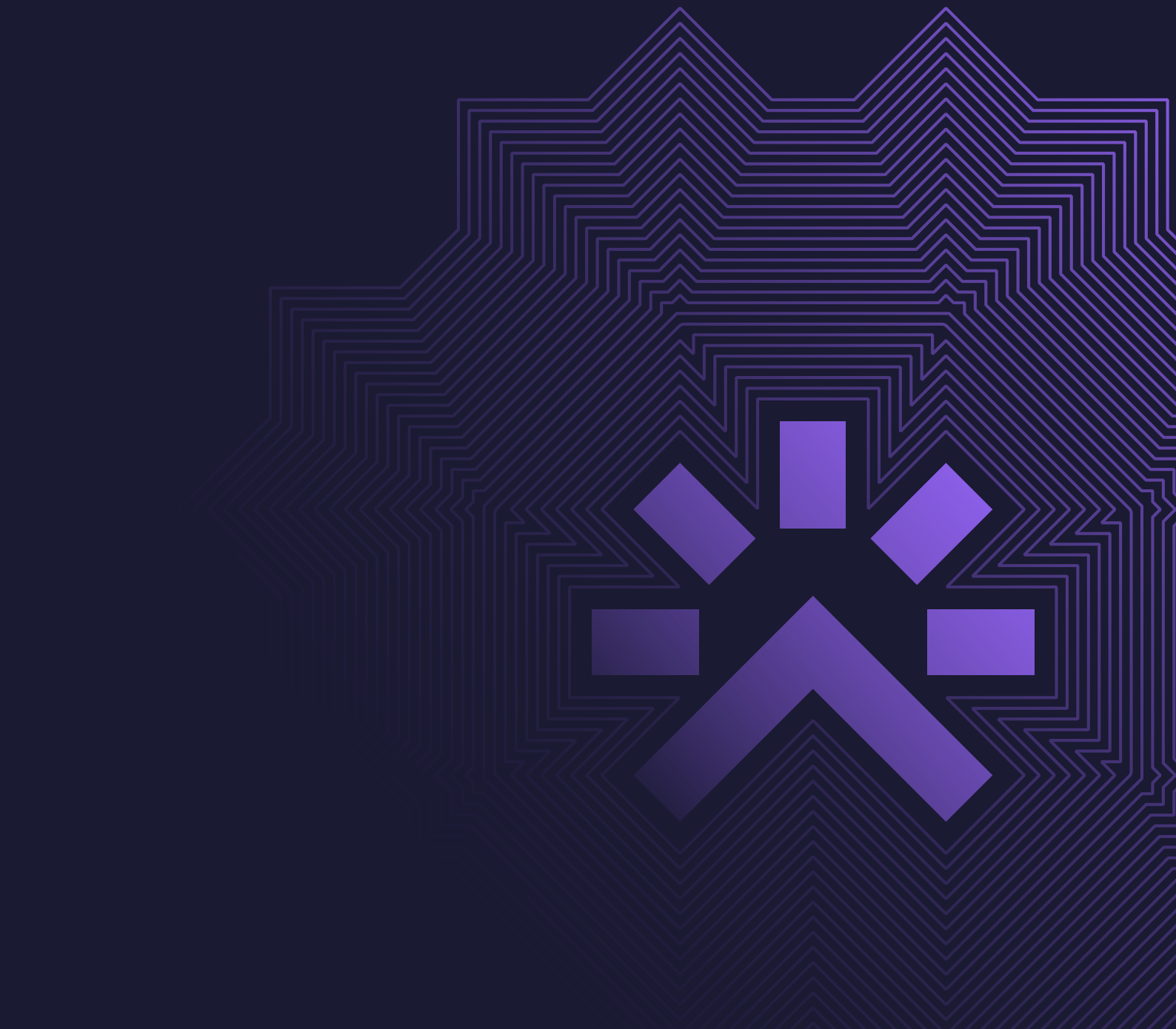
Cybercrime Atlas

Hosted at the **World Economic Forum**

Cybercrime Atlas: Impact Report 2025

OCTOBER 2025



Images: Getty Images, Adobe Stock

Contents

Executive summary	**3**
01 Vision and mission	**4**
02 Cybercrime Atlas outcomes	**5**
03 About the Cybercrime Atlas	**8**
04 The Cybercrime Atlas community	**18**
05 The value of engaging in the Cybercrime Atlas	**22**
Conclusion	**23**
Contributors	**24**
Endnotes	**25**

Executive summary

The second year of the Cybercrime Atlas shows the impact of taking a systematic approach to the disruption of cybercrime.

An effective model of collaboration

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

Since the first *Cybercrime Atlas Impact Report 2024*, the Cybercrime Atlas community has progressed from delivering research to applying it to the disruption of cybercrime networks at scale.

Cybercrime Atlas research has consequences for criminals

In 2024-2025, the Cybercrime Atlas was a partner for operations Serengeti and Serengeti 2.0,[1] two major cross-border actions coordinated by the International Criminal Police Organization (INTERPOL) and the African Union Mechanism for Police Cooperation (AFRIPOL).

Each of these operations was high-impact, leading to arrests, infrastructure confiscations and asset seizures. Satisfyingly, there was a clear deepening of the disruption to criminals' infrastructure, funding and ability to evade arrest from one operation to the next.[2]

The increase in the Cybercrime Atlas's impact was facilitated by a gradual expansion of expert participation in the community, including an expansion into Latin America and Asia Pacific, and a wider range of specialist tool providers. This increased the diversity of expertise and skills, enhancing research and the community's ability to act on it. Findings from 2024-2025 suggest that there truly is strength in diversity of expertise once structures are in place to harness it.

Accelerating collaboration

Lessons learnt from the Cybercrime Atlas community contributed heavily to the recommendations of the World Economic Forum Partnership Against Cybercrime's *Disrupting Cybercrime Networks: A Collaboration Framework*.[3]

Based on this Partnership Against Cybercrime framework, the Cybercrime Atlas community built and delivered pre-operation training to cybercrime unit commanders, prosecutors and policy-makers on harnessing non-government expertise. This has supported public-sector decision-makers across more than 40 countries in Asia, South-East Europe and the Americas, and strengthened communication channels between private- and public-sector organizations in these regions.

Cybercrime Atlas partnership with the public sector

The Cybercrime Atlas's public-sector relationships rely on hubs of expertise such as INTERPOL's Cybercrime Directorate in Singapore and the European Cybercrime Centre (EC3) at Europol. These relationships matured in 2025, with joint training of operational anti-cybercrime leaders with INTERPOL and regular participation by the Cybercrime Atlas in advisory groups at EC3.

