WORLD ECONOMIC FORUM

Disrupting Cybercrime Networks: A Collaboration Framework

WHITE PAPER

NOVEMBER 2024

Images: Getty Images

Contents

Disclaimer
This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Executive summary

Collaborations between industry experts and the public sector are disrupting cybercriminals. Here's how this can be scaled up and accelerated.

The internet allows criminals to operate seamlessly across borders, accessing a marketplace of victims anywhere, anytime and at scale. Cybercrime has expanded for the same reasons that drove the mega growth of legal online businesses.

At the same time, criminals copy what they see in the legal markets. Think about the advent of subscription model "software-as-a-service" offerings that give businesses access to user-friendly products ranging from video calls to project management and customer service tools. Equally, criminals have their own "cybercrime-as-a-service"[1] business model where experienced cybercriminals sell accessible tools and knowledge to help others carry out cybercrimes. This brings more criminals into the cybercrime market by lowering the cost and level of skill needed to be an effective online fraudster and deliver ransomware attacks that can bankrupt businesses[2] and destroy livelihoods.

The Global Anti-Scam Alliance estimated that 25.5% of the world's population were impacted by cyber-enabled fraud in 2023.[3] The profits this generates for criminals have a wider impact than the immediate victims. In 2023, the United Nations reported that at least 220,000 people had been trafficked in South-East Asia, some from as far away as Africa and Latin America, and forced to run online scams.[4]

The convergence of cybercrime and violent organized crime has also led to a cultural shift, with the new entrants to the cybercrime market less concerned about causing physical harm at scale. For example, in June 2024, a ransomware attack on a blood-test provider prompted the United Kingdom's National Health Service to make an urgent call for blood donations[5] and rearrange more than 800 planned operations after they lost the service's ability to match patients' blood.[6]

New ground being broken in the fight against cybercriminals

Often, responses to cybercrime have been fragmented. Existing knowledge of cybercriminal activity, while often deep, has been split across different companies and public agencies. But there are an increasing number of examples where these limitations are overcome. In 2024, law enforcement in Thailand and the Philippines successfully rescued hundreds of people from forced labour in cyber-scam farms and worked with the private sector to recover criminal profits. In West Africa and Latin America, operations supported by INTERPOL have led to coordinated arrests.[7] In Europe and North America, collaborations between industry and law enforcement[8] have led to unprecedented success in the disruption of cybercriminals' technical infrastructure,[9] creating new levels of risk for cybercrime service providers and the criminals who use them.

The expanding list of successful disruptions is heartening and the result of several years of hard work and good-faith partnerships between industry and the public sector. The aim is to have a systematic disruptive impact on cybercrime and the path towards it is clear. It is also clear that industry partnerships, as well as collaborations between industry and the public sector, will be a driving force in making the internet a hostile environment for cybercriminals.

Operational collaboration framework

This white paper, developed by the World Economic Forum's Partnership against Cybercrime community, asks how to build on the success of the anti-cybercrime partnerships that already exist. It identifies some of the leading operational collaborations to counter cybercriminal networks and infrastructure and draws on the expertise of the Partnership against Cybercrime community to identify common characteristics of successful partnerships and the challenges they face. It then provides recommendations for setting up, maintaining and accelerating the success of anti-cybercrime partnerships. This is the starting point for a framework for anti-cybercrime operational collaborations.

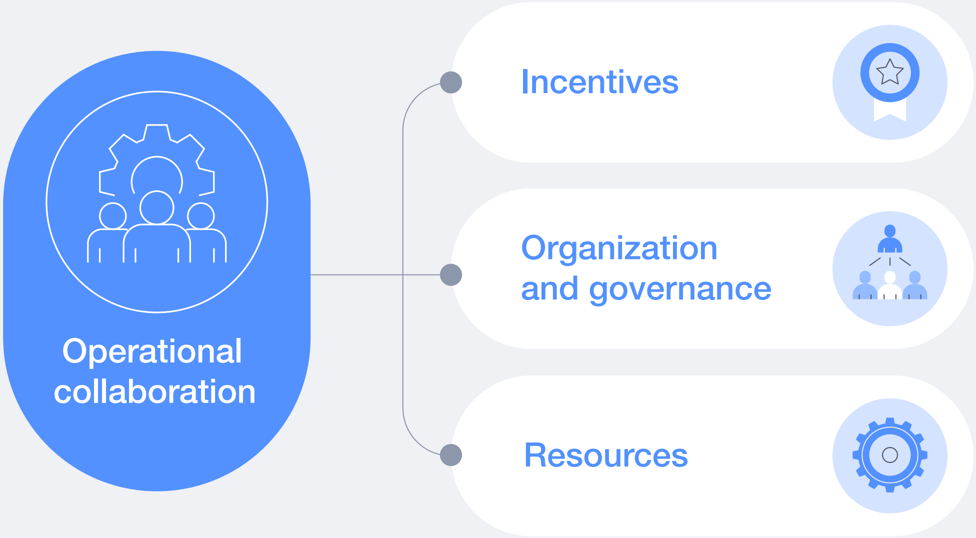
1

Collaborating to disrupt cybercrime

Understanding the "why" and "how" of operational collaboration.

Successful operational collaborations to counter cybercrime incentivize participants' alignment around a shared mission and over time. These partnerships have organizational processes and governance adapted to the requirements of their activities, and show an ability to reassess and restructure how they collaborate as needs change. Importantly, these collaborations understand how to link technology and skilled cybercrime professionals with legal and policy experts.

FIGURE 1 **Operational collaboration: Three main pillars**



Source: World Economic Forum.

Incentives for collaboration

Successful operational collaborations to counter cybercrime demonstrate:

- **A clear mission:** This provides participants with an ongoing justification for joining and remaining part of the collaboration.

- **Impact:** Frequent feedback to individuals, participating organizations and external stakeholders shows how their input to a collaboration has created impact.

- **Peer-to-peer learning:** Successful operational collaborations are sites of ongoing learning for the experts engaged in operations. They also provide skills, information and assessments that help participating organizations to improve their internal cybersecurity capacity. Formal training programmes also support the creation of communities of trust that help maintain the collaboration over time.

- **Public recognition:** Support can be used to show that an organization is using its capabilities to support society by reducing criminal harms. This reputational support provides an additional business incentive to engage.

- **Cyber-resilience as a value creator:** Information obtained from a collaboration can be used to improve cyber defences and post-attack recovery.

By aligning on definitions of cybercriminal activity, taxonomies enable faster identification and categorization of threats, which supports an effective operational response.

Organization and governance

- **Flexible governance frameworks:** The governance structure of the collaboration is designed to support stringent control over sensitive areas such as data management and use, through legal contracts, where necessary. At the same time, there is flexibility in how experts from sometimes vastly different types of organizations interact and proceed with an operation. Operational interaction is often governed by standard operating procedures and codes of conduct that are developed by the expert community itself.

- **Membership capability assessments:** Participants in a collaboration are sought based on the capabilities they bring. Participants understand what they are obliged to provide to the collaboration in order to retain membership. The collaboration has ways of measuring engagement and the value provided by each member.

Resources and expertise

- **Technology and people are interlinked:** The success of technology and IT platforms is dependent on having the technical, legal and operational expertise to use them.

- **Taxonomies and data normalization:** There is strength in the diversity of skills created by a cross-industry or public-private partnership but there can also be confusion. Taxonomies create a common language that facilitates clear communication across participants. By aligning on definitions of cybercriminal activity, taxonomies enable faster identification and categorization of threats, which in turn supports an effective operational response.

