Cybercrime Atlas

Hosted at the World Economic Forum

Cybercrime Atlas: Impact Report 2024

OCTOBER 2024

Images: Getty Images, Midjourney, Unsplash

Contents

Executive summary

The first year of the Cybercrime Atlas provides a roadmap for the systematic disruption of cybercrime.

The past year demonstrates that cyber defenders are getting better at countering cybercrime globally.[1] Law enforcement and the private sector, individually and in collaboration, are demonstrating consistent progress in disrupting cybercriminal activities, protecting critical services and providing justice to victims.

At the same time, the volume of cybercrime is growing. Criminals copy what they see in the legal markets. Consider 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"[2] 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 or deliver ransomware attacks that can bankrupt businesses[3] and destroy livelihoods.

Even as the ability to disrupt cybercrime increases, criminals can still outpace efforts when work is done in isolation. Concerningly, there is an increasing connection between cybercriminal groups and organized violent crime groups such as drug traffickers and human trafficking gangs. For example, in 2023, United Nations (UN) research highlighted that at least 220,000 people had been trafficked in South-East Asia and forced to work in online scam farms. It is clear that the impact of cybercrime is rapidly shifting from the digital world to having real-life consequences.

To shrink the space in which cybercriminals operate, it is crucial to understand the criminal ecosystem and how its different components interact. A detailed mapping of these networks is essential. Much like legitimate businesses, cybercriminals rely on supply chains, creating dependencies across various criminal activities and hubs of illicit technology and services. Disrupting these interconnected networks can significantly weaken their operations.

The Cybercrime Atlas

Since July 2023, the World Economic Forum has hosted the secretariat and project management office for the Cybercrime Atlas, an initiative to improve understanding of how cybercriminals operate. The Cybercrime Atlas community uses shared knowledge and collaboration to disrupt and reshape the cybercrime landscape.

The Cybercrime Atlas was launched in January 2023 with support from Banco Santander, Fortinet Microsoft and PayPal[4] and has since expanded to include 23 private sector organizations and individual experts from across cybersecurity, information technology, financial services, digital assets and open-source intelligence (OSINT) investigations. These organizations and expert contributors provide support through deep subject matter expertise and capabilities provided through their world-leading tools and investigative platforms.

The Cybercrime Atlas continues to scale up efforts and impact, promoting new collaborative approaches to accelerate the fight against cybercrime.

An effective model of collaboration

In a world where cyber defenders often work in isolation, the Cybercrime Atlas provides experts and organizations with a platform to multiply the impact of their individual efforts. This provides a path towards the systematic disruption of cybercriminal activities.

01

Vision and mission

Mapping cybercriminal networks supports the systematic disruption of cybercriminal activities.

BOX 1 The challenge

Cybercrime is global: Cybercrime groups are large and globally distributed organizations. They often have extensive and complex technical and money laundering infrastructure.

Knowledge of cybercrime is fragmented: Cyber defenders possess valuable insights into how cybercriminals operate, but this knowledge is often confined to individual organizations or countries. Without collaboration, defenders lack a comprehensive understanding of cybercrime and a full picture of criminal activities.

Responses are scattered: Cybercrime is inherently transnational and law enforcement operates within national boundaries. Cross-industry collaboration in the private sector can also be challenging.