Launching the Cybercrime Atlas Research and Mapping group

Another milestone was the launch and development of Cybercrime Atlas Research and Mapping, an applied research group. The group works to understand the intricate web of infrastructure tools and services used by cybercriminals and applies this knowledge to identify critical choke points whose disruption would have long-lasting impact.

The Cybercrime Atlas consistently creates new and actionable insights into cybercrime networks, but insights are only the beginning of how it creates value. The Cybercrime Atlas relies on its community's ability to act on joint research. The new Research and Mapping group facilitates evidence-based selection of targets for disruptive operations, creates insights that support policy recommendations, enriches the cybersecurity community's knowledge of the cybercrime landscape, and supports prevention and mitigation strategies. Mutual understanding and trust between partners accelerate operations.

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, supporting systematic mitigation and disruption of cybercrime. The community collaborates to:

- **Map** the landscape, criminal operations, networks and infrastructure using open-source intelligence (OSINT)
- **Use** this research to enable coordinated disruption of cybercriminal activities and infrastructure
- **Shape** the online environment by creating evidence-based recommendations to make it safer

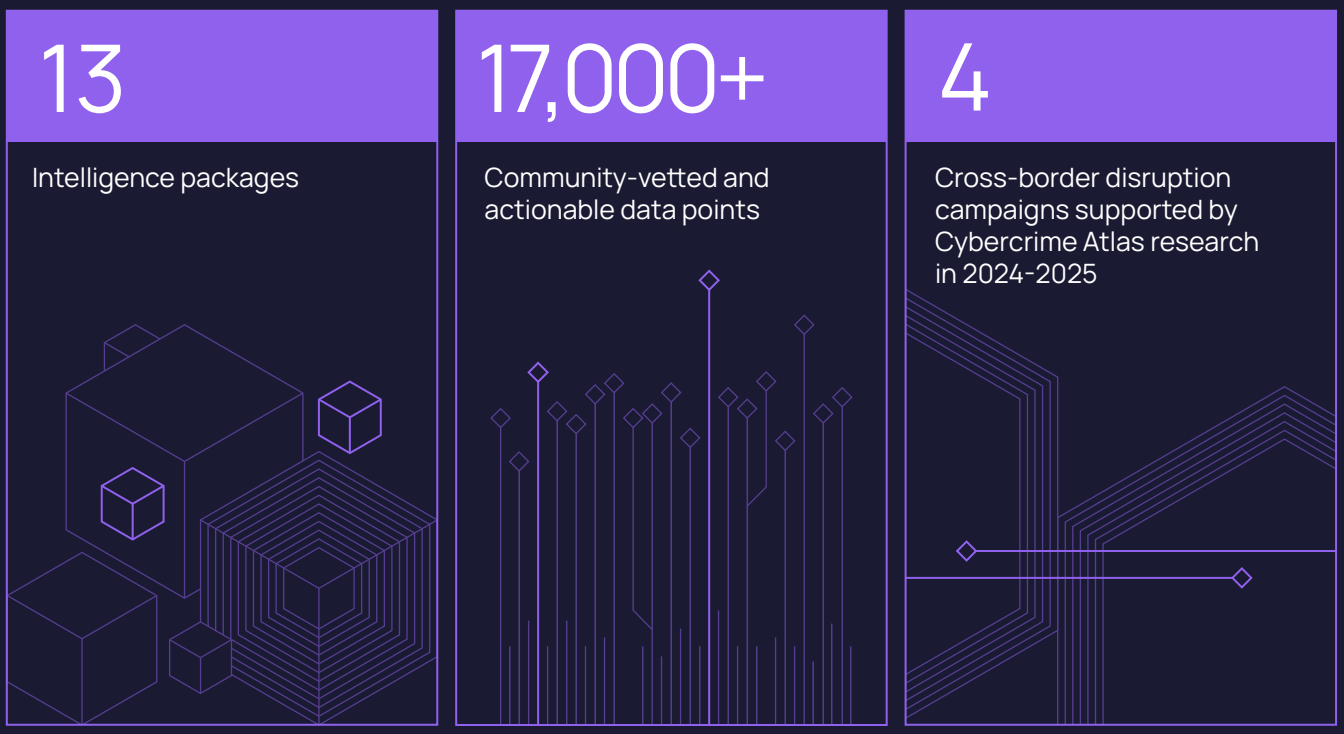
02

Cybercrime Atlas outcomes

Cybercrime Atlas research, developed by global experts, delivers actionable insights with impact at scale and across regions.

FIGURE 1 **Cybercrime Atlas outcomes by October 2025**

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.



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.

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.

The Cybercrime Atlas creates impact

> 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 Chief Information Security Officer, PayPal

Supporting disruption of cybercrime networks, operations Serengeti and Serengeti 2.0

The Cybercrime Atlas was named by the International Criminal Police Organization (INTERPOL) as an operational partner in the Serengeti and Serengeti 2.0 series of cybercrime disruptions that took place across 19 countries in Africa.