- **Data management and information security:** Ensuring that information is securely stored, properly classified and easily retrievable is critical to taking a collaboration out of its start-up phase and ensuring that it can grow.

2 A roadmap for collaboration

Strengthening defenses and increasing the costs for cybercriminals.

2.1 Incentives

Cybercriminal groups have evolved into highly lucrative transnational enterprises linked by complicated networks of commercial relationships and supply chains. This allows cybercriminals to operate at scale but also creates opportunities to make cybercrime less attractive through disruption and arrest, significantly altering the risk-reward calculus for perpetrators. Operational collaborations increase the difficulty, costs and risk associated with executing cybercriminal activities.

Cross-sector partnerships allow for the pooling of resources, leading to enhanced capabilities that individual organizations might not achieve on their own.

All the organizations participating in this research were motivated to disrupt cybercrime. A shared motivation was to protect their organizational assets and their wider group of stakeholders, whether this be companies, customers or citizens.

Workshops and expert interviews suggest that these motivations can be broken down into connected incentives that bring organizations together and help maintain a collaboration over time:

- Feedback on impact.
- Public recognition.
- Business and regulatory support.
- Cyber resilience as a value creator for the participating organization.

> **While building cyber resilience is important, purely defensive measures will never be enough on their own. We must also impose costs on cybercriminals to make their efforts less profitable. However, imposing such costs requires a broad spectrum of capabilities resident in different parts of society, including the public, private and non-profit sectors. As a result, operational collaboration is not a "nice to have" or a "good to do"; it is the core process needed to reduce the impact of cybercrime on our societies.**
>
> Michael Daniel, President; Chief Executive Officer, Cyber Threat Alliance

Feedback loops and public recognition

Tangible impact

Anti-cybercrime collaborations that succeed over time ensure participants can see the tangible impact of their contributions. Feedback loops that keep participants informed of the results of shared intelligence, joint operations or collective strategies are essential. Feedback processes validate the efforts of individual members and encourage continuous participation by highlighting the direct correlation between input and outcome.

For example, when an organization shares threat intelligence that leads to the prevention of a major cyberattack, this success should be communicated back to the contributor, demonstrating the value of their participation. Sharing reports that show the overall impact of the collaboration, for example a reduction in cybercrime incidents, can motivate continued and enhanced engagement.

Recognition of participant input

These feedback mechanisms also serve as a learning tool, allowing organizations to refine their contributions based on what has been most effective in previous collaborations. This iterative process helps in building a more robust and resilient cybersecurity posture across the network.

Public recognition is also a powerful incentive for organizations to engage in operational collaborations against cybercrime. Collaborations require time and resources and organizations need a way to validate their participation internally to their own executives as well as externally to their clients and stakeholders. In a world where reputation and brand trust are critical assets, being acknowledged for contributing to the global fight against cybercrime can enhance an organization's standing in the market.

Cyber resilience as a value creator

Participating in operational collaborations strengthens an organization's security by providing access to a broader set of intelligence, enabling better threat detection and trend identification. Insights gained from joint efforts can be used to immediately improve internal security measures, creating a continuous improvement loop that bolsters both the organization and the collaboration network.

Training opportunities

Operational collaborations provide a unique platform for continuous learning and expertise building. Collaborations often involve a diverse group of participants, each bringing different skills and perspectives to the table. This diversity is a rich resource for knowledge exchange and individual participants appreciate the opportunities for peer-to-peer learning that help build a community and an ecosystem of trust among expert participants.

BOX 1

Data Security Council of India (DSCI) Centre for Cybercrime Investigation Training & Research (CCITR)

Founded in 2005, the NASSCOM-DSCI Cyber Labs Initiative[10] initially relied on expertise and tools from the private sector to train police in Mumbai and the wider Maharashtra state. Over time, the programme spread to several regions of India, including Bengaluru, Kolkata, Hyderabad, Haryana and Chennai, creating a network of police trained to an equally high standard.

CCITR gradually increased its focus on training using free and open-source forensic tools while continuing to maintain advisory connections to private-sector partners, who supported access to and training in new technology. The focus on open-source tools ensured a baseline capability across all police officers trained at Cyber Labs, regardless of their particular constraints of budget or access to technology.

The Cyber Labs initiative was expanded in 2019 by establishing the Centre for Cybercrime Investigation Training & Research (CCITR) at the Criminal Investigation Department in Bengaluru, Karnataka, with DSCI as the implementation and knowledge partner and the non-profit Infosys Foundation as the funding partner.

CCITR has created a trusted network of highly-skilled police officers spread across India with shared standard operating procedures for handling electronic evidence developed through CCITR's Cybercrime Investigation Manual. This supports cross-regional collaboration in the most populous country on earth. The maintenance of connections to the private sector aids the expansion of CCITR's training into new areas, such as drone forensics and Internet of Things (IoT) forensics. It also helps maintain informal connections between law enforcement and private-sector experts, which help both sides better understand each other's capabilities and constraints.

CCITR is now a collaboration between the Criminal Investigations Department of Karnataka state, the Data Security Council of India and Infosys Foundation. The basis of its growth is the stability provided by its hosting at the Criminal Investigations Department of Karnataka state and the accountability created by a governance structure that includes oversight from its host organization, funding partner, law enforcement partners, private-sector participants and regional government.

Business and regulatory support

> **Operational collaboration is an essential tool to both prevent and disrupt cybercrime and drive ecosystem resilience. Unfortunately, it remains drastically underutilized.**
>
> Megan Stifel, Chief Strategy Officer, Institute for Security and Technology

Research from 2022 by the World Economic Forum Partnership against Cybercrime demonstrates a high level of support for collaborative cyber information sharing from specialist government agencies such as the European Union Agency for Cybersecurity (ENISA) and the Cyber Security Agency of Singapore. Agencies such as the United States Cybersecurity and Infrastructure Security Agency (CISA) lead the way in supporting public-private cyberthreat sharing and collaborations for analysis such as the Joint Cyber Defense Collaborative (JCDC).[11]

The common factor among organizations whose legal team took a constructive approach for data sharing was that business leaders viewed cybersecurity as strategically important.

Legal teams' risk appetite remains a challenge

Despite the clear support shown for cybersecurity and anti-cybercrime collaborations by key government agencies, workshops and interviews undertaken for this paper indicate that corporate legal teams will regularly take a defensive posture with regard to cross-industry and public-private information sharing. This is because of the possible implications of breaching regulations overseen by non-cyber agencies, such as privacy regulators, which can include hefty fines and reputational damage.

It is possible that additional regulatory statements of support for operational collaboration could ease this challenge. However, research for this paper found variation in how corporate legal teams approach information sharing, with some organizations finding more flexibility than others even when in the same sector. The common factor among organizations whose legal team took a constructive approach was that business leaders viewed cybersecurity as strategically important to business continuity and set aside resources for the legal team to actively support cross-sector partnerships and collaborations.

The workshops and interviews undertaken for this paper indicate that where business leaders make it clear that supporting an anti-cybercrime or cybersecurity collaboration adds value to the business, and provide legal teams with the time and resources to explore this, corporate legal teams are more likely to adopt a constructive and problem-solving approach that identifies routes for collaboration.

2.2 Organizational structures and governance

Balancing formal and informal approaches to collaboration

The governance structure of the collaboration is designed to support both stringent control over sensitive areas such as data management and use, and flexibility in how experts from sometimes vastly different types of organizations interact.

This paper found that successful collaborations incorporate strict governance of data and risk, a sharp focus on measuring impact, and also considerable flexibility on how exactly experts interact with each other.

