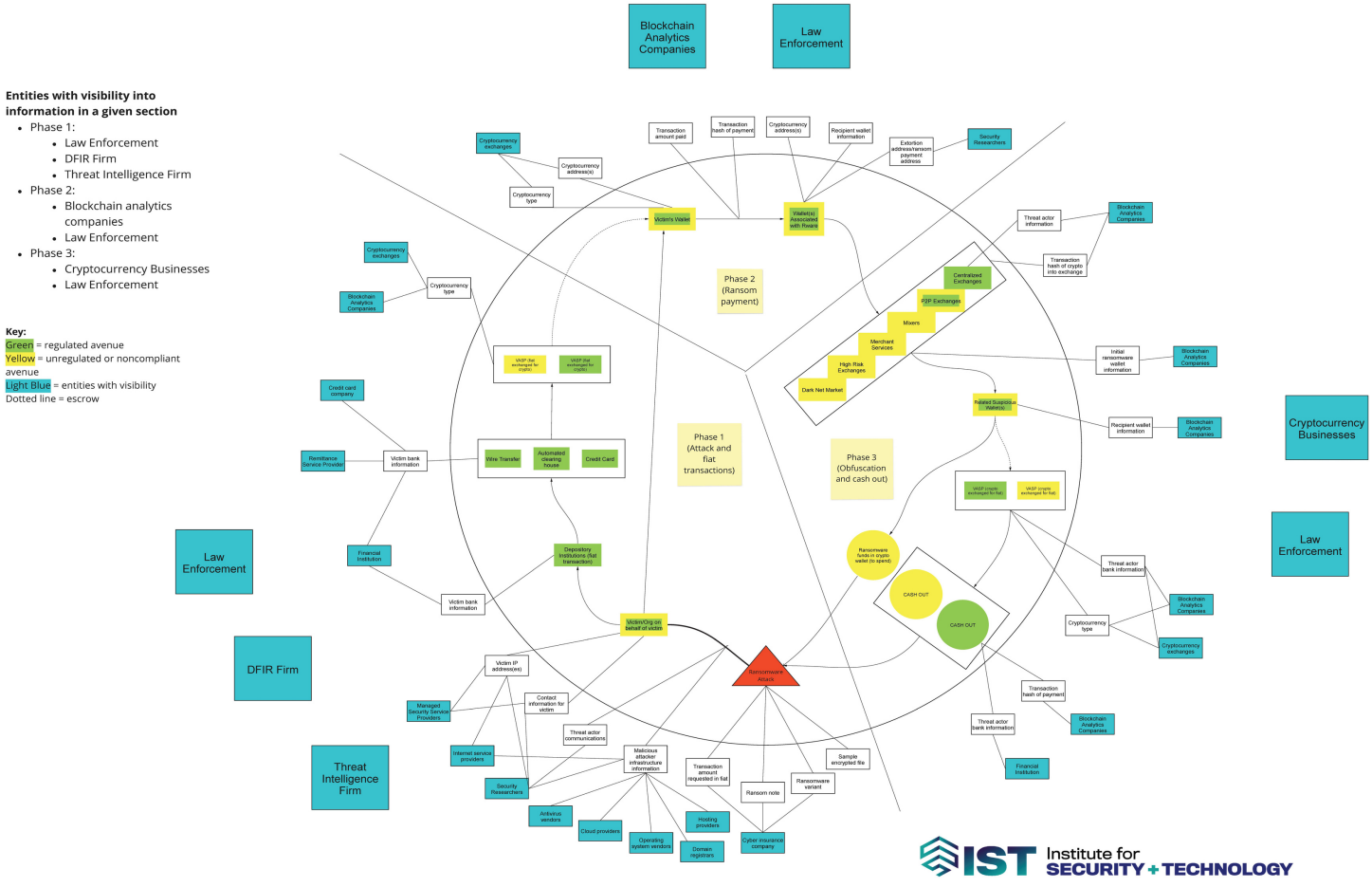
- The report breaks down the ransomware payment process into six main stages: (1) attack, (2) negotiation, (3) payment, (4) obfuscation, (5) cash out, and (6) resourcing. Using these six stages, the RTF developed a comprehensive visualization or "map" of the ransomware payment ecosystem, depicting the ransomware payment process from attack to cash out.