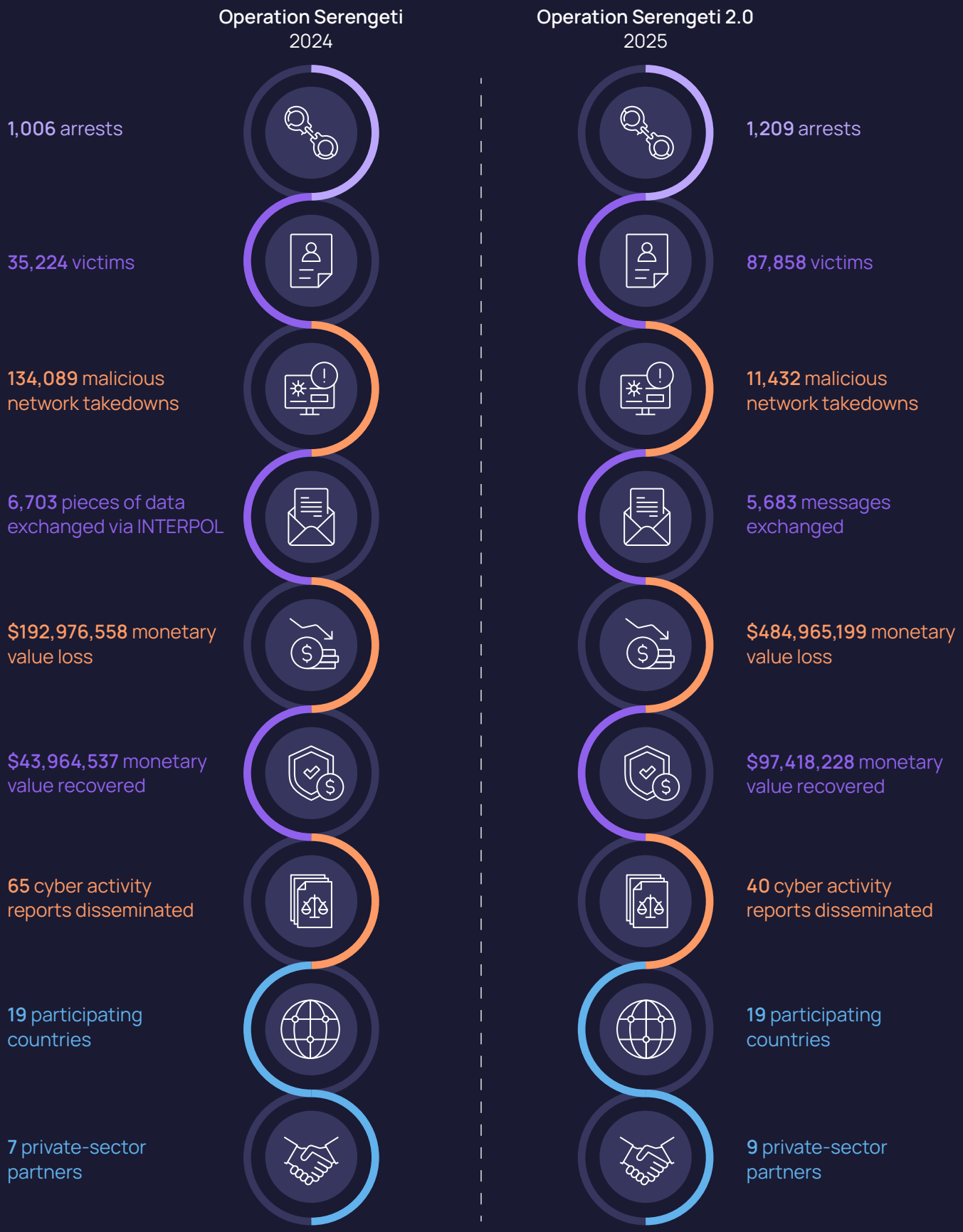
The cumulative effect of these operations, coordinated by the African Union Mechanism for Police Cooperation (AFRIPOL) and INTERPOL, shows how industry collaborations, civil society experts, academia, and partnerships between the public sector and experts from the private sector can destabilize criminal networks.

The Serengeti operations targeted criminal groups that had impacted more than 100,000 victims. The operations disrupted criminals' technical and physical infrastructure, such as cryptocurrency mining equipment and electricity generators, seized $140 million in funds suspected to be from criminal activities and undermined the personal networks of trust that help cybercriminals collaborate.

Hard drives, cryptocurrency mining equipment and illicit power stations were seized during the INTERPOL- and AFRIPOL-led Operation Serengeti 2.0 in August 2025.

FIGURE 2 **Operation Serengeti**

Empowering law enforcement and partners to disrupt cybercrime networks across Africa



Source International Criminal Police Organization (INTERPOL).

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 with the support of a grant from Fortinet, Microsoft, PayPal and Banco Santander, 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- 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 ecosystem is vastly complex, and INTERPOL values its partnerships with the World Economic Forum and the Cybercrime Atlas as we navigate this landscape together. Collaboratively, we can make connections and share insights involving cyberthreats that otherwise might be missed, resulting in a world that is safer for all.
>
> **Neal Jetton**
> Cybercrime Director, INTERPOL

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[4] and continues to have a close relationship with this world-leading source of expertise in how to tackle cybercrime. This includes applying recommendations from the Partnership Against Cybercrime on how to incentivize, govern and resource collaborations to disrupt cybercrime.

> When we bring together the insights, tools and capabilities of international private- and public-sector partners, we create a force multiplier against cybercrime. The Cybercrime Atlas is helping to turn intelligence into action – and action into accountability. It's an example of how we collectively drive meaningful disruption at scale.
>
> **Steven Masada**
> Assistant General Counsel,
> Microsoft Digital Crimes Unit

Cybercrime Atlas highlights August 2024-September 2025

This section covers publicly disclosed or Traffic Light Protocol (TLP)[5] CLEAR highlights only. The impact of most Cybercrime Atlas research, however, remains TLP AMBER or TLP RED, and is available only to Cybercrime Atlas community participants or the community's partners.

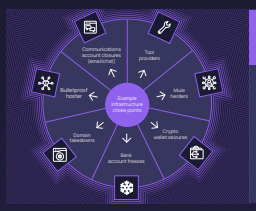
FIGURE 3 **Cybercrime Atlas highlights 2024-2025**

August 2024

UN Office on Drugs and Crime names Cybercrime Atlas in report on best practice in countering cybercrime

October 2024

Cybercrime Atlas first Annual Impact Report



November 2024

Research and Mapping group launched

January 2025

Cybercrime Atlas at World Economic Forum Annual Meeting in Davos 2025

March 2025

Cybercrime Atlas insight sharing at Global Coalition to Fight Financial Crime (GCFFC) Virtual Asset Summit, INTERPOL, Lyon

May 2025

Cybercrime Atlas joins Europol EC3 Advisory Groups to enhance insight sharing

October 2024

Cybercrime Atlas session at the World Economic Forum Annual Meeting on Cybersecurity 2024

November 2024

Disrupting Cybercrime Networks: A Collaboration Framework published

November 2024

INTERPOL Operation Serengeti – Cybercrime Atlas publicly recognized as an operational partner

February 2025

Operation Secure: joint-training with INTERPOL for cybercrime unit commanders – Bangkok, Thailand

April 2025

Joint training at INTERPOL 10th Americas Working Group, Panama

May 2025

Cybercrime Atlas workshop for public-sector agencies' operational collaboration at the Western Balkans Cyber Capacity Centre, Podgorica, Montenegro

Source Cybercrime Atlas.

FIGURE 3 **Cybercrime Atlas highlights 2024-2025** (continued)

June 2025

Cybercrime Atlas grant extended until June 2027

July 2025

Collaboration Agreement with STOP THE TRAFFIK's Traffik Analysis Hub signed – supports research into cyber-scam farms

September 2025

Underground Economy Conference, Council of Europe and Team Cymru Live threat hunt and first in-person researcher meeting

June 2025

Annual Strategy Review and in-person meeting at Partnership Against Cybercrime, London, UK

August 2025

INTERPOL Operation Serengeti 2.0

October 2025

Cybercrime Atlas at World Economic Forum Annual Meeting on Cybersecurity 2025, Dubai

Source Cybercrime Atlas.

What does the Cybercrime Atlas target?

In 2024-2025, the Cybercrime Atlas continued to focus its research on financially motivated cybercriminal groups and their methods. Research into state-controlled or state-sponsored 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 the potential to disrupt cybercriminal activities that harm society. This includes cases in which 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.
Driving 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.