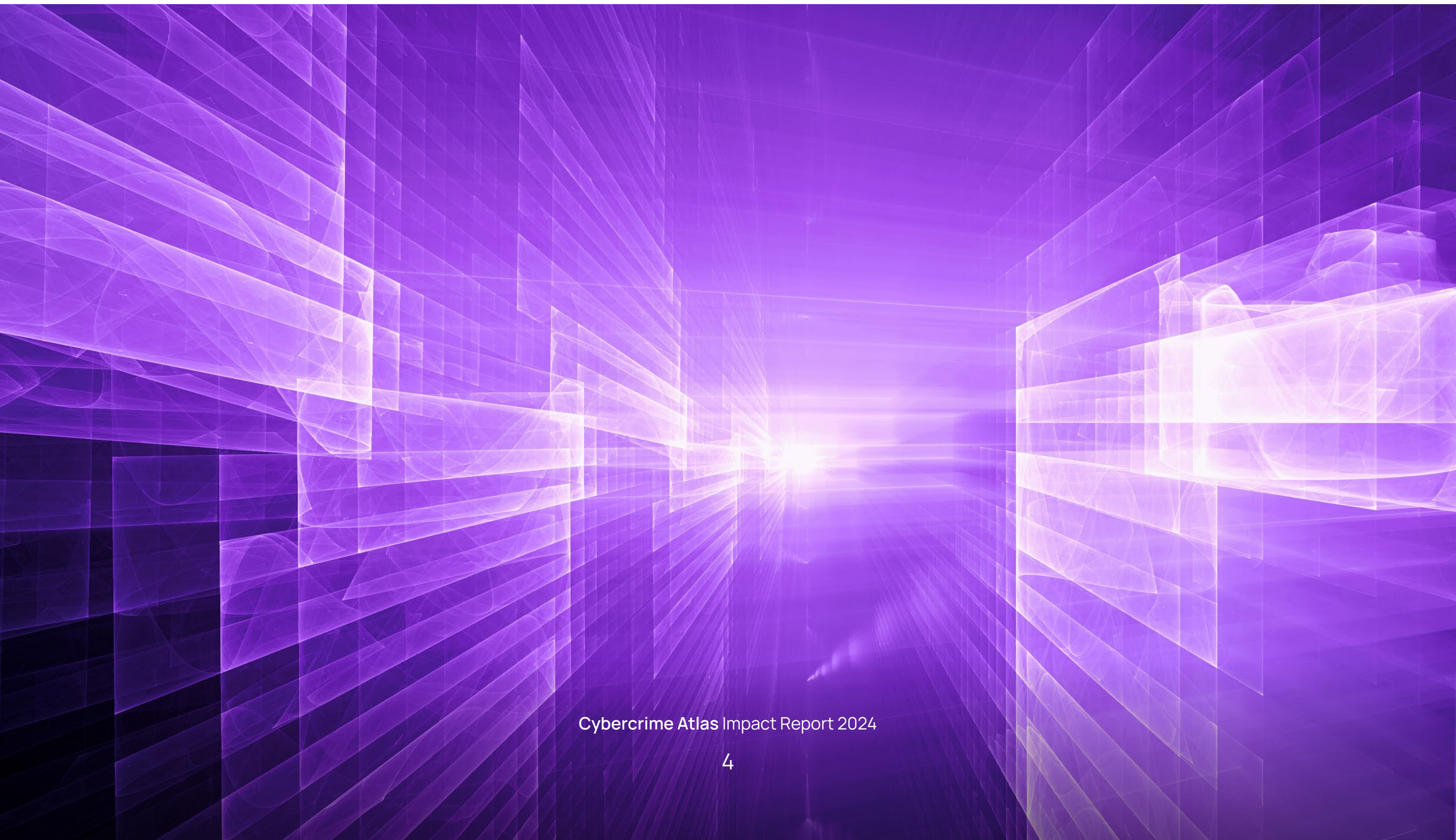
BOX 2 The response

The Cybercrime Atlas builds a shared knowledge base of the cybercriminal ecosystem that supports systematic mitigation and disruption of cybercrime.

Map the landscape, criminal operations, networks and infrastructure.

Disrupt cybercrime by using Cybercrime Atlas research to enable coordinated action against criminal activities and infrastructure.

Shape the online environment by creating evidence-based recommendations to make it safer.



02

Cybercrime Atlas outcomes

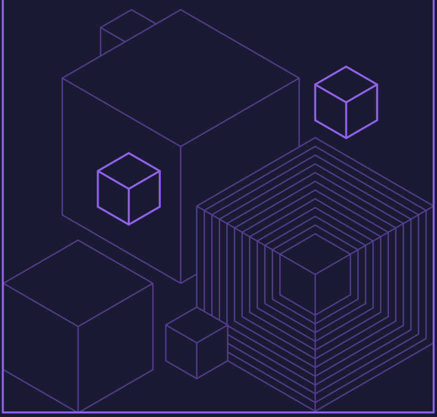
Cybercrime Atlas research, developed by global experts, delivers actionable insights with increasing quality and output.

FIGURE 1 Cybercrime Atlas outcomes in year 1

Cybercrime Atlas research is vetted by a community of world-leading cybercrime experts.
Research and intelligence packages focus on identifying cybercriminal actors and technical infrastructure.

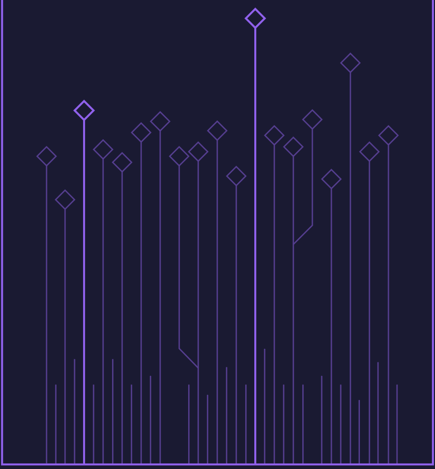
7

Intelligence packages completed July 2023-July 2024



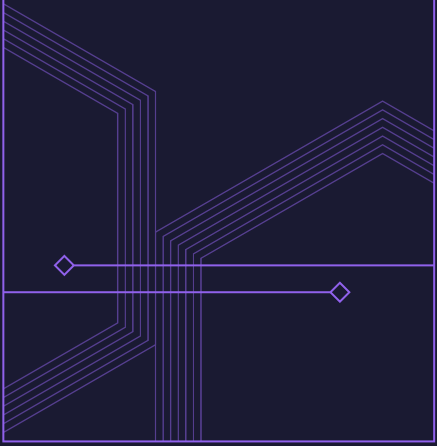
10,000+

Community-vetted and actionable data points



2

Cross-border disruption campaigns supported by Cybercrime Atlas research in 2024



Source Cybercrime Atlas

Cybercrime Atlas research is different

Cybercrime Atlas research is developed and vetted by a community of world-leading experts in cybercrime investigations, threat intelligence and cybersecurity research. These experts come from a diverse range of industries and skill sets, making the Cybercrime Atlas unique in value.

Cybercrime Atlas research and intelligence packages contain only information that the community deems actionable.

Gathering speed

Significant progress has been made in completing Cybercrime Atlas research and intelligence packages, from two packages in the second half of 2023 to seven by mid-2024, with several others under development.

The feedback mechanisms within and between the Cybercrime Atlas community and public sector partners mean that the quality of research output is improving while production rates increase simultaneously.

03

About the Cybercrime Atlas

Cybercrime Atlas research identifies criminals' vulnerabilities, supporting cyberthreat mitigation and enabling collective disruption with public sector partnerships.

Launched in 2023 and hosted at the World Economic Forum, the Cybercrime Atlas community uses open-source research to create new insights into the cybercriminal ecosystem.

Cybercrime Atlas participants and partners in the public sector use this research to disrupt cybercrime and mitigate the impact of cyberattacks.