Six main stages of the ransomware payment according to IST. Source: https://securityandtechnology.org/wp-content/uploads/2022/11/Mapping-the-Ransomware-Payment-Ecosystem.pdf

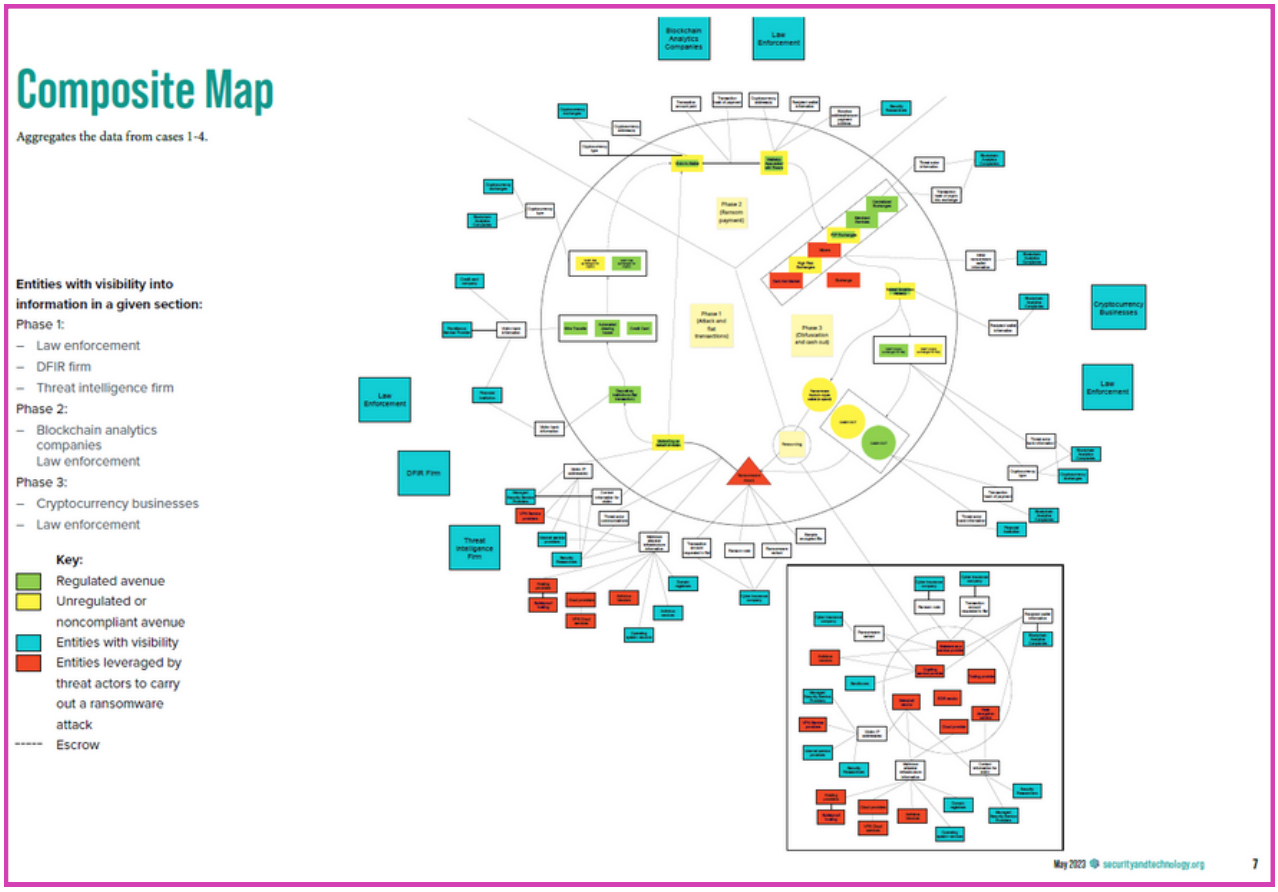
IST's report "Mapping the Ransomware Payment Ecosystem" is available online here: https://securityandtechnology.org/ransomwaretaskforce/

- In the figure below, the circle of white boxes identifies types of information produced along each point of the ransomware payment process, the second concentric circle of blue boxes depicts entities with potential access to these pieces of information.



To display the above image larger, please use the following link: https://securityandtechnology.org/wp-content/uploads/2022/11/Mapping-the-Ransomware-Payment-Ecosystem.pdf

- Ultimately, the aim of the mapping process is to empower relevant stakeholders to take actions to disincentivize threat actors from carrying out attacks. As an additional step, IST has conducted a mini-pilot, to test the map against four cases of ransomware attacks and look to identify which kinds of disruption could be the most effective.