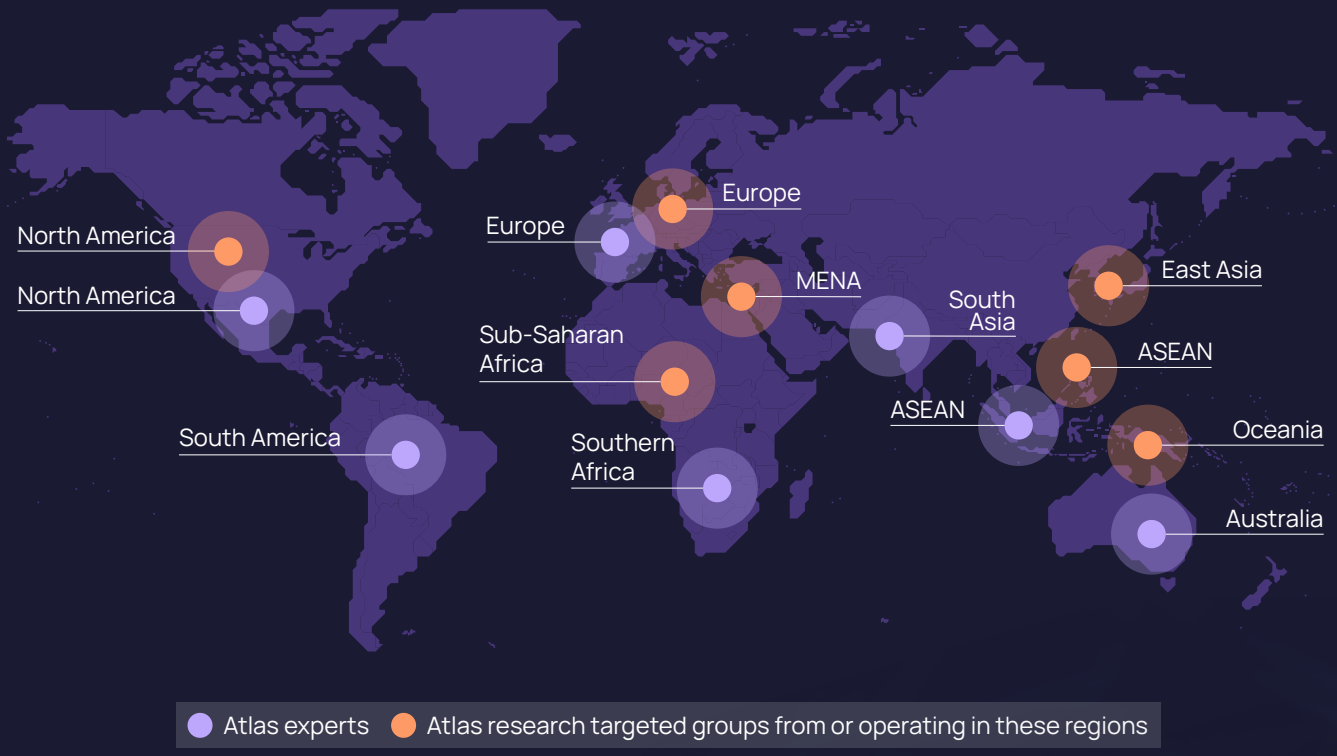
Where does the Cybercrime Atlas operate?

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 4 contains a snapshot of the regions from which the Cybercrime Atlas drew expertise in 2024-2025. It also shows the geographical spread of cybercrime groups researched in the Cybercrime Atlas's first year of operations.

FIGURE 4 **Cybercrime Atlas: areas of operations**

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



Source Cybercrime Atlas.

> We must address the continued global proliferation of cybercrime head-on. We need to hold cybercriminals accountable for their crimes, systemically at scale. Effectively halting cybercrime requires a global and collaborative approach. By embracing best practices and proven frameworks for anti-adversary partnerships, we can jump-start new and enhance existing initiatives.
>
> **Derek Manky**
> Chief Strategist and Global Vice-President, Threat Intelligence at Fortinet

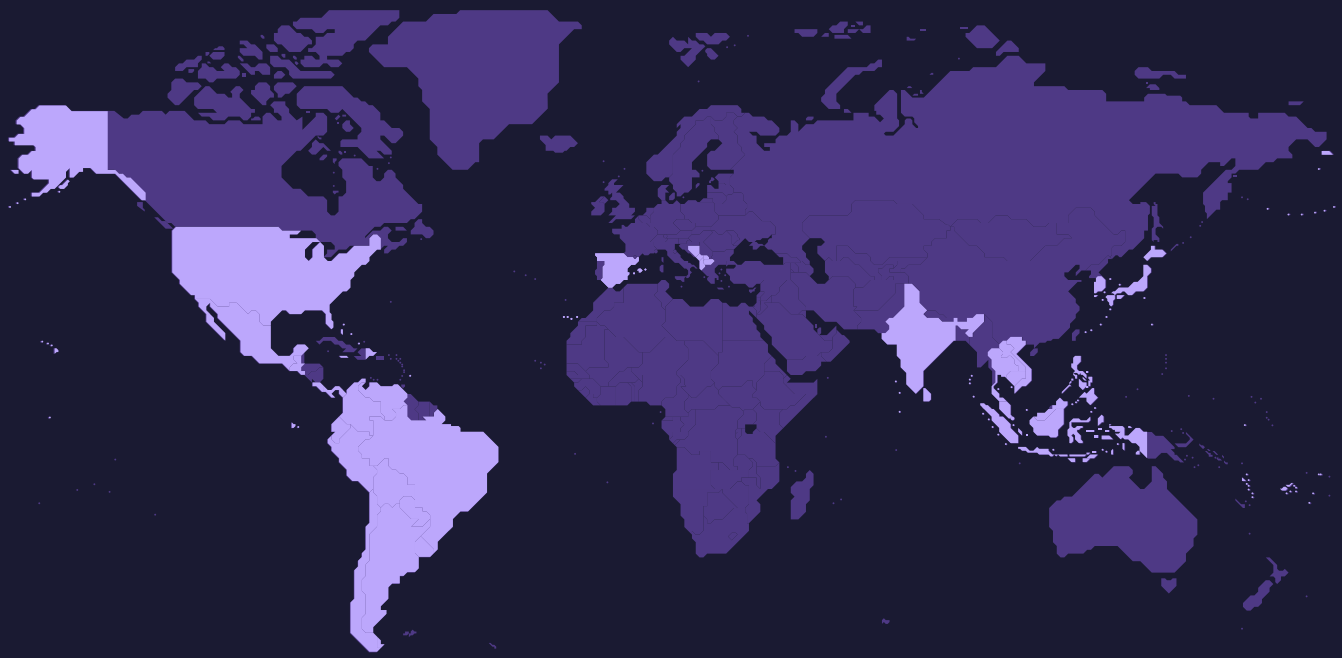
Enhancing operational collaboration through joint training

The Cybercrime Atlas Project Management Office, with support from the Cybercrime Atlas community and the Partnership Against Cybercrime, adapted the World Economic Forum's *Disrupting Cybercrime Networks: A Collaboration Framework* to train Cybercrime Unit commanders and cybercrime prosecutors working with INTERPOL's Cybercrime Directorate.