Disrupting organized cybercrime requires a global effort, with strong, trusted relationships between private sector participants and between the private sector and public sector partners. The World Economic Forum provides the Cybercrime Atlas community with an impartial platform to support international public-private collaboration.

> [The Cybercrime Atlas] underlines the need for an enhanced multi-sector approach to combat the increasing cybercrime threat. A global solution must include private sector insights to enable law enforcement to prevent, detect, investigate and disrupt cybercrime.
>
> Jürgen Stock
> Secretary-General, INTERPOL, January 2023

Collaboration is the key

Collaborative research is key to the Cybercrime Atlas's mission. By combining diverse expertise, participants generate new insights and ensure confident joint assessments while identifying which organizations can apply the research most effectively.

Collaborative and well-governed research also creates trust between experts and between the institutions they work for.

By developing new knowledge to disrupt cybercriminals, the Cybercrime Atlas helps identify joint responses, breaking down barriers to collaboration across industries and with the public sector.

The Cybercrime Atlas grew out of recommendations of the World Economic Forum's Partnership Against Cybercrime and continues to have a close relationship with this world-leading source of expertise on tackling cybercrime.

FIGURE 2 Cybercrime Atlas highlights January 2023-July 2024

January 2023

Cybercrime Atlas announced at World Economic Forum Annual Meeting in Davos

July 2023

Atlas secretariat and project management office launched

September 2023

First research package delivered

October 2023

Public-sector workshops

November 2023

In-person community meeting at the World Economic Forum Annual Meeting on Cybersecurity

December 2023

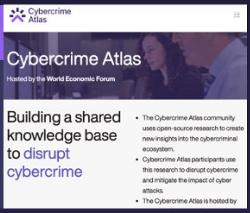
Cybercrime Atlas visual identity finalized

January 2024

Cybercrime Atlas at World Economic Forum Annual Meeting in Davos 2024

January 2024

Public website launched



Cybercrime Atlas

Cybercrime Atlas

Hosted by the World Economic Forum

Building a shared knowledge base to disrupt cybercrime

- The Cybercrime Atlas community uses open-source research to create new insights into the cybercriminal ecosystem.
- Cybercrime Atlas participants use this research to disrupt cybercrime and mitigate the impact of cyber attacks.
- The Cybercrime Atlas is hosted by

March-May 2024

Microsoft
Digital Crimes Consortium 2024
March 11-14, 2024 | Tokyo Hilton | Shinjuku-Ku, Tokyo, Japan
FORTINET
ACCELERATE 2024

Engagement with expert stakeholders and the public

May 2024

First confirmation that Atlas research supported successful cybercrime disruptions

June 2024

Annual Review meeting, Washington D.C.

June 2024

Work starts on an Anti-Cybercrime Collaboration Framework at Partnership Against Cybercrime meeting, World Bank, Washington D.C.

July 2024

Seventh research package delivered

August-September 2024

Scoping begins for next stage of Cybercrime Atlas development

Source Cybercrime Atlas

What does the Cybercrime Atlas target?

In its launch year, the Cybercrime Atlas focused its research on financially motivated cybercriminal groups. Research into sophisticated state-controlled or state-sponsored groups, as well as well-known ransomware groups, was out of scope. This was due to the already significant amount of high-quality research into these groups.

TABLE 1 Two guiding principles that shape Cybercrime Atlas research

Serving public interest	Atlas research has a strong potential to disrupt cybercriminal activities that harm society. This includes cases where cybercrime groups target vulnerable individuals, attack critical infrastructure like hospitals, or are involved in violent organized crime, large-scale fraud, human trafficking or other harmful activities.
Having systemic impact	The Atlas community has determined that researching a specific cybercrime group will generate new insights into the broader cybercrime ecosystem, helping to support efforts to mitigate or disrupt cybercrime on a systemic level.

Note The full list of principles guiding decisions on research targets is shared with the Atlas community and public-sector partners but is not released publicly.

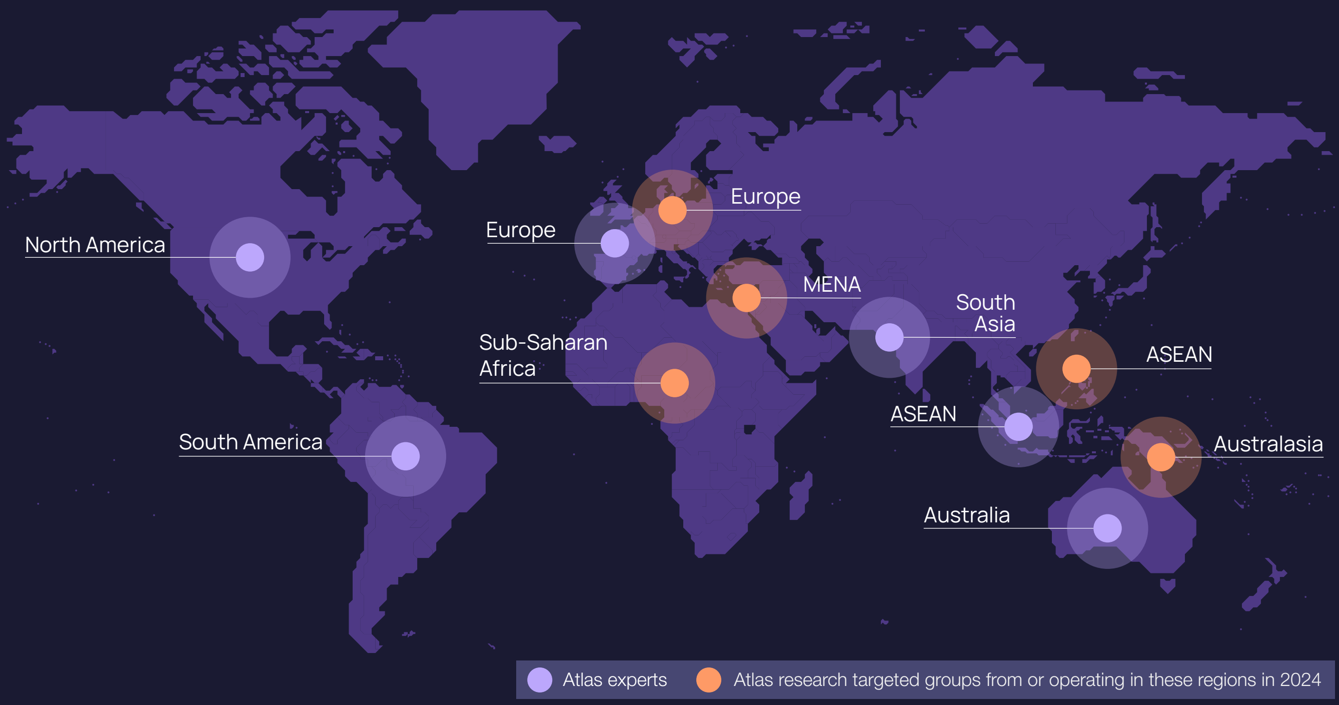
Where does the Cybercrime Atlas operate?