BOX 2

Cyber Threat Alliance

The Cyber Threat Alliance (CTA) started in 2014 as an informal collaboration between leading cybersecurity companies, including Fortinet, McAfee, Palo Alto Networks and Symantec, to improve the fight against cybercrime through cooperation. In 2017, it relaunched as an independent legal entity with a wider membership.

CTA members share timely and actionable information about cyberthreats, allowing them to enhance their products, better protect customers and more effectively disrupt cyberattacks. The organization also has an Early Sharing programme, in which members share finished research and analysis with each other before it is released to the public, receiving three to five of these early shares each week.

CTA uses a platform that allows members to upload and access data about cyberthreats in a standardized format. This system organizes information around key patterns and techniques used by attackers, making it easier for members to understand and act on. An algorithm scores each submission, rewarding members for sharing valuable and timely intelligence. This scoring creates a healthy sense of competition, further motivating members to improve the quality of their shared intelligence. With over 12 million data points exchanged monthly, this collaboration ensures CTA members have timely information, collectively strengthening global cybersecurity.

Core activities should be predictable but allow space for innovation

Several of the long-standing collaborations this paper studied had a core activity for which participants could plan and apply staff and resources predictably over the long term. These also had the capability to put up ad hoc groups where operations were focused on responding to a particular target or needed to move into an additional sector. These ad hoc operations were often supported by a clear mission and a commitment by participants to pursue this mission in a specified timeline.

The variation in activities was supported by clear standard operating procedures and rules that governed data management and participant behaviour, such as codes of conduct, that were consistent across all types of activity. This consistent and repeatable structure allows ad hoc groups to be set up quickly as they can follow familiar rules and procedures.

> “For effective operational collaboration, appropriate governance structures are necessary to strike a balance between the costs and benefits for affected stakeholders. INTERPOL’s Cybercrime Directorate is accountable to member countries and we strive to fight cybercrime with open, inclusive and diverse partnerships for a safer world.
>
> Neal Jetton, Cybercrime Director, INTERPOL

Governance is as much art as science

The art of supporting formal and informal governance structures requires that a collaboration’s leadership and management be sensitive to participating organizations’ risk appetites and each participant’s ability to adapt how they work to the needs of the collaboration. While some parts of governance will be rigid, others will need to have space into which the collaboration can grow. Building a community and shared work culture requires time and incremental development, so that the participants have sufficient trust in each other that they can work effectively.

BOX 3

Operation “Trust No One”

Operation “Trust No One” demonstrates how proactive collaborations between private companies and law enforcement can effectively combat transnational cyber threats.

The Royal Thai Police (RTP) dismantled a major online crime group responsible for high-value scams that targeted Thailand residents. The RTP action was supported by intelligence from the US Department of Homeland Security and private-sector partners such as the cryptocurrency exchange, Binance. This operation uncovered a sophisticated transnational cybercrime syndicate involved in hybrid scams where victims were lured into fake investments via social media platforms. Perpetrators posed as trustworthy individuals, engaging victims in long-term deception before persuading them to invest in fraudulent schemes.

The operation unfolded in several phases, including multiple raids that led to the arrest of key suspects and the seizure of significant assets. Between May and September 2023, the authorities searched over 70 locations, seizing luxury vehicles, property documents, cash and other high-value items worth billions of Thai baht. These assets were all linked to the fraudulent activities.

The operation also highlighted a balance between formal and informal collaboration methods, fostering cross-border cooperation among agencies. Victims of cybercrime were empowered to report incidents across multiple jurisdictions. The operation traced financial flows through digital wallets, transferring assets to centralized exchanges such as Binance and Huobi, with a total scam value of nearly $126 million.

This data was crucial in tracking the movement of digital assets linked to fraudulent activities and facilitated eventual arrests.

งานแถลงข่าว
การรับคำร้องขอคุ้มครองสิทธิเพื่อเฉลี่ยทรัพย์
คืนผู้เสียหายคดี Hybrid Scam
ณ อาคารประชุมสัมมนาและฝึกอบรม สำนักงานตำรวจแห่งชาติ (เมืองทองธานี)

Source: Binance[12]

“ Building and maintaining trust among partners is fundamental to the success of the collaboration.

The governance fork

A dual-tiered governance model can prove helpful, where strict governance is applied to data management while allowing for a more adaptable approach in other operational areas.

This bifurcated approach ensures that sensitive data is protected in accordance with the highest standards of security and compliance, including adherence to relevant legal frameworks such as the European Union’s General Data Protection Regulation (GDPR), while other components of the collaboration – such as resource allocation, project management and innovation initiatives – benefit from a governance model that encourages agility and responsiveness.

Strict data governance

Data governance protocols include detailed procedures for data sharing, storage and access. These protocols should be documented and regularly updated to reflect changes in technology and regulatory environments. Access to data is controlled through a system of role-based permissions, ensuring that only authorized individuals have access to sensitive information. Audit trails are at the core of monitoring data access and usage, providing a mechanism for accountability and transparency.

Flexible governance of collaboration between people

In contrast, other aspects of the collaboration, such as strategic decision-making, resource deployment and partner engagement, can be managed under a lighter governance structure. This approach allows for faster decision-making and the ability to adapt to emerging threats or opportunities without the burden of excessive bureaucracy. However, even within this lighter framework, it is important to establish baseline protocols to ensure consistency and alignment across the collaboration. Consistency in collaboration practices, from onboarding new partners to executing joint operations, reinforces trust and ensures that all partners feel valued and engaged.

Consider how actions impact trust between community members

Building and maintaining trust among partners is fundamental to the success of the collaboration. Trust can be established through consistent adherence to agreed-upon processes, transparent decision-making and the equitable sharing of responsibilities and benefits. Regular and flexible interactions, both formal and informal, help build relationships and foster a sense of shared purpose, while also allowing for adjustments that adapt to different organizational cultures.

BOX 4

The art of formal and informal structures

For each collaboration, the sensitivity of the underlying data it uses influences the speed of set-up and the rigidity of its data management requirements.

The Cybercrime Atlas

The Cybercrime Atlas is an initiative launched in 2023 and hosted at the World Economic Forum Centre for Cybersecurity. Participants collaborate to build a shared understanding of cybercriminal networks using open-source intelligence. This information is then used to support community members to create friction across cybercriminal activities and to support action by public-sector agencies.