This was first delivered during preparations for Operation Secure,[6] during which the Asia and South Pacific Desk of INTERPOL's Cybercrime Directorate convened cybercrime unit heads and prosecutors, and anti-cybercrime professionals, from more than 21 countries. INTERPOL and the Royal Thai Police were crucial for hosting this multi-day training and insight-sharing event, which included participants from the the Cybercrime Atlas community.

The training was extended to operational anti-cybercrime leaders from a further 21 countries during INTERPOL's 10th Americas Working Group on Cybercrime for Heads of Unit in Panama City in April 2025.[7] The training was later adapted to support an independent Cybercrime Atlas-led training at the Western Balkans Cyber Capacity Centre in Montenegro in May 2025, supporting discussions on collaboration between law enforcement, computer emergency response teams (CERTS) and private-sector experts from five countries in the region.

FIGURE 5 **Cybercrime Atlas: countries with units participating in Cybercrime Atlas-designed training**



Countries with units participating in Cybercrime Atlas-designed training

Source Cybercrime Atlas.

How does the Cybercrime Atlas work?

> The true value of the Cybercrime Atlas lies not only in collaboration, but in the diversity of perspectives it brings together. Industry, law enforcement and academia each contribute unique insights to the challenge. By fostering cross-border, cross-sector public-private collaboration, we can turn fragmented knowledge into actionable intelligence, disrupt cybercrime more effectively and strengthen the collective resilience needed to protect society as a whole.
>
> **Hazel Diez Castaño**
> Chief Information Security Officer, Santander

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's decision to rely on OSINT alleviates several of these challenges:

- Reduces data-sharing and privacy concerns
- Includes many rich data sources
- Facilitates collaboration between experts in different countries
- 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 6 **Atlas research: start with open source intelligence (OSINT)**