The Cybercrime Atlas community includes experts in investigations, cybersecurity research, cyberthreat intelligence, engineering and research governance from across the globe. Cybercrime Atlas research targets are transnational groups with multiple centres of operation.

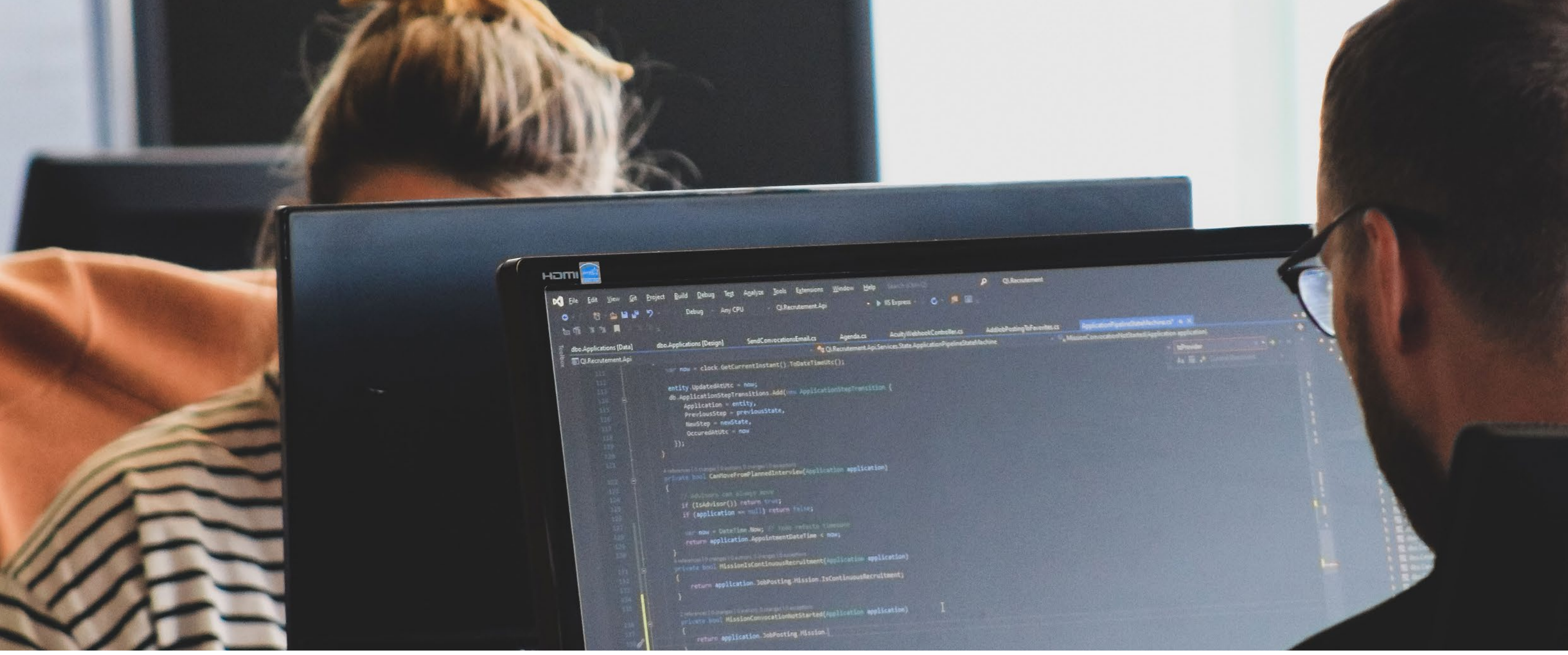
Figure 3 contains a snapshot of the regions from which the Cybercrime Atlas drew expertise in 2024. It also shows the geographical spread of cybercrime groups researched in the Cybercrime Atlas' first year of operations.

FIGURE 3 Cybercrime Atlas: areas of operations

Atlas draws on expertise from around the world and targets cybercrime globally



Source Cybercrime Atlas



How does the Cybercrime Atlas work?