One of the four cases discussed in the mini-pilot is displayed above. To view the image larger, please use the following link: https://securityandtechnology.org/virtual-library/reports/mapping-threat-actor-behavior-in-the-ransomware-payment-ecosystem-a-mini-pilot/

- As was explained during the presentation, by developing a clearer picture of the ransomware payment process, law enforcement officers can better collaborate with other entities to identify opportunities to intervene. They can pinpoint at what stage a particular incident is in the payment process, which can allow counter-ransomware efforts to disrupt that process.
- The mapping exercise also makes it easier identify which entities are involved in the process and who should be contacted during operations, either to gather information or coordinate action.

Approaches to Fighting Cyberscams: The Singapore Experience

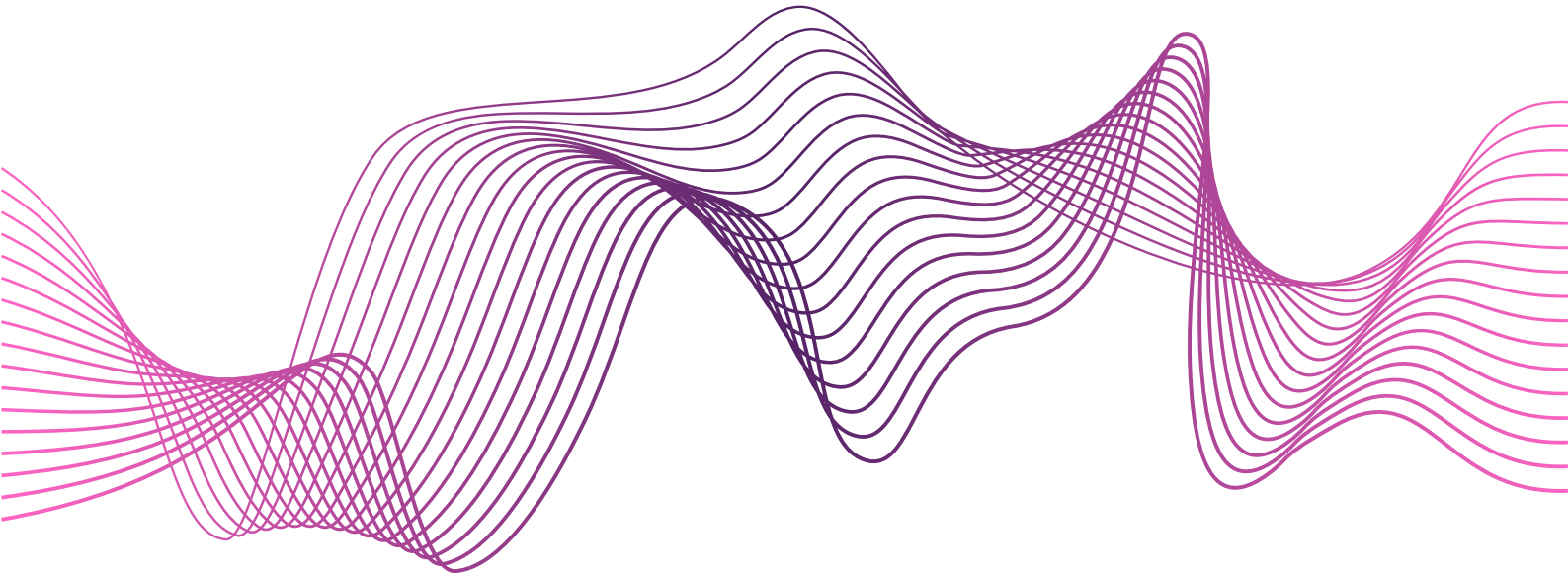
The final presentation of block 4 focused on Singapore's approach to disrupting online scams, sharing lessons learnt and best practices.

- **Since 2020, Singapore has experienced a dramatic growth in cyber scams**, as the COVID-19 pandemic and its aftermath increased the volume of online transactions. **Both the number of scams and the amount lost have more than doubled** (from 15,651 reported scams amounting to SGD 265.7 million in 2020 to 31,728 scams in 2022 amounting to SGD 660.7 million). Looking at the first half of 2023, the total number of scam cases has continued to increase rapidly (by 64.5 %), though the total amount reported to have been cheated decreased slightly by 2.2 % compared to the same period in the previous year.
- Worryingly, **the types of online scams have been evolving quickly,** with some of the most recent trends involving the use of malware, including malware-as-a-service, and young people being recruited as mules. Some of the most prolific forms of online scams in Singapore are displayed below:

Top 10 scams of concern in Singapore according to the Singapore Police Force.