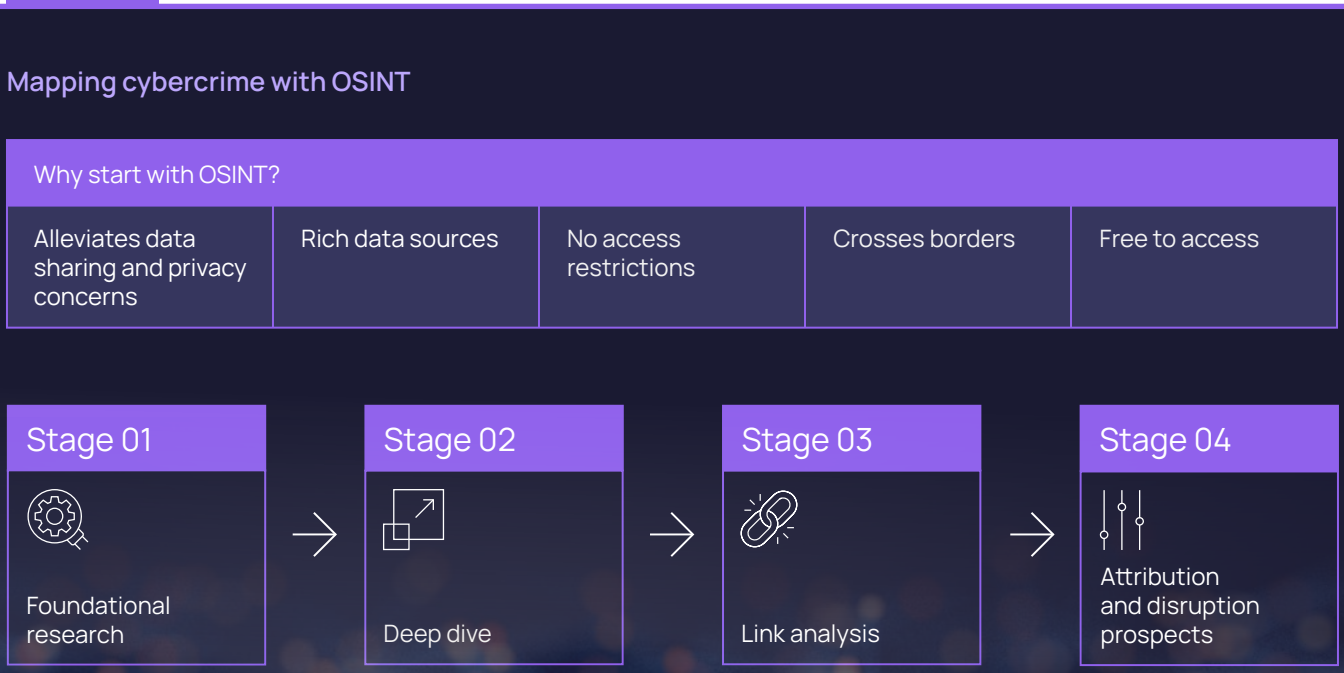


FIGURE 7 **Cybercrime Atlas mapping: applied research**

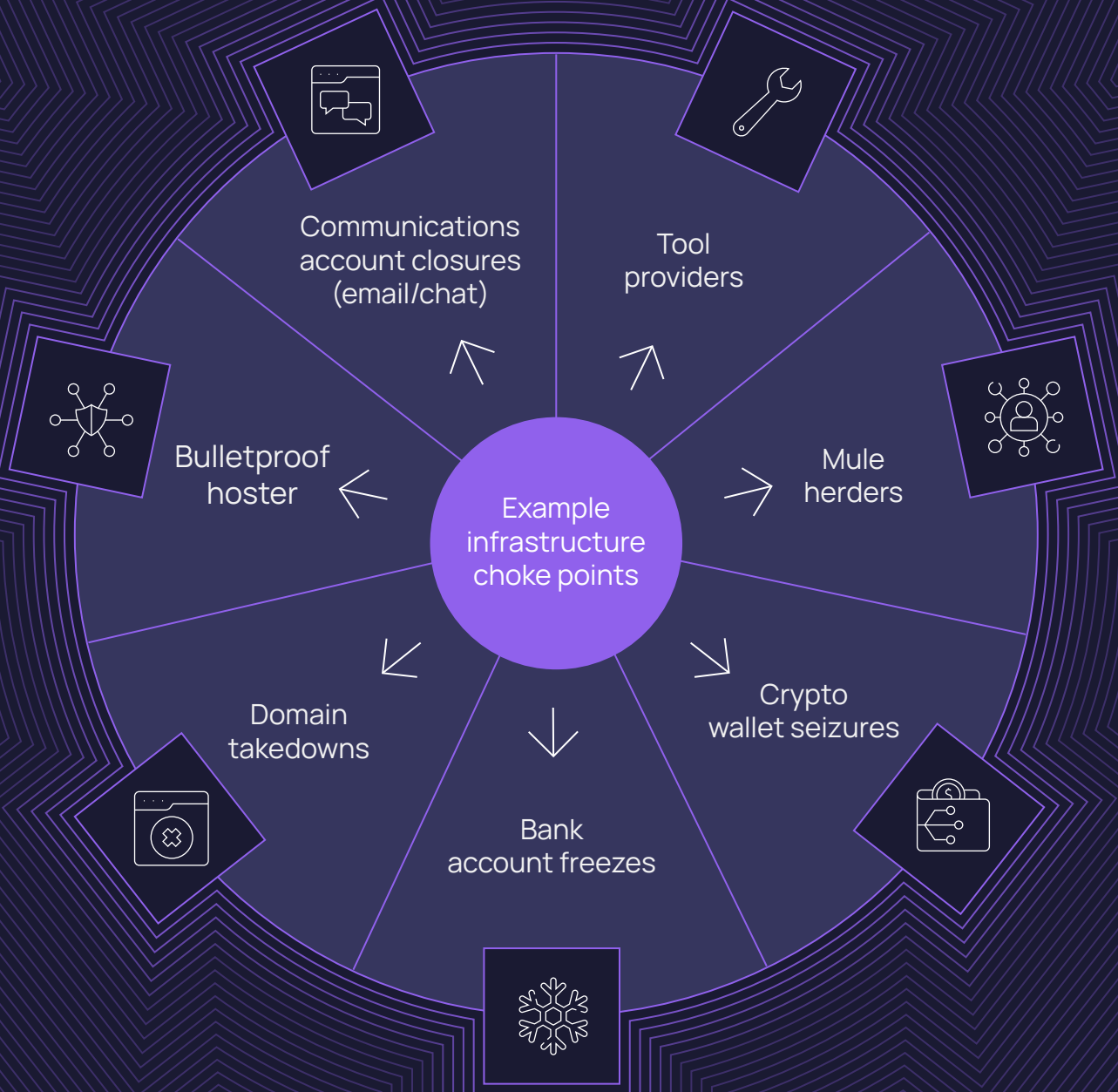
The Cybercrime Atlas

Mapping the cybercrime ecosystem

Cybercrime operates as a collaborative ecosystem, underpinned by specialized providers and enablers

It is important to understand cybercrime's intricate web of infrastructure tools and services

Cybercrime Atlas's goal is to identify critical choke points to obtain long-lasting disruption



Source Cybercrime Atlas.

In November 2024, the Cybercrime Atlas launched an applied research group known as Cybercrime Atlas Research and Mapping.

This began with a core group drawn from Banco Santander, Group-IB, Binance and OrangeCyberDefence. In the second half of 2025, this expanded to include Mastercard, Recorded Future, Lemon Cash, SpyCloud and Scitum, and applied research institutions like TNO Nederlands.

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.[8]

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

FIGURE 8 **Disrupting cybercrime networks collaboration framework**

Source World Economic Forum. (2025). *Disrupting Cybercrime Networks: A Collaboration Framework.*

BOX 3 **Governing the Cybercrime Atlas collaboration: balancing formal and informal structures**

Cybercrime Atlas participants collaborate to build a shared understanding of cybercriminal networks using OSINT. This information then supports community members in creating friction across cybercriminal activities and supports action by public-sector agencies. Participants come from different regions, different types and sizes of organization, or both because of their individual expertise. This mix of skills, cultures and legal contexts requires a balance between strict governance of some areas of activity and significant flexibility in others, so that participants can continue to collaborate despite their differences.

For example, the starting point for Cybercrime Atlas 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 able to start research while relying on already-accepted standards for information classification, such as the TLP. This allowed the Cybercrime Atlas community to build rules around the needs and activities of the community as it developed.

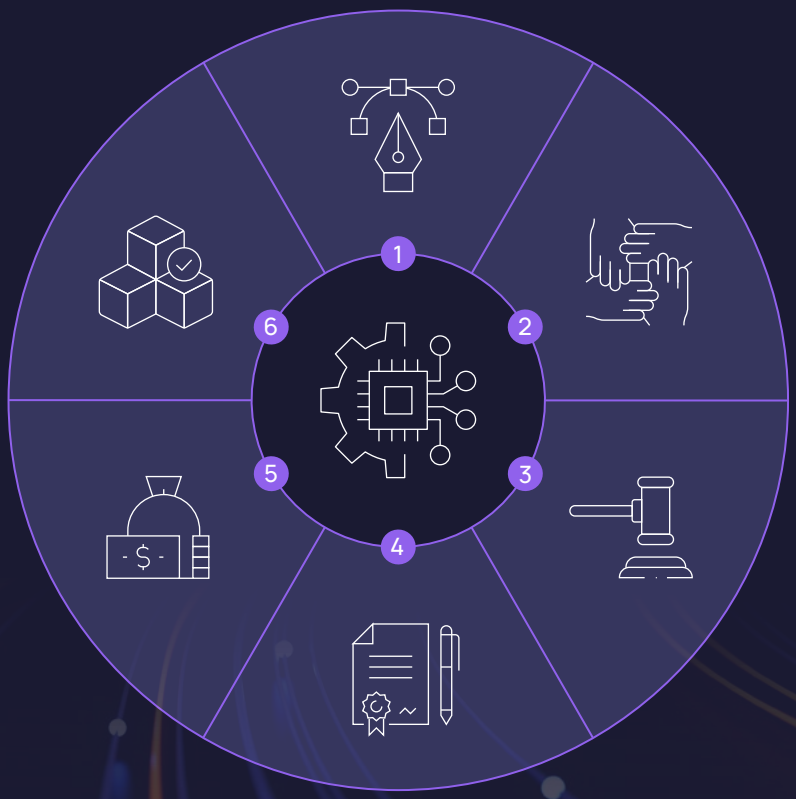
A strong emphasis was put on information security from the outset, but the reliance on OSINT allowed the community to avoid time-consuming deliberations over the legality of sharing information generated by the collaboration between participants. This allowed for speedy set-up and the development of standard operating procedures by the Cybercrime Atlas expert community itself.