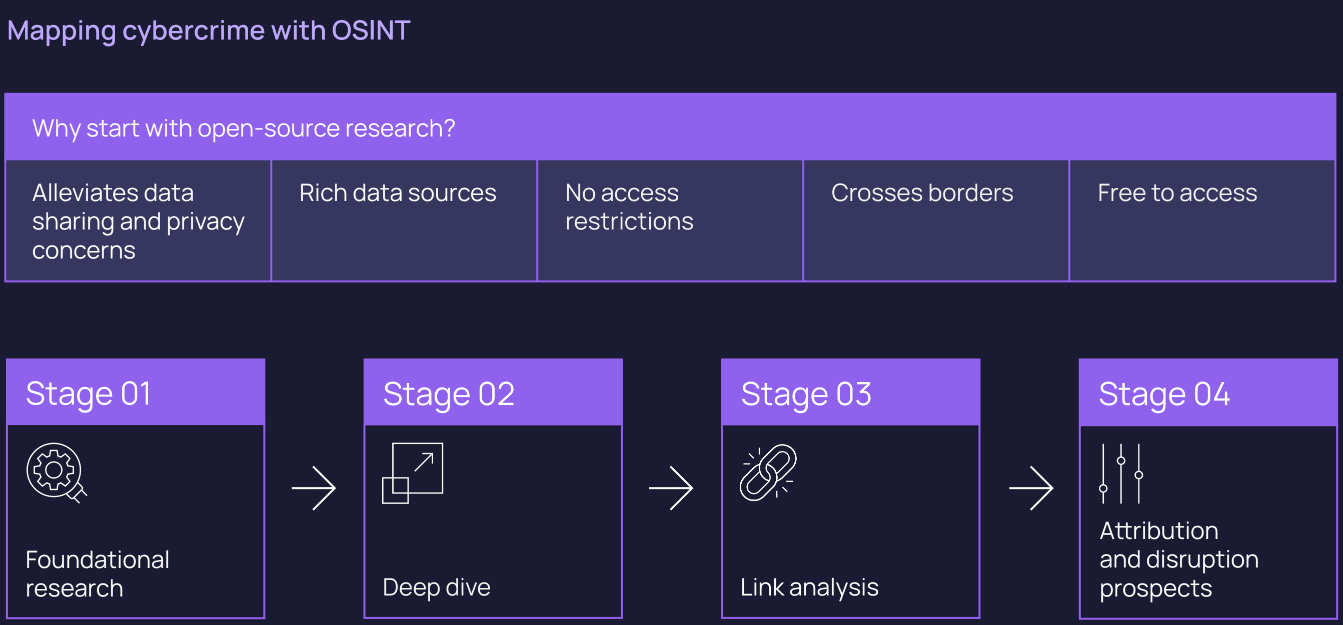
Open-source intelligence

Cybercriminals share and sell information freely, while cyber defenders face the challenge of gathering data scattered across organizations and jurisdictions. Additionally, factors such as commercial sensitivity, protection of privacy and other legal requirements can make it difficult for cyber defenders to share information, limiting efforts to create friction for cybercriminals.

The Cybercrime Atlas' decision to rely on open-source intelligence (OSINT) alleviates several of these challenges:

- OSINT reduces data-sharing and privacy concerns.
- OSINT includes many rich data sources.
- OSINT facilitates collaboration between experts in different countries.
- OSINT allows the Cybercrime Atlas community to tap into a diverse group of experts, helping to build a more complete understanding of cyberthreats and criminal activities.

FIGURE 4 **Atlas mapping: start with open-source research**



Mapping cybercrime with OSINT

Why start with open-source research?				
Alleviates data sharing and privacy concerns	Rich data sources	No access restrictions	Crosses borders	Free to access

Stage 01 → Stage 02 → Stage 03 → Stage 04

Stage 01: Foundational research

Stage 02: Deep dive

Stage 03: Link analysis

Stage 04: Attribution and disruption prospects

Disruption: Identifying "choke points" in criminal infrastructure and activities

As Cybercrime Atlas research builds out, the information collected will identify where criminals are most vulnerable to disruption by highlighting single points of failure or "choke points" in their activities.[5]

This can support cyberthreat mitigation by participating organizations and identify opportunities for collective disruption of cybercriminal activities in partnership with the public sector.