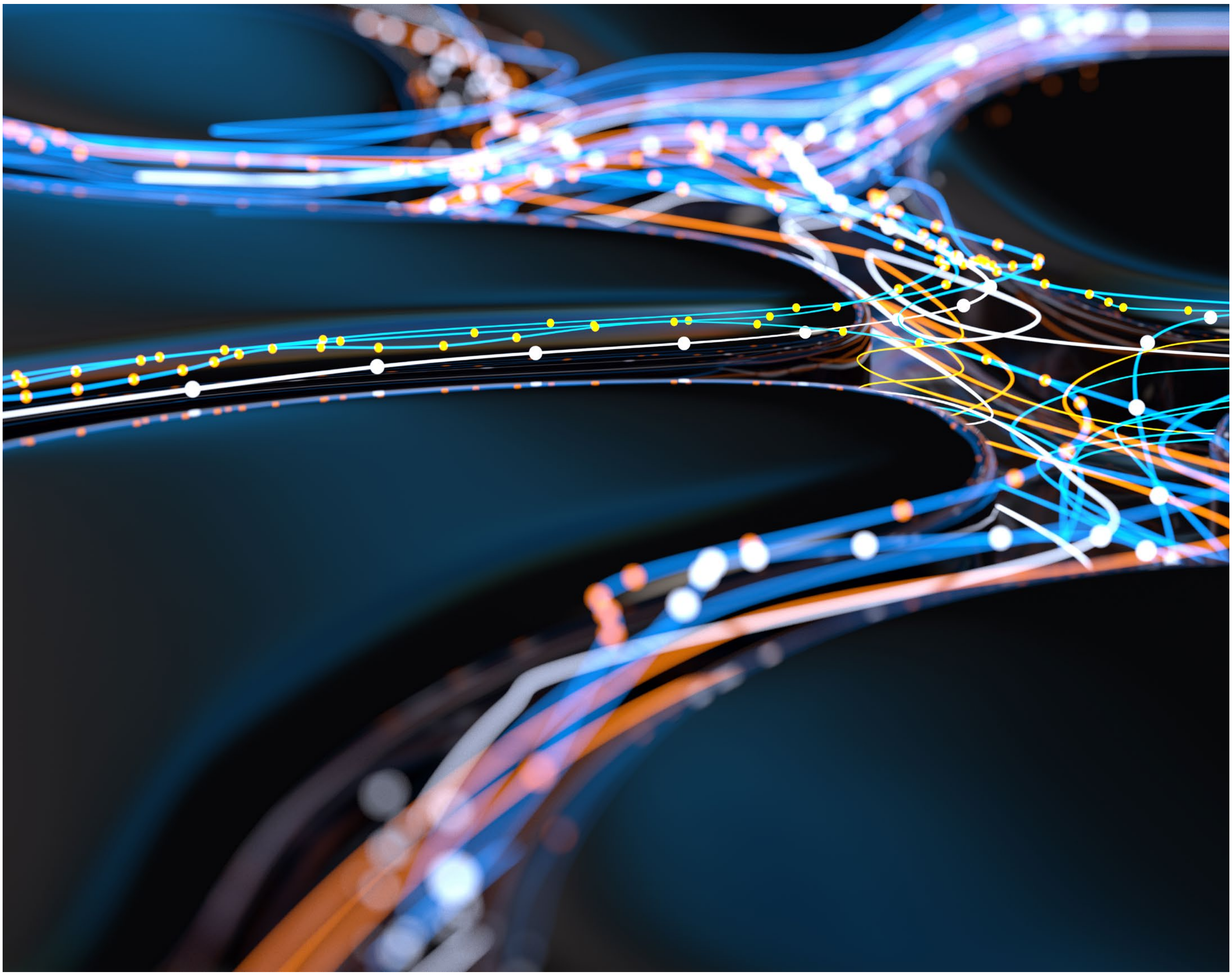
The starting point for the information is that it is open-source and shareable. Information only becomes sensitive as assessments of criminal activity are built around it.

Because the underlying information is not sensitive, the Cybercrime Atlas was in a position to start research while relying on already accepted standards for information classification, such as the Traffic Light Protocol. This allowed the Cybercrime Atlas to build rules around the needs and activities of the community as it developed. A strong emphasis was put on security of information from the outset but the reliance on open-source intelligence (OSINT) allowed the community to avoid time-consuming deliberations over the legality of sharing information generated by the collaboration between participants. This allowed for speedy set-up and the development of standard operating procedures by the Cybercrime Atlas expert community itself.

The Cyber Threat Alliance (CTA)

Unlike many threat-sharing organizations, CTA membership requires participating companies to share data directly related to their core business. This situation differs significantly from asking a financial institution or hospital to share cyberthreat intelligence and it generated concerns ranging from anti-trust to competitive advantage to intellectual property.

Due to these factors, the rules, guidelines and data management procedures had to be clear, robust and in place before it began operation. The formalization, testing and legal review of these rules took place over a two-year period from 2015 to early 2017. This focus on business rules has enabled CTA to maintain trust, support growth at scale and achieve its mission, but it also shows that data-sharing collaborations can encounter time-consuming and expensive barriers to formation.



Processes and standard operating procedures

Operational collaborations aimed at combating cybercrime are rooted in a foundation of clear, purpose-driven processes.

Mission statement

A well-articulated mission, developed collaboratively by all stakeholders, serves as the guiding principle for activities and is periodically reviewed within the collaboration's governance framework to adapt to changing cyberthreats. The collaboration's duration should be clearly defined from the start, with options for extension or termination based on performance, goal achievement or contextual changes. Clear criteria and transparency in decision-making help maintain focus and efficiency throughout the collaboration.

Membership capability assessments: No free-riders

Effective collaboration depends on the quality and commitment of participants, which is ensured through capability assessments conducted before onboarding new partners. These assessments evaluate prospective partners' interests, and technical, operational and strategic capabilities to ensure alignment with the collaboration's mission and objectives. Clear criteria, such as cybersecurity expertise or access to unique resources, help avoid free-riders and ensure meaningful contributions.

Protective measures that facilitate collaboration

A significant barrier to collaboration in cybersecurity is the fear of reputational damage or commercial loss, particularly if a shared operation goes awry or sensitive information gets misused. Clear protocols and legal agreements that govern behaviour and support participants' trust in each other help mitigate this risk.

BOX 5 | LabHost: Arrests, disruption and brand destruction

In April 2024, police in the United Kingdom (UK) took down the online criminal service provider LabHost[13] and arrested key actors in the criminal service as well as their clients. This was supported by coordinated arrests by law enforcement in 19 countries.[14]

Private-sector expertise creates leads

The origin of the disruption was a private-sector collaboration, the Cyber Defence Alliance (CDA). This is a group of cybercrime investigators funded by UK financial services whose aim is to provide insights that disrupt cyberthreat networks and enhance cybersecurity.

Law enforcement builds a case and takes action

The CDA shared leads with UK law enforcement who, with support from Europol, were able to share the information with partners in North America and Europe, gather intelligence on criminal activities and then use it to take down cybercrime services and make coordinated arrests.

Brand disruption creates more than reputational risk

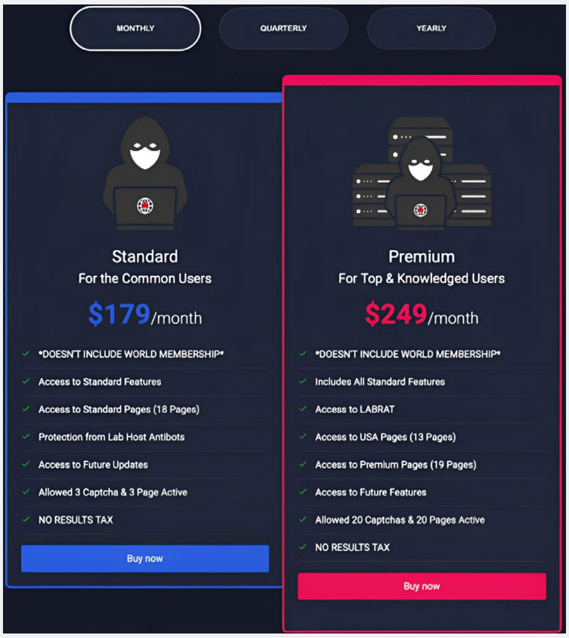
After the arrests and the take-down of technical infrastructure were made public, cybercriminals using LabHost were sent short personalized "LabHost Wrapped" videos. This gave a summary of the evidence gathered by law enforcement against the individual criminal. This was coupled with other strategic communication campaigns on platforms where the cybercrime-as-a-service providers ran their communications with users, such as Telegram.

Focusing on brand destruction builds a sense of distrust and uncertainty among criminals. This heightens the sense of risk criminals should feel.[16] It also highlights the value of strategic communications expertise in helping to design an effective anti-cybercrime operation, by understanding the cybercriminal environment and the tactics cybercriminals use.