FIGURE 9 **Cybercrime Atlas structure: building a global disruption chain**

Insights

Cybercrime Atlas – a platform for collaborative disruption by:

1. Research and development (R&D)/private sector
2. NGO and non-profit
3. Law enforcement
4. Policy experts
5. Banking, payments and cryptocurrency
6. Cybersecurity vendors



04

The Cybercrime Atlas community

The Cybercrime Atlas has grown from 22 participating organizations in 2023-2024 to more than 30 participants in 2024-2025.

Cybercrime Atlas grantors

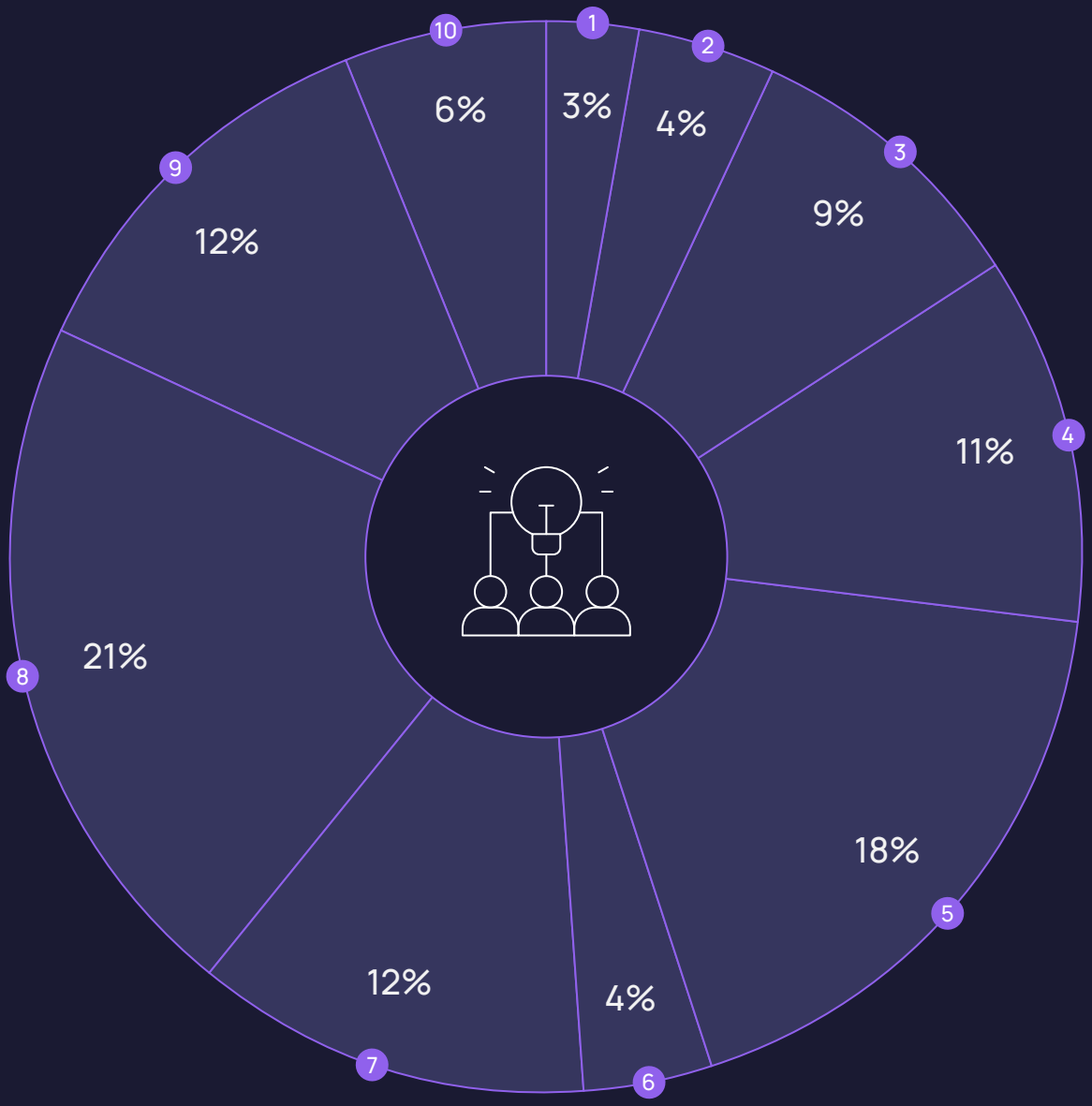
The Cybercrime Atlas community includes

The Cybercrime Atlas is powered by

Source Cybercrime Atlas.

FIGURE 10 **Diversity is strength: new insights through collaboration**

Example: Top 10 contributing companies in April-May 2025 (investigations snapshot)



1	Domain name system specialist	3%	6	OSINT investigations tool provider	4%
2	Corporate intel specialist	4%	7	Cloud and IT services provider	12%
3	Enterprise security	9%	8	Criminal infrastructure intel	21%
4	Bank	11%	9	Threat intel specialist	12%
5	Hardware security/anti-malware	18%	10	IT consultancy	6%

Source Internal Cybercrime Atlas data.

All experts participating in the Cybercrime Atlas, and the organizations they represent, join based on an assessment of their expertise, insights and role in disrupting cybercriminal activity.

By bringing these diverse capabilities and skills together, the Cybercrime Atlas community contributes new insights. The impact goes beyond what participants can create by working in isolation.

This is demonstrated in Cybercrime-Atlas supported disruptions like the INTERPOL-led Operation Serengeti and 2.0. For example, Fortinet, Trend Micro and Group-IB[9] provided individual support to the operations but are also members of the Cybercrime Atlas community and research groups that contributed insights to these operations.

Focus on tooling

Cybercrime Atlas research and impact have been enhanced through support from specialist tool providers. The Cybercrime Atlas community collaborates with these organizations based on an assessment of mission alignment and quality.

FIGURE 11 Focus on OSINT tooling

Epieos provides insights into email addresses and phone numbers under suspicion of use by criminal threat actors or their affiliates. It reverses this information into additional insights such as social media accounts, domains, payment platforms used and more.

Kasm is the Cybercrime Atlas's secure workspace provider. Without access to Kasm, Cybercrime Atlas researchers could not start work. Kasm's security has supported onboarding of new experts, allowing them to work swiftly and safely with all needed operational security measures.

Maltego is an OSINT platform that supports Cybercrime Atlas researchers in analysing and visualizing connections across diverse data sources. The partnership with Maltego has allowed Atlas researchers to reliably conduct link analysis and draw new insights from their findings. Additionally, with access to Maltego's Hunchly, Atlas researchers can capture and preserve web data in a structured way to support their investigations.

ShadowDragon Horizon is an intelligence platform used by the Cybercrime Atlas for trusted, ethical information collection and analysis. It enables the identification of social media accounts and the mapping of relationships between online entities worldwide – delivering actionable intelligence to drive informed decisions.