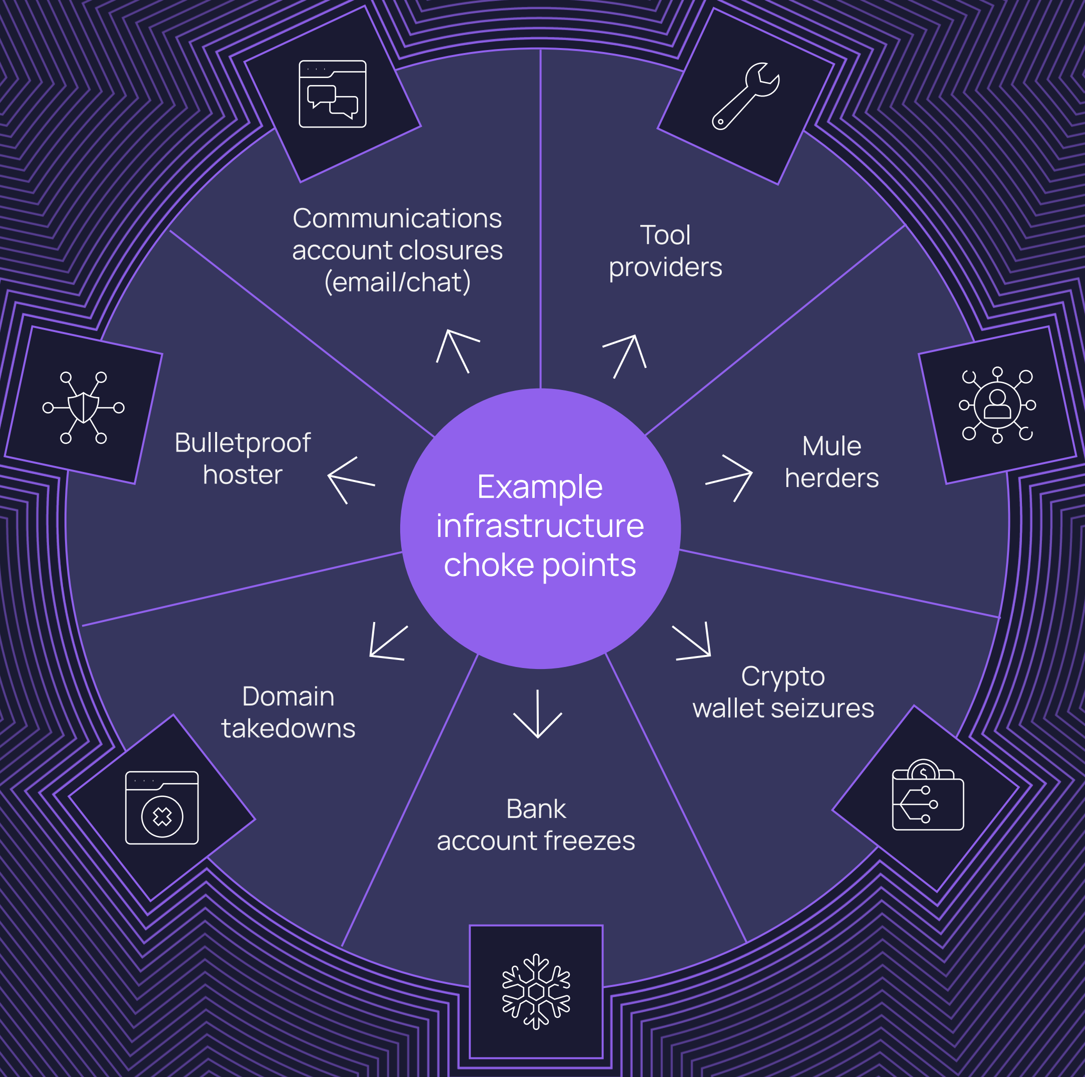
FIGURE 5 **Disruption: use Atlas research to drive collaboration**

Disruption model

Collaborative use of Atlas findings supports disruption of cybercrime

Atlas research helps identify:

Choke points in the criminal ecosystem	Opportunities for **collective disruption** of cybercriminal activities by Atlas participants	Opportunities for **threat mitigation** by Atlas participants	Opportunities for **collaboration** with the public sector



04

The Cybercrime Atlas community

The Cybercrime Atlas is driven by its community, and its growth in 2023-2024 is encouraging.

Cybercrime Atlas grantors

FORTINET

Microsoft

PayPal

Santander

The Cybercrime Atlas community includes

BINANCE

cfc

coinbase

CONINSEC CONSULTING INVESTIGATION SECURITY

Constellation Cyber

CDA CYBER DEFENCE ALLIANCE

ING

INTEL471

SAYARI

TREND MICRO

TeamViewer

W/TH secure

wmc GLOBAL

The Cybercrime Atlas is powered by

Kasm TECHNOLOGIES

MALTEGO

Resecurity

SAPPER LABS

SHADOWDRAGON

SpyCloud

05

Selected community voices

> Disruption of criminal activity made with the support of collaborative research from the Cybercrime Atlas demonstrates the power of public and private collaboration to make the world a safer and more sustainable place. This clearly demonstrates how we can move quickly and effectively together in a unified and coordinated effort to impactfully disrupt these cybercriminal ecosystems. These disruptions create friction and send a message to cybercriminals – and this is just the beginning.
>
> Derek Manky
> Chief Security Strategist and Global Vice-President, Threat Intelligence, FortiGuard Labs

> The Cyber Defence Alliance is an international coalition of action fighting for a better digital future. Nobody is going to gift this future to us. We are focused on achieving impact against the threat actors and networks, who seek to undermine our digital prosperity and societies. Contributing to the Cybercrime Atlas project alongside like-minded individuals and organizations is completely consistent with our missions.
>
> Craig Rice
> Chief Executive Officer, Cyber Defence Alliance

> The Cybercrime Atlas has provided a real-world example of how a model of open-source intelligence gathering combined with operational collaboration can have a meaningful impact in tackling the global threat posed by cybercrime. By working together across sectors, we are showing what industry can do to help to make the internet a safer place.
>
> Jen Silk
> Senior Director, Office of the CISO, PayPal

> I think that the biggest strength is the genuine collaborative nature of everyone within the group. There are so many experts in fields that I have little to no experience in that are more than happy to jump in and help/teach through a situation.
>
> Member of the Cybercrime Atlas Research & Investigations Group[6]

> The results we're seeing underscore that public-private collaboration is effective in the fight against cybercrime. We must continue to cooperate, and we encourage others to join the Atlas initiative as we go after malicious actors and hold them accountable.
>
> Amy Hogan Burney
> General Manager, Cybersecurity Policy & Protection, Microsoft