Impact

The LabHost operation had such high impact because it made full use of capabilities across the affected organizations. Private-sector expertise was pooled, enhanced and shared via the CDA. Law enforcement were able to use this at scale thanks to facilitation through an international organization, in this case, Europol. Moreover, this information was used to damage LabHost's branding, severely affecting the group's reputation and modus operandi.

Organizations such as Europol and INTERPOL sit at the centre of networks of collaborations between nation-states and between the private and public sectors. This allows them to spot opportunities to support operational innovation and act as important points of coordination and capacity building when tackling cross-border cybercrime networks.



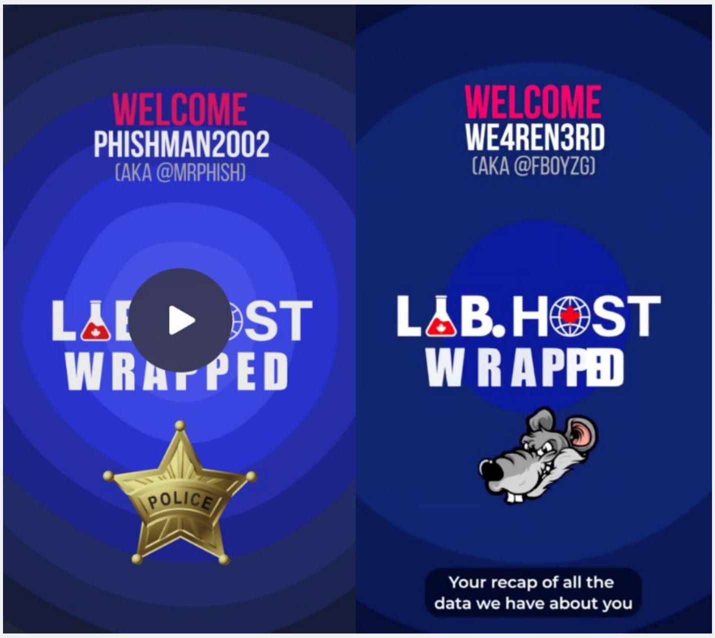
Standard
For the Common Users
$179/month

- ✓ •DOESN'T INCLUDE WORLD MEMBERSHIP•
- ✓ Access to Standard Features
- ✓ Access to Standard Pages (18 Pages)
- ✓ Protection from Lab Host Antibots
- ✓ Access to Future Updates
- ✓ Allowed 3 Captcha & 3 Page Active
- ✓ NO RESULTS TAX

Premium
For Top & Knowledged Users
$249/month

- ✓ •DOESN'T INCLUDE WORLD MEMBERSHIP•
- ✓ Includes All Standard Features
- ✓ Access to LABRAT
- ✓ Access to USA Pages (13 Pages)
- ✓ Access to Premium Pages (19 Pages)
- ✓ Access to Future Features
- ✓ Allowed 20 Captchas & 20 Pages Active
- ✓ NO RESULTS TAX

Source: Screenshot LabHost subscription offers[15]



Source: "LabHost Wrapped"[17]

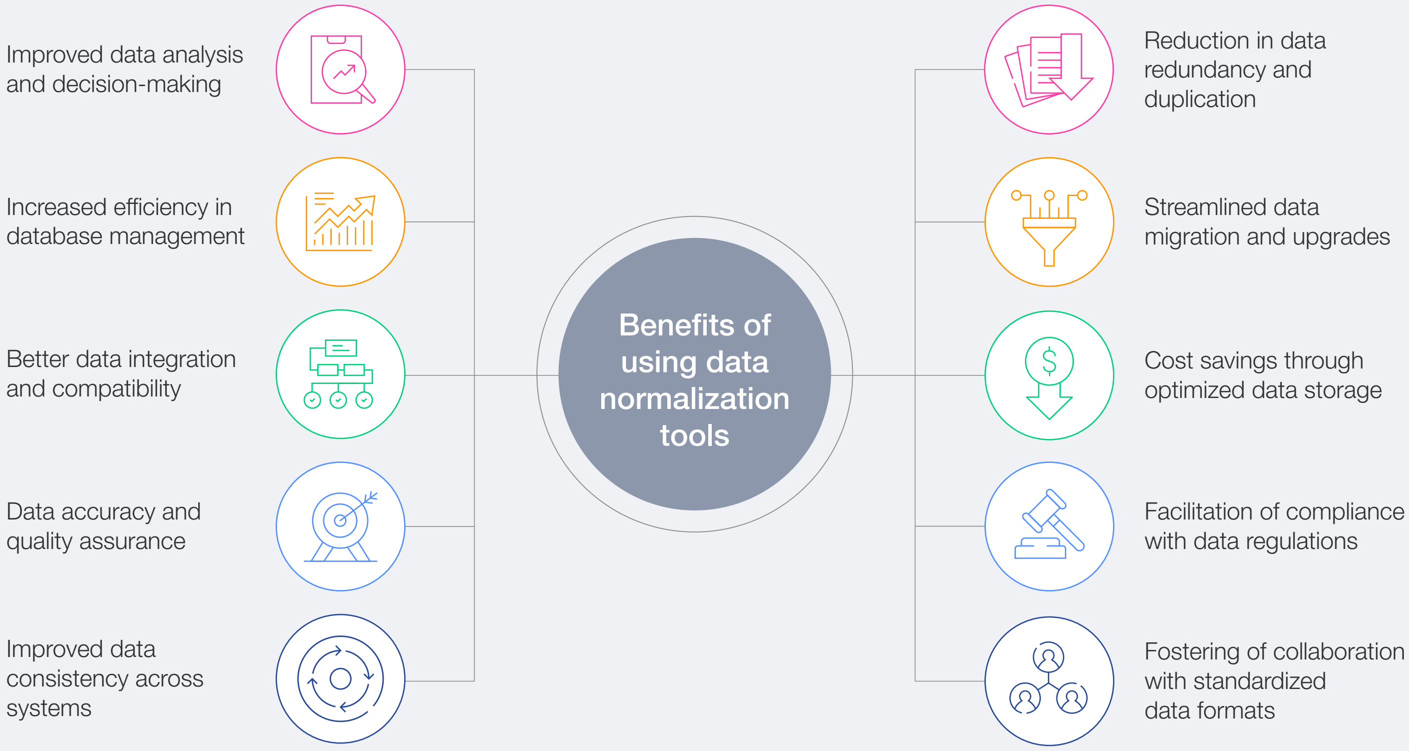
2.3 Resources

Effective operational collaboration in the fight against cybercrime requires a well-coordinated deployment of resources. The complexity and global nature of cybercrime demand an array of tools, legal frameworks, human expertise and technological capabilities that must work together to ensure a cohesive response.

A unified response to cyberthreats is dependent on the standardization of threat definitions. Cybercrime taxonomies create a common language that facilitates clear communication across different organizations and sectors. By aligning on definitions of specific cybercrimes, taxonomies enable faster identification and categorization of threats. Standardized taxonomies also simplify incident reporting, allowing organizations to accurately classify and communicate the nature of cyber incidents.

Data normalization is an extension of this standardization, ensuring that data from various sources is harmonized into comparable formats. As cyberthreat information is typically generated by a variety of sensors, systems and platforms, it arrives in different formats, often incompatible with one another. Through the process of data normalization, these disparate data streams are converted into a unified structure, which is essential for effective aggregation, analysis and dissemination across stakeholders.