Silent Push provides Cybercrime Atlas researchers with intelligence on malicious technical infrastructure. This supports the identification of criminal IT infrastructure before it is weaponized by cybercriminals. Many of the crimes investigated by the Cybercrime Atlas involve the use of domains as a primary vehicle to lure victims, which is one of several areas in which Silent Push provides Atlas investigators with unique insights.

SpyCloud recaptures identity data stolen in phishing attacks, malware infections, and data breaches directly from criminal networks, enabling proactive threat hunting and criminal attribution. Cybercrime Atlas uses these capabilities for reverse engineering on passwords and obtaining insights into breach data, identifying malicious tools used by threat actors and further datapoints related to criminal actors' additional online accounts.

Cybercrime Atlas law enforcement partnerships

The Cybercrime Atlas is a platform for collaboration between private-sector, academic and non-profit experts. Its success depends on strong partnerships with organizations that act as hubs for collaboration and coordination between law enforcement and civil society.

INTERPOL

INTERPOL's innovative approach to partnerships has created space for the Cybercrime Atlas community to experiment and improve the relevance of its research over time.

The Cybercrime Atlas community provided operationally actionable insights to Operations Serengeti in November 2024 and Serengeti 2.0 in August 2025.

The Serengeti operations involved coordinated action by law enforcement across more than 19 countries in Africa, leading to significant numbers of arrests and the seizure of $140 million in criminal assets linked to crimes of a value totalling $678 million, and impacting more than 120,000 victims.

Operations Serengeti led to the seizure, destruction or re-use of technical infrastructure ranging from hard drives to mobile electricity generators.

Europol

Cybercrime Atlas engagement with Europol deepened in 2024-2025 and now includes insight sharing through participation in advisory groups at Europol's European Cybercrime Centre (EC3) and interactions with the EC3-hosted Joint-Cybercrime Action Task Force (J-CAT).[10]

The value of Europol's openness to collaboration is magnified by EC3's growing role as a hub for public-private insight sharing and collaboration to disrupt cybercrime networks.

The Cybercrime Atlas is also thankful for EC3's engagement in capacity-building training in the wider EU neighbourhood, where EC3 experts supported Cybercrime Atlas-led training for law enforcement, CERTs and policy-makers at the Western Balkans Cyber Capacity Centre in May 2025.

Cybercrime Atlas civil society partnerships

STOP THE TRAFFIK

In mid-2025, the Cybercrime Atlas began a targeted collaboration with **STOP THE TRAFFIK**, which includes data sharing to support Cybercrime Atlas research into cyber scam farms. Cyber scam farms regularly depend on human trafficking and exploitation to secure the workforce needed to carry out large-scale online fraud.

STOP THE TRAFFIK is a UK-based non-profit working to prevent human trafficking worldwide. Through intelligence-led approaches, including hosting of the **Traffik Analysis Hub** (a global technology platform sharing and analysing human trafficking data), STOP THE TRAFFIK works with businesses, financial institutions, governments, vulnerable communities and community partners to identify, disrupt and reduce the risk of human trafficking and exploitation.

This marks the Cybercrime Atlas's first formalized collaboration with an organization outside its core community.

05

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 clients. This can enhance the security of participating organizations, their wider supply chain, their clients and ordinary citizens.

Improve the skills of 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. The Atlas research community cite peer-to-peer research 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 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 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

Conclusion

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 enhance the resources available to Cybercrime Atlas researchers. The Cybercrime Atlas will continue to gradually grow its community of participants. This growth will increase the diversity of skills and disruption capabilities available to the community.

Partnerships with the public sector have extended Cybercrime Atlas activities beyond the community, supporting broader public interest activities such as capacity-building in the public sector and insight-sharing with private-sector partners outside the Atlas community.

To succeed, the Cybercrime Atlas will continue to scale up joint research, diversify research types and harness new tools. These enhancements will support a broader range of anti-cybercrime activities and policy developments, requiring gradual adaptation of processes, governance and participation structures.

Contributors

World Economic Forum

Seán Doyle
Lead, Cybercrime Atlas Initiative,
World Economic Forum

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

Acknowledgements

The Cybercrime Atlas community

We extend 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 include vetted individuals from the wider information security community, which harnesses their time and knowledge for the common good. For reasons of operational security, they cannot be named or pictured in this report, but they are the driving force behind the successes highlighted here.

Production

Louis Chaplin
Editor, Studio Miko

Rose Chilvers
Designer, Studio Miko

Laurence Denmark
Creative Director, Studio Miko

Jay Kelly
Designer, Studio Miko

Endnotes

1. World Economic Forum. (2025). *Cybercrime is borderless. This global bust shows how law enforcement can be too.* https://weforum.org/stories/2025/08/cybercrime-global-collaboration/.

2. Operation Serengeti INTERPOL. (2024). *Major cybercrime operation nets 1,006 suspects.* https://www.interpol.int/en/News-and-Events/News/2024/Major-cybercrime-operation-nets-1-006-suspects; Operation Serengeti INTERPOL. (2025). *African authorities dismantle massive cybercrime and fraud networks, recover millions.* https://www.interpol.int/en/News-and-Events/News/2025/African-authorities-dismantle-massive-cybercrime-and-fraud-networks-recover-millions.

3. World Economic Forum. (2024). *Disrupting Cybercrime Networks: A Collaboration Framework.* https://www.weforum.org/publications/disrupting-cybercrime-networks-a-collaboration-framework/.

4. World Economic Forum Partnership Against Cybercrime: https://initiatives.weforum.org/partnership-against-cybercrime/home.

5. FIRST. (2025). *Traffic Light Protocol (TLP).* https://www.first.org/tlp/.

6. Council of Europe. (2025). *Operation Secure: Strengthening Cybersecurity in Asia and the South Pacific.* https://www.coe.int/en/web/cybercrime/-/operation-secure-strengthening-cybersecurity-in-asia-and-the-south-pacific.

7. INTERPOL "Examining the evolving cybercrime threat landscape in Latin America" 13 May 2025. https://www.linkedin.com/pulse/examining-evolving-cybercrime-threat-landscape-latin-america-6dutf/.

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

9. International Criminal Police Organization. (n.d.). *African authorities dismantle massive cybercrime and fraud networks, recover millions.* https://www.interpol.int/News-and-Events/News/2025/African-authorities-dismantle-massive-cybercrime-and-fraud-networks-recover-millions.

10. Europol. (n.d.). *Joint Cybercrime Action Taskforce (J-CAT).* https://www.europol.europa.eu/how-we-work/services-support/joint-cybercrime-action-taskforce.

Cybercrime Atlas

Hosted at the **World Economic Forum**