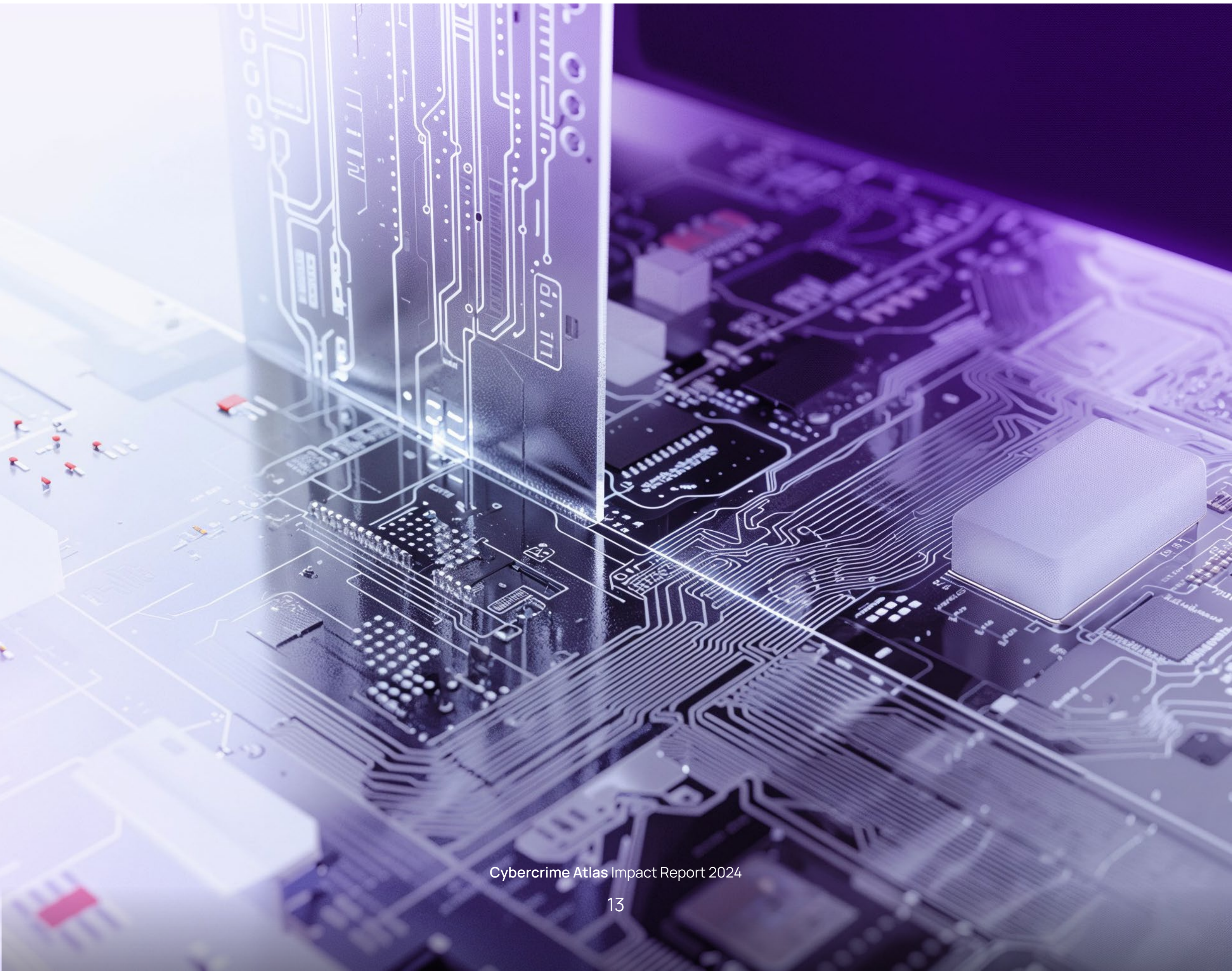
> [What makes the Cybercrime Atlas effective is] diversity of the team. Wide-ranging expertise and knowledge. Differing viewpoints and approaches, diversity of thought. The general quality of the people involved, their willingness to do the work to fight cybercrime.
>
> Member of the Cybercrime Atlas Research & Investigations Group[7]

> The Cybercrime Atlas is a group that has brought together many skilled researchers with diverse expertise to investigate cybercriminals and identify the real actors behind cybercrimes. The group focuses heavily on technical investigations and provides researchers with the opportunity to use their skills during these investigations.
>
> Member of the Cybercrime Atlas Research & Investigations Group[8]

> “Protecting IT ecosystems requires both robust cyber defence measures and effective legal actions against attackers. Cyber defence is crucial for continuous protection, but legal tools and law enforcement actions are essential and cost-effective to efficiently prevent future attacks and dismantle criminal networks. However, the rapidly evolving nature of cybercrime, the volume of victim reports and other challenges faced by law enforcement, including retaining skilled government investigators, necessitate support from various initiatives from industry and academia for a safer internet and future. Moreover, industry partners are playing a critical role by identifying and contributing to investigative areas where law enforcement may lack full oversight. This is what Atlas is all about.
>
> Member of the Cybercrime Atlas Research & Investigations Group[9]

> “[The Cybercrime Atlas is] a focused and enthusiastic group of investigators and information security professionals working together in a focused and pragmatic way against selected threat actors.
>
> Member of the Cybercrime Atlas Research & Investigations Group[10]

> “Cybercriminals have the battlefield advantage: it’s easier to attack than to defend, as defending requires more effort and resources. Therefore, the public and private sectors must act together to develop collective cyberthreat intelligence and detection sharing, security and technology and coordinated incident response mechanisms. By joining forces and creating concrete channels for collaboration, we can make a decisive shift in the fight against cybercrime.
>
> Hazel Diez Castaño
> Chief Information Security Officer, Banco Santander



06

The value of engaging in the Cybercrime Atlas

Cybercrime Atlas participants collaborate with leading experts and law enforcement, gaining skills and helping disrupt cybercrime.