FIGURE 2 **Taxonomies and data normalization**


Improved data analysis and decision-making
Increased efficiency in database management
Better data integration and compatibility
Data accuracy and quality assurance
Improved data consistency across systems
Benefits of using data normalization tools
Reduction in data redundancy and duplication
Streamlined data migration and upgrades
Cost savings through optimized data storage
Facilitation of compliance with data regulations
Fostering of collaboration with standardized data formats

Source: Kohezion[18]

> **Despite their inherently deceptive activities – breaking into systems, stealing data and encrypting vital information – ransomware groups must convince their victims of their trustworthiness. This trust encompasses not just the promise not to release the stolen data but also the assurance that payment will result in the decryption of the affected systems. A key way for ransomware groups to gain this trust is through branding and reputation. Indeed, each time they interact with a victim, they are negotiating not just for that particular ransom but also for their reputation. If they fail to uphold their end of the bargain, they risk damaging their reputation, which deters future potential victims from trusting and engaging with them.**
>
> Max Smeets, Co-Director, European Cyber Conflict Research Incubator

Data management and information security

Information security protocols safeguard shared intelligence against unauthorized access, breaches and data corruption. Data encryption, user authentication and secure communication channels are necessary to maintain the integrity of sensitive data. Without these protections, the collaborative sharing of cyberthreat intelligence could expose organizations to additional vulnerabilities, undermining the goals of such initiatives.

Additionally, the exponential growth of cyberthreat data has placed significant demands on data storage and processing infrastructures. Collaboration requires the capacity to store vast amounts of structured and unstructured data while maintaining the ability to process and analyse this data at scale. As data streams are continuously generated and shared across the collaborative ecosystems, the infrastructure supporting data storage and processing must ensure that insights can be derived quickly and efficiently.

High-performance computing environments allow for the rapid execution of complex algorithms, enabling organizations to respond to threats in real time, before the data becomes obsolete. Moreover, data storage solutions must adhere to rigorous security standards to prevent unauthorized access or breaches, further ensuring the integrity of the collaborative effort.

Data feeds

Data feeds play a crucial role in cybersecurity collaboration by providing continuous, automated streams of actionable intelligence to organizations' security systems, enabling timely detection, analysis and response to threats. These feeds include various types of data, such as threat indicators, vulnerabilities and malware signatures, sourced from multiple platforms. By integrating data feeds into threat intelligence platforms (TIPs) and security information and event management (SIEM) systems, organizations can shift from a reactive to a proactive cybersecurity approach, automating the ingestion and analysis of large volumes of data. This real-time data flow is crucial for several reasons:

- **Speed and automation**: Automated data feeds reduce the time it takes to detect and respond to threats by constantly updating security systems with the latest information.

- **Cross-sector sharing**: Data feeds are a core element of collaborative efforts across industries. Public-private partnerships often rely on shared data feeds to provide early warnings about specific threats.

- **Contextualizing threats**: Data feeds not only supply raw data, but often come enriched with contextual information. This context allows organizations to prioritize their responses based on the relevance of the threat and the reliability of the data.

Mapping the threat ecosystem and tactics

The work of operational collaboration is supported by an ability to identify threat actors and understand their motivations, methods and the infrastructure they use. Threat maps, built through the aggregation of intelligence from multiple sources, provide valuable insights into the operational behaviours of cybercriminal groups.

These maps help organizations understand how specific tactics are deployed, which in turn enables more targeted defences and the identification of the disruption opportunities that are a vital part of protecting organizations and society against cyberthreats.

BOX 6 | LockBit: Anatomy of a cross-border cybercrime provider

In February 2024, an international task force of law-enforcement agencies from 10 countries, dubbed Operation Cronos, disrupted the operations of the world's then most prolific ransomware group, LockBit.

This was led by the UK National Crime Agency with cross-border coordination through Europol and Eurojust. In what Europol describes as a "significant breakthrough in the fight against cybercrime", LockBit's technical infrastructure and its public-facing leak site on the dark web was seized, including 34 servers across multiple countries and the freezing of over 200 cryptocurrency accounts. Over 14,000 accounts belonging to affiliates were also seized and taken down thanks to the cooperation of private partners. The arrest of key individuals and the seizure of their dark web platform was a crucial step in diminishing the group's ability to execute large-scale ransomware attacks, which had caused billions of euros in damage globally.

How did LockBit operate?

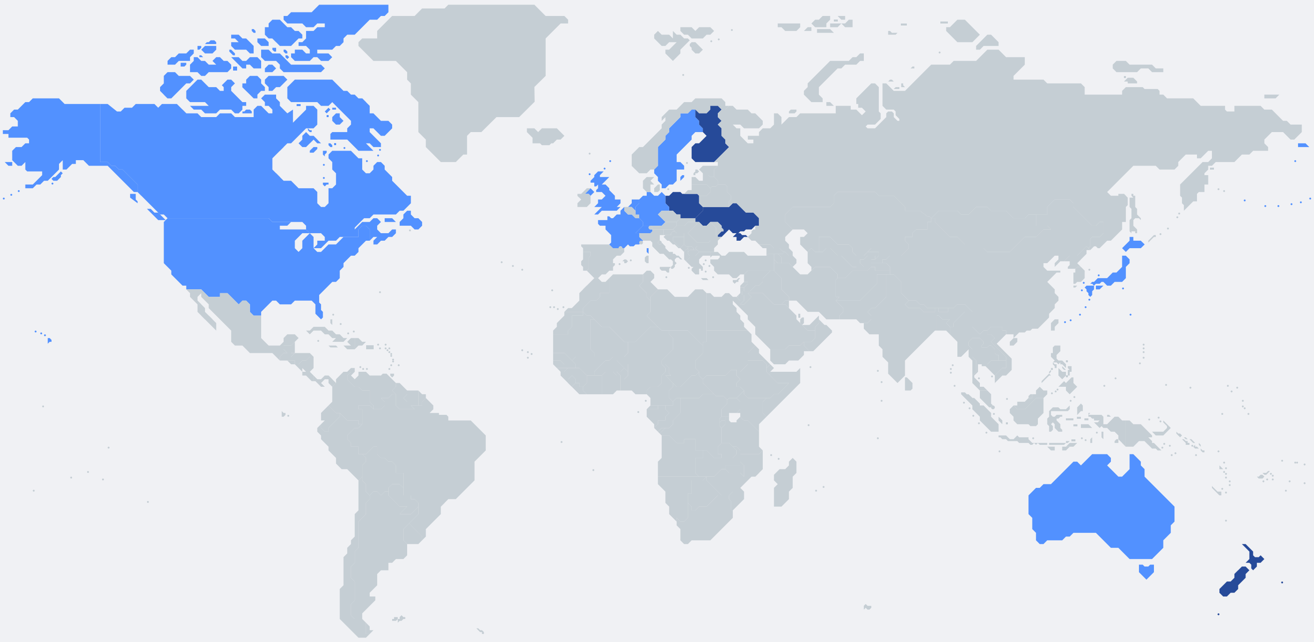
A ransomware attack is one where cybercriminals hack into your device, use malicious software (malware) to encrypt and steal information, preventing you from accessing it, and then threaten to leak that data unless you pay a ransom.

LockBit offered ransomware services to its global network of hackers or "affiliates", giving them the malware and platform to carry out these attacks and collect ransoms from thousands of victims globally, including global high-profile organizations.

What lesson does it hold?

Operation Cronos highlights the growing success of international cooperation in law enforcement. This is supported by organizations like the European Cybercrime Centre (EC3) at Europol which, on top of its role in information-sharing between police forces, acts as a facilitator of multiple networks of expertise, bringing experts from law enforcement together in a trusted environment. This supports the sharing of advanced technical skills, legal expertise and operational knowledge across borders.

