Mapping cybercrime: How can the Cybercrime Atlas Cosmos help disrupt digital crime?

weforum.org/stories/2026/05/mapping-cybercrime-how-a-shared-ecosystem-view-can-help-disrupt-digital-crime

Natalia Umansky, World Economic Forum May 12, 2026

Cybersecurity

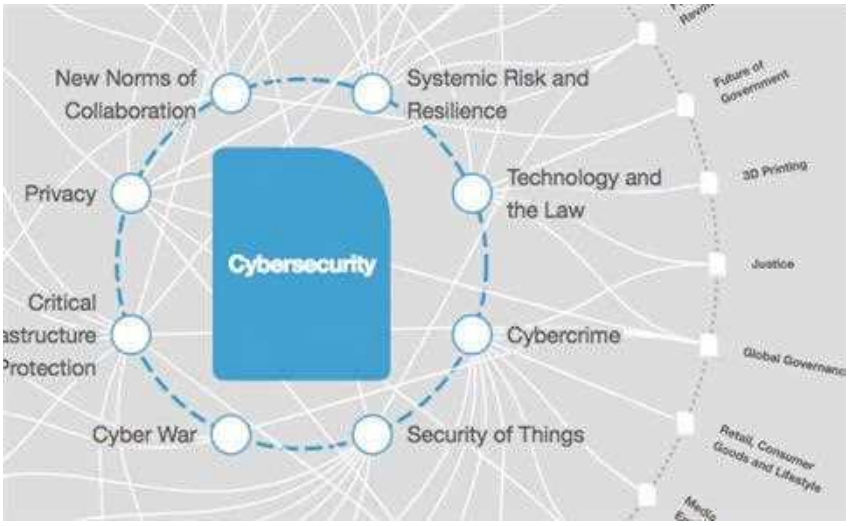
Combatting cybercrime requires multiple players

Image: Pexels/Cottonbro Studios

Natalia Umansky

Project Specialist, Cybercrime Atlas, World Economic Forum

Our Impact



[The Big Picture]

[Explore and monitor how Cybersecurity is affecting economies, industries and global issues]

Stay up to date:

Cybersecurity

- Numerous interdependent players in the cybercrime ecosystem create economies of scale for criminals.
- Given the covert nature of cybercrime operations, greater information and transparency will help combat them.
- A shared map of the ecosystem will serve cybercrime defenders, prosecutors, legislators and investigators to plan, communicate and collaborate effectively.

As highlighted in the *Global Cybersecurity Outlook 2026*, cybersecurity is accelerating in response to escalating threats, geopolitical fragmentation and a widening technological divide.

With global cybercrime damages projected to exceed trillions annually and ransomware, fraud and illicit digital services becoming increasingly industrialized, the need for coordinated disruption has never been greater.

Yet, in a landscape where cyber defenders often operate in isolation, the Cybercrime Atlas offers a platform that connects experts and organizations, amplifying the impact of their individual efforts and enabling a more coordinated, systematic disruption of cybercriminal activities.

Cybercrime has evolved into a vast and complex ecosystem, comprised of diverse players that trade, collaborate, specialize and depend on each other across every phase of criminal operations.

The groups are large, globally distributed and supported by complex technical and money-laundering infrastructure. Yet, knowledge about how they operate remains fragmented, often siloed within individual organizations or countries, leaving defenders without a complete picture.

At the same time, responses are scattered. Cybercrime is transnational but law enforcement and industry efforts are often constrained by borders and limited coordination. The ecosystem gives scale and improves returns for criminals, enabling the meteoric rise of cybercrime.

It has launched Cosmos, an open-source map of the cybercrime ecosystem. The tool is available on the Cybercrime Atlas website and was developed by the Cybercrime Atlas community, led by Orange Cyberdefense, with contributions from Universitat de Girona, Scitum and TrendAI.

Defenders, legislators, prosecutors and investigators can use this shared "map" to develop a unified view of the ecosystem and its constituent parts; to plan, communicate and collaborate effectively; and ultimately to prevail in the struggle against cybercrime.

Disrupting cybercrime requires collaboration

The complexity of cybercrimes has led to numerous frameworks aimed at breaking them down into understandable events and many useful models already exist.

Researchers and practitioners use typologies, taxonomies, ontologies, crime scripts and cyber kill chains to understand different parts of the problem.

But these approaches rarely provide a single, integrated view of both criminal processes and the wider ecosystem that enables them. In parallel, the vast, diverse structures of the cybercrime ecosystem have been analyzed using social network analysis or with a variety of machine learning approaches.

However, there is no single framework that allows the individual cybercrime processes to be comprehensively understood within the broader, networked cybercrime ecosystem in a manner that is both integrated and practically usable.

Disruption of cybercrime on a large scale involves collaboration between multiple organizations, yet they often use different terms to describe the same concepts, making communication difficult.

A unified response to cyber threats depends on shared definitions. Cybercrime taxonomies and ontologies create a common language, making it easier for organizations to communicate, identify and classify threats quickly and consistently. They also streamline incident reporting by ensuring everyone describes cyber events consistently.

Data normalization builds on this by bringing information from different systems into a consistent format. Since threat data comes from many sources and in many forms, normalization makes it comparable and usable, enabling more effective analysis, sharing and coordinated action.

Despite significant advances in understanding individual threats and attack methods, there remains a critical gap: a shared, practical way to understand how these elements fit together as a system. Without this, efforts to combat cybercrime risk remaining fragmented and reactive.

Exposing cybercrime networks

Cybercrime Atlas “Cosmos” was designed to fill the current gap in understanding the cybercrime ecosystem. The map illustrates how the diverse players, platforms, technologies and markets connect and interact to commit acts that harm victims.