- To respond to the growing threat of online scams, in March 2022 **the Singapore Police Force (SPF)** established a dedicated department known as **the Anti-Scam Command**. The aim of the Anti-Scam Command is to provide for greater coordination and speed in combating and disrupting scams. To achieve this objective, the Anti-Scam Command adopts a multi-pronged approach, featuring innovative public-private partnerships and international cooperation.

- This includes **the collocation of SPF officers with staff from selected banks and telecommunications companies** inside the Anti-Scam Centre, to promote faster collaboration. Thanks to this innovative approach, the Anti-Scam Command has enabled banks to freeze more than 50,000 accounts and recover over USD 360 million; telcos to terminate more than 15,000 lines and report over 67,800 WhatsApp accounts; and online marketplaces to remove over 9,000 suspicious accounts and advertisements.
- Recent efforts to disrupt cyberscams have brought to the fore **several legislative gaps**. One case involved scammers promising to purchase an individual's national online identification (SINGPASS) credentials. Though the individual never received the promised payment, the scammers still used their credentials to open bank accounts to launder money.
- The issue from a disruption perspective is that at the time there was no specific legislation governing the use or sale of such credentials in Singapore. Similarly, cases involving the sale of banking credentials to scammers, which were later used to conduct bank malware scams, exposed the lack of a clear position as to allowing others to use banking facilities, especially online.
- **In response, Singapore has developed new and amended legislation to address these gaps.** This includes the Computer Misuse (Amendment) Bill of 18 April 2023; the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) (Amendment) Bill of 18 April 2023 and the Online Criminal Harms Act of 5 July 2023. These legislative changes establish new offences, for instance targeting buying and selling of national digital identity or the selling and renting of bank accounts and empower authorities to issue directions if there is suspicion of malicious online activity.



KEY TAKEAWAYS

1. DON'T FOCUS ONLY ON THE ARRESTS OF SUSPECTS. ALSO DESTROY CRIMINALS' INFRASTRUCTURE AND TAKE THEIR MONEY.

- Besides apprehending suspects, the focus should be on dismantling and seizing their infrastructure and financial resources.

2. FIND PARTNERS WITH THE SAME MISSION. PUBLIC AND PRIVATE SECTOR PARTNERSHIPS ARE KEY, AS IS INTERNATIONAL COOPERATION.

- Both the public and private sectors have a mutual interest in fighting cybercrime. There is a need to think creatively about how to enhance the effectiveness of partnerships - as was done in the case of Singapore's Anti-Scam Command.
- It is important to collaborate with a range of public and private sector actors not just domestically but also at the international level. International cooperation was key to the operational successes discussed by representatives of INTERPOL and the German BKA.

3. ORGANIZE YOUR DATA COLLECTION AND TRANSFORM DATA INTO ACTION.

- Developing a clearer picture of threats and their modus operandi (including thinks like the ransomware payment process) can empower law enforcement to collaborate better with other entities and pinpoint more opportunities for disruption. A good example of this is the ransomware payments map developed by IST.
- Besides enabling the identification of weak links, detecting and recognizing trends in the way that criminals operate is critical to enable law enforcement authorities to work with relevant authorities to legislative close gaps and appropriately empower disruption efforts.

4. RELATEDLY, SHARE YOUR INFORMATION ENTIRELY WITH YOUR PARTNERS.

- INTERPOL can act as a trusted, neutral interlocker to facilitate the exchange of information and the development of a global picture to enable more effective disruption.

5. BE PREPARED TO KEEP FIGHTING. BE BRAVE AND TAKE RISKS.

- All the presentations demonstrated that cybercriminal activity is constantly evolving. Monitor the impact of AI and new technologies on cybercrime.
- Keep innovating.

ACTIONS FOR INTERPOL

- INTERPOL will continue to facilitate international cooperation, including through regional working groups, to promote the exchange of intelligence and the coordination of operations.
- Member countries are invited to make use of INTERPOL platforms and tools, including the INTERPOL Cyber Knowledge Exchange CCP-Operations platforms.
- INTERPOL will continue to offer opportunities for direct country to country cooperation at the global, regional and national level.

CONCLUSION

CONCLUSION

The INTERPOL Global Cybercrime Conference 2023 was a significant event, exemplifying a global commitment to combatting cybercrime. Under the theme "Creating Communities to Protect Communities," the conference showcased a collective resolve to strengthen the response against cybercrime across nations and sectors.

The event was marked by the **diverse participation** of leaders from law enforcement, academia, the private sector, and international organizations from all over the world. This wide-ranging representation underscored the universal nature and challenge of cybercrime, emphasizing the need for collaborative, cross-border solutions.

Key areas such as **prevention, detection, investigation, and disruption** were thoroughly explored, in agreement with the INTERPOL Global Cybercrime Strategy 2022-25. The discussions and presentations at the conference underscored the importance of innovative methods and best practices in tackling the complexities of cyber threats.

A recurring theme throughout the conference was the vital role of **public-private partnerships** in effective cybercrime management. This synergy highlighted the necessity for collaborative efforts across various sectors to develop robust cybersecurity measures. Additionally, the conference reinforced the concept that safeguarding against cybercrime is a shared responsibility, necessitating the active participation of all societal sectors.

The event also served as a foundation for **future international cooperation**, with initiatives like the Cybercrime Atlas and the International Cyber Offender Prevention Network (InterCOP) set to drive collaborative efforts forward.

In conclusion, the proactive and collective efforts discussed and initiated at this conference are significant steps towards a future where communities are better protected against the ever-changing landscape of cybercrime. INTERPOL stands ready to support these efforts, fostering global partnerships and driving innovative solutions to ensure a safer digital world.

About INTERPOL and the Global Cybercrime Programme

About INTERPOL

Today's crimes are interconnected and global. More than ever, there is a need for multilateral police cooperation to address the security challenges facing the world. INTERPOL's role is to enable police in our 196 member countries to work together to make the world a safer place.

We provide secure access to global databases of police information on criminals and crime, operational and forensic support, analysis services and training. Our colour-coded INTERPOL Notices are used to alert police worldwide to wanted persons, security threats and modus operandi.

All these policing capabilities are delivered worldwide and support four global programmes against the issues that we consider to be the most pressing today: cybercrime; counter-terrorism; organized and emerging crime; and financial crime and anti-corruption.

The INTERPOL General Secretariat is based in Lyon, France, supported by the INTERPOL Global Complex for Innovation in Singapore, six regional bureaus, three liaison offices, as well as special representative offices at the African Union, the European Union and the United Nations.

Each member country runs an INTERPOL National Central Bureau, staffed by national law enforcement officials, which connects them and their frontline officers to our global network.

About the INTERPOL Cybercrime Programme

In a dynamic digital age, where over half the global population is at potential risk from cybercrime, the **INTERPOL Global Cybercrime Programme** stands in support of the international law enforcement community. We are dedicated to developing and leading a global response to prevent, detect, investigate and disrupt cybercrime – with the ultimate mandate to reduce its global impact and protect communities for a safer world.

The **INTERPOL Global Cybercrime Strategy** focuses on four main objectives:

1. Enable a proactive and agile posture in the prevention and disruption of cybercrime by developing an in-depth understanding of the cybercrime threat landscape through information sharing and intelligence analysis.
2. Effectively prevent, detect, investigate and disrupt cybercrime that causes a significant harm on a national, regional and global scale by leading, coordinating and supporting member countries in transnational operational activities.
3. Support the development of strategies and capabilities of member countries in combating cybercrime by cultivating open, inclusive and diverse partnerships and building trust in the global cybersecurity ecosystem.
4. Promote INTERPOL's role and capabilities in shaping global security by engaging with international forums in the field of cybercrime.

We implement our Strategy and objectives via a simple and constructive delivery model, which consists of three core pillars:

- **Cybercrime Threat Response**: Addressing immediate and emerging cyber threats with a rapid and coordinated response.
- **Cybercrime Operations**: Implementing a regionally-focused operational strategy to combat cybercrime effectively.
- **Cyber Capabilities Development:** Enhancing strategies and capabilities through innovative projects and platforms.

Underpinning these pillars is our extensive public-private partnership, fostering collaboration and leveraging collective expertise to fight cybercrime.

For any further information, you are encouraged to contact us at the following email address: **EDPS-CD@interpol.int**.

INTERPOL

INTERPOL appreciates any feedback regarding the 2023 INTERPOL Global Cybercrime Conference and this report. Please provide comments by email at:
CYBERCONF@interpol.int