In this groundbreaking effort, law enforcement agencies from 10 countries worked together to "hack the hackers",[20] seize their tools and recover over 1,000 decryption keys, which have helped victims regain access to their data. With these decryption keys collected by the UK, Europol proactively prepared country-specific packages to support victims, which were distributed to 33 countries.



● **Participating countries:** Finland, New Zealand, Poland, Ukraine

● **Core countries:** Australia, Canada, France, Germany, Japan, Netherlands, United Kingdom, United States, Sweden, Switzerland

Source: Europol[19]

Open-source intelligence (OSINT)

OSINT offers a dynamic resource for operational collaboration. It refers to the collection and analysis of publicly available information from sources such as social media, news reports and online forums. It provides a complementary dimension to traditional intelligence sources and is often available in real time. The integration of OSINT into collaborative frameworks expands the range of available data, supporting early threat detection, situational awareness and more timely responses.

One of the key advantages of OSINT lies in its accessibility. Unlike proprietary or classified intelligence, OSINT can be shared widely across organizations, enhancing transparency and cross-sector collaboration. Furthermore, its use is bound by fewer legal restrictions, thus facilitating its incorporation into multistakeholder operations. With the right analytical tools, OSINT can be integrated into existing data streams, enriching the overall intelligence picture.

Legal protocols

Collaborations benefit from frameworks, contracts and other legal tools that support data sharing and rules of engagement. These protocols provide the legal foundation for cross-border cooperation, enabling diverse stakeholders – public institutions, private enterprises, law enforcement agencies and civil society – to engage in the timely exchange of intelligence. Legal protocols formalize relationships between entities, clarifying roles and responsibilities while ensuring compliance with international privacy standards.

BOX 7 INTERPOL's Global Cybercrime Expert Group and Project Gateway

INTERPOL's interactions with the private sector are governed by a combination of cooperation agreements in the framework of Project Gateway for cybercrime data sharing, organizational rules on the processing of data, and principles of interaction established by INTERPOL's Constitution.[21]

Police actions such as Operation Synergia in 2023 benefitted from these partnerships. Operation Synergia[22] was launched in response to the clear growth, escalation and professionalization of transnational cybercrime and the need for coordinated action against new cyberthreats.

The operation involved 60 law enforcement agencies from more than 50 INTERPOL member countries, with officers conducting searches and seizures of servers and electronic devices. Gateway Partners from the private sector provided analysis and intelligence support throughout the operation.

Operations like this require building trusted partnerships with the private sector and maintaining engagement over time. The limits set by INTERPOL's governance of private-sector partnerships create the time, space and ground rules to support a variety of collaborations. This ranges from the INTERPOL Global Cybercrime Expert Group[23] that supports development of law enforcement strategies and best practices, to operational collaborations built on the Project Gateway model.

By combining strict governance of data sharing with flexibility on the character of each collaboration, INTERPOL has developed long-term relationships with key private-sector partners while retaining the ability to bring in ad hoc expertise when needed.

↓ **Source:** World Economic Forum, based on an image from INTERPOL

Operation Synergia Global Operation Against Malicious Infrastructure of Phishing, Banking Malware, and Ransomware

55 Countries

63 Cyber activity reports

1,300+ Malicious servers

70% Servers taken down

30 House searches

70 Suspects identified

> **In today's rapidly evolving digital landscape, an operational collaboration framework is imperative to effectively combat cybercrime. Fostering seamless coordination between public- and private-sector entities by leveraging their collective expertise, resources and capabilities, and promoting information sharing to pre-emptively address threats will help us all respond to incidents with heightened agility and precision.**
>
> Alexandra Gerst, Senior Corporate Counsel, Microsoft Digital Crimes Unit, Microsoft

These frameworks support the exchange of actionable intelligence without compromising the confidentiality or integrity of sensitive data. Alignment on legal requirements mitigates challenges related to jurisdictional issues, ensuring that intelligence and resources can be mobilized swiftly and securely across borders.

> Collaboration fosters a knowledge-sharing environment in which best practices, lessons learned and advanced strategies can be disseminated throughout the community.

To streamline legal and operational relationships within the collaboration, model non-disclosure agreements (NDAs) and memoranda of understanding (MoUs) provide standardized and tailored regulations to address the unique needs of working within a public-private partnership. Model NDAs focus on protecting sensitive information and intellectual property while facilitating the necessary sharing of data among partners. They outline the obligations of each party regarding confidentiality, data handling and legal resources in case of breaches.

Model MoUs, on the other hand, establish the roles, responsibilities and expectations of each partner within the collaboration. The use of standardized MoUs and NDAs helps reduce the time and complexity involved in formalizing partnerships, allowing the collaboration to focus more on operational activities.

Human expertise and skill development

Human expertise and the continuous development of skills are critical resources in combating cybercrime. Cybersecurity threats evolve rapidly, requiring that personnel remain up-to-date with the latest tactics, techniques and procedures used by cybercriminals. Effective operational collaboration depends on highly skilled professionals across a range of disciplines. Capacity building through shared training programmes and joint exercises ensures that all participating entities maintain the necessary skill sets to address emerging cyberthreats. Collaboration fosters a knowledge-sharing environment in which best practices, lessons learned and advanced strategies can be disseminated throughout the community, ultimately enhancing the overall capabilities of the collective defence.

BOX 8

National Cyber-Forensics and Training Alliance (NCFTA)

In the US, the National Cyber-Forensics and Training Alliance (NCFTA) has emerged as a leading model for operational collaboration in the fight against cybercrime, uniting the private industry, academia and law enforcement to disrupt global cyberthreats. Established over two decades ago, the NCFTA has built a trusted environment where over 200 partners collaborate to exchange real-time intelligence, mitigate risks and take actionable steps to dismantle cybercriminal infrastructure. With a dedicated team of more than 60 experts, NCFTA fosters a community-driven approach that enables effective, rapid information-sharing and validation, empowering its members to manage cyber risks and support law-enforcement efforts worldwide.

A core component of NCFTA's success is its focus on community-building through specialized training programmes. By creating an ecosystem of trust, NCFTA delivers impactful training that enhances the cybersecurity capabilities of its partners. These programmes not only provide the technical knowledge required to combat cybercrime but also foster long-term, personal collaborations between stakeholders. This approach strengthens the ability to manage cyber risks and also creates a resilient network capable of proactively addressing and mitigating cybercrime on a global scale.

Conclusion

The recommendations in this white paper lead to a framework for building and sustaining operational partnerships that systematically disrupt cybercrime. The recommendations focus on flexibility in governance, the importance of building a sense of trust and community to facilitate the sharing of expertise, and the value of maintaining feedback mechanisms that ensure participants see the tangible impact of their contributions and can explain this impact to their own stakeholders.

By strengthening collaboration, stakeholders improve their own defences while also increasing the costs for cybercriminals to enter the cybercrime market. Effective operational collaborations between the private and public sectors raise the personal cost of cybercrime through disruption to technical infrastructure and can increase the personal risk to cybercriminals of being arrested. When effective, these collaborations impose real costs on cybercriminals, diminishing their ability to cause harm.

Looking ahead, it is clear that continued success hinges on further developing these partnerships, integrating new technologies and fostering a culture of trust and knowledge sharing. Operational collaborations are not merely a “nice to have” but are essential to mitigating the growing cyberthreats facing societies globally. The progress made thus far is a testament to the power of collective action, and with sustained commitment, it is possible to create a more secure and resilient digital future.