Gain a systemic understanding of cybercrime

Organizations participating in the Cybercrime Atlas have benefitted from an improved understanding of how cybercrime groups operate as well as opportunities to disrupt the cybercrime groups that target their sectors and their clients. This can enhance the security of participating organizations, their wider supply chain, their clients and ordinary citizens.

Improve the skills of your expert staff

Experts assigned to support the Cybercrime Atlas benefit by building their skills alongside some of the world's top cybercrime researchers, investigators, threat-intelligence experts, engineers and governance experts. Peer-to-peer learning is cited by the Atlas research community as one of the core benefits of engaging in the initiative.

Improve collaboration with public-sector stakeholders

The Cybercrime Atlas, hosted by the World Economic Forum, provides an impartial platform for collaboration across industry and between industry and the public sector. Participants have the opportunity to collaborate with leading law enforcement agencies.

Through its connection to the World Economic Forum's Partnership Against Cybercrime, the Cybercrime Atlas' work also facilitates evidence-based policy recommendations that support anti-cybercrime operations and ecosystem-wide cybersecurity.

Demonstrate effective corporate social responsibility

Several organizations in the community include their contribution to the Cybercrime Atlas within their corporate social responsibility (CSR) reporting. Community members are also encouraged to speak about their role in the Cybercrime Atlas at approved external events.

Engage in the Cybercrime Atlas:

The Cybercrime Atlas accepts new participants based on their expertise, capabilities and the completion of a vetting process.

The community can benefit from the following:

- Open-source cybercrime investigators
- Systems and tools to support Cybercrime Atlas research
- Experts in investigative governance, processes and procedures
- Data resilience experts
- Solutions architects
- Legal, policy and regulatory experts.

07

Cybercrime Atlas outlook

Research scope will expand, peer-to-peer learning opportunities will grow and new strategies to disrupt cybercrime will be tested.

The Cybercrime Atlas is driven by its community's commitment to making the internet safer for society, citizens and organizations. Tackling cybercrime requires collaboration between the public and private sectors; without private sector input, stopping cybercrime is impossible. The trust built across organizations through ongoing collaboration has made the Cybercrime Atlas effective.

The diverse capabilities of the Cybercrime Atlas community create friction at every stage of criminal activity, raising the risk of detection and lowering criminals' return on investment.

The next phase

The next phase will expand Cybercrime Atlas research and create more opportunities for community members to share expertise and test ways to undermine cybercriminal activities.

Partnerships with the public sector have extended Cybercrime Atlas activities beyond the community, supporting broader public interest. The openness to experimentation from organizations like INTERPOL has been appreciated. Cybercrime Atlas engagement with Europol is at an exploratory phase, and Europol's openness to collaboration is highly valued. The Cybercrime Atlas will continue to innovate in collaborating with the public sector in 2025.

The Cybercrime Atlas' first policy recommendations are expected to be published at the World Economic Forum's Annual Meeting on Cybersecurity in November 2024, developed in collaboration with the Partnership Against Cybercrime. These recommendations are set to be tested and implemented in 2025. To succeed, the Cybercrime Atlas will evolve by scaling up joint research, diversifying research types and using new tools. These enhancements will support a broader range of anti-cybercrime activities and policy development, requiring gradual adaptation of processes, governance and participation structures.

Contributors

World Economic Forum

Seán Doyle
Lead, Cybercrime Atlas Initiative, World Economic Forum

Tal Goldstein
Head of Strategy and Policy, Centre for Cybersecurity,
World Economic Forum

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

Acknowledgements

The Cybercrime Atlas community

Our deepest thanks to the researchers, investigators, engineers and governance experts from the Cybercrime Atlas community. They are at the heart of its success. These experts come from organizations in the Cybercrime Atlas community but also include vetted individuals from the wider information security community who use their time and knowledge for the common good. For operational security reasons, they cannot be named or pictured in this report, but they are the driving force behind the successes highlighted here.

Production

Laurence Denmark
Creative Director, Studio Miko

Martha Howlett
Editor, Studio Miko

Charlotte Ivany
Designer, Studio Miko

Endnotes

1. World Economic Forum. (2023). *Cybercrime and Violent Crime are Converging: here's how to deal with it.* https://www.weforum.org/agenda/2023/10/cybercrime-violent-crime/.

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

3. Martin, Alexander. (2023, September). *UK logistics firm blames ransomware attack for insolvency, 730 redundancies.* The Record. https://therecord.media/knp-logistics-ransomware-insolvency-uk.

4. World Economic Forum. (2023, January) *Forum-hosted Cybercrime Initiative to Boost Coordination Between Private Sector and Law Enforcement* [Press release]. https://www.weforum.org/press/2023/01/forum-hosted-cybercrime-initiative-to-boost-coordination-between-private-sector-and-law-enforcement/.

5. Harvard Business Review. (2023, June). *How Global Information Sharing Can Help Stop Cybercrime.* https://hbr.org/2023/06/how-global-information-sharing-can-help-stop-cybercrime.

6. Identity anonymized to maintain operational security.

7. Identity anonymized to maintain operational security.

8. Identity anonymized to maintain operational security.

9. Identity anonymized to maintain operational security.

10. Identity anonymized to maintain operational security.

Cybercrime Atlas

Hosted at the **World Economic Forum**