Appendix: Methodology

This report is based on desk research and a series of workshops held between March 2024 and August 2024 which included 58 members of the World Economic Forum's Partnership Against Cybercrime. These workshops were supplemented by 21 extended interviews, which included several experts from the World Economic Forum's wider community of experts.

Contributors

Lead author

Natalia Umansky
Project Specialist, Cybercrime Atlas Initiative, World Economic Forum

World Economic Forum

Seán Doyle
Lead, Cybercrime Atlas Initiative

Tal Goldstein
Head of Strategy and Policy, Centre for Cybersecurity

Giulia Moschetta
Initiatives Lead, Centre for Cybersecurity

Acknowledgements

Jorij Abraham
Managing Director, Global Anti-Scam Alliance

Akbar Akhtar
Head of Investigations, APAC, Binance

Shane Britten
Chief Executive Officer, Crime Stoppers International

Jessada Burinsuchat
Superintendent, Cyber Security Investigations Unit, Royal Thai Police

Anna Chung
Principal Researcher, Unit42, Palo Alto Networks

Jethro Cornelissen
Global Anti-Fraud Officer, ING Group

Michael Daniel
President and Chief Executive Officer, Cyber Threat Alliance

Erin Fracolli
Global Head of Intelligence and Investigations

Alexandra Gerst
Senior Corporate Counsel, Microsoft Digital Crimes Unit, Microsoft

James Gill
Global Head, Cyber Threat Response, Banco Santander

Kayle Giroud
Strategy and Development Associate Director, Global Cyber Alliance

Fredrik Heiding
Research Fellow, Harvard University

Mohammed Isah
Head, Africa Cybercrime Operations Desk, Cybercrime Directorate, INTERPOL

Steven Kelly
Chief Trust Officer, Institute for Security and Technology

Josh Kenway
Manager, Strategic Cybersecurity Programs, PayPal

Jason Lancaster
Senior Vice-President, Sales Engineering and Investigations, SpyCloud

Aidan Larkin
Founder, Asset Reality

Matt LaVigna
President and Chief Executive Officer, National Cyber Forensics and Training Alliance

Pei Ling Lee
Head of Cyber Strategy and Capabilities Development, Cybercrime Directorate, INTERPOL

Garry Lilburn
Operations Director, Cyber Defence Alliance

Bertha Nayelly Loya
Head of Global Programme on Cybercrime, United Nations Office on Drugs and Crime

Derek Manky
Chief Security Strategist and Global Vice-President, Fortinet

Robert McArdle
Director FTR, Cybercrime Research, Trend Micro

Venkatesh Murthy
Senior Director, Data Security Council of India

Lenno Reimand
Stakeholder Manager, Europol

Craig Rice
Chief Executive Officer, Cyber Defence Alliance

Max Smeets
Co-Director,
European Cyber Conflict Research Incubator

Peter Stanier
Cybercrime Intelligence Officer,
Cybercrime Directorate, INTERPOL

Megan Stifel
Chief Strategy Officer,
Institute for Security and Technology

Mathew Stith
Industry Liaison, Spamhaus

Ian Tien
Chief Executive Officer, Mattermost

Production

Laurence Denmark
Creative Director, Studio Miko

Jay Kelly
Designer, Studio Miko

Madhur Singh
Editor, World Economic Forum

Cat Slaymaker
Designer, Studio Miko

Endnotes

1. Raza, Muhammad. “Cybercrime as a Service (CaaS) Explained”. *Splunk Blog.* 14 February 2023. https://www.splunk.com/en_us/blog/learn/cybercrime-as-a-service.html

2. Bakshi, Mousumi. “Kettering firm KNP Logistics Group’s sudden collapse upsets drivers”. *BBC News.* 4 October 2023. https://www.bbc.com/news/uk-england-cambridgeshire-66997691

3. Global Anti-Scam Alliance (GASA). “The Global State of Scams – 2023”. https://www.gasa.org/_files/ugd/7bdaac_b0d2ac61904941aeb4cbf0217aa355d2.pdf

4. Doyle, Seán. “Cybercrime and violent Crime are converging: here’s how to deal with it”. *World Economic Forum Agenda Blog.* 31 October 2023. https://www.weforum.org/agenda/2023/10/cybercrime-violent-crime/

5. Kelly, James W. “O-type blood donors needed after London cyber-attack”. *BBC News*. 10 June 2024. https://www.bbc.com/news/articles/c2eeg9gygyno

6. BBC News. “Hospitals cyber attack impacts 800 operations”. 14 June 2024. https://www.bbc.com/news/articles/cd11v377eywo

7. INTERPOL. “INTERPOL operation strikes major blow against West African Financial Crime”. 16 July 2024. https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-operation-strikes-major-blow-against-West-African-financial-crime

8. Symonds, Tom. “Police bust global cyber gang accused of industrial-scale fraud”. *BBC News.* 18 April 2024. https://www.bbc.com/news/uk-68838977

9. Europol. “International Investigation disrupts phishing-as-a-service platform LabHost”. April 2024. https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost

10. Data Security Council of India. Centre for Cybersecurity Investigation Training & Research. https://www.dsci.in/content/ccitr

11. CISA Joint Cyber Defense Collaborative. https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative

12. Binance. Binance Aids Royal Thai Police in Crackdown on Criminal Networks (2023-10-03). https://www.binance.com/en/blog/ecosystem/binance-aids-royal-thai-police-in-crackdown-on-criminal-networks-9108477038245506340#Operation-Trust-No-One

13. Symonds, Tom. ”Police bust global cyber gang accused of industrial-scale fraud”. *BBC News*. 18 April 2024. https://www.bbc.com/news/uk-68838977

14. Europol. “International Investigation disrupts phishing-as-a-service platform LabHost”. 28 April 2024. https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost

15. Bartlett, Jamie. “The police have a new approach to cybercrime: And it’s actually quite good”. *How to Survive the Internet*. 19 April 2024. https://jamiejbartlett.substack.com/p/the-police-have-a-new-approach-to

16. Tyler, Michael. “LabHost Wrapped – Notorious Phishing-as-a-Service Platform Taken Down”. *Fortra PhishLabs*. 18 April 2024. https://www.phishlabs.com/blog/labhost-wrapped-notorious-phishing-service-platform-taken-down

17. Bartlett, Jamie. “The police have a new approach to cybercrime: And it’s actually quite good”. *How to Survive the Internet*. 19 April 2024. https://jamiejbartlett.substack.com/p/the-police-have-a-new-approach-to

18. Kohezion. Benefits of Using Data Normalization Tools. https://www.kohezion.com/blog/data-normalization-tools

19. Europol. “Law enforcement disrupt world’s biggest ransomware operation”. 20 February 2024. https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

20. Whiting, Kate. “LockBit: How an international operation seized control of ‘the world’s most harmful cybercrime group’”. *World Economic Forum Agenda*, https://www.weforum.org/agenda/2024/02/lockbit-ransomware-operation-cronos-cybercrime/

21. INTERPOL. “Statement on Procedural measures and law enforcement”. 22 June 2023. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Fifth_intersessional_consultation/Submissions/INTERPOL_Statement_on_Procedural_measures_and_law_enforcement_FINAL.pdf

22. INTERPOL. “INTERPOL-led operation targets growing cyber threats.” 01 February 2024. https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats

23. INTERPOL. “Public-private partnerships”. https://www.interpol.int/en/Crimes/Cybercrime/Public-private-partnerships. (Last accessed on 1 October 2024)

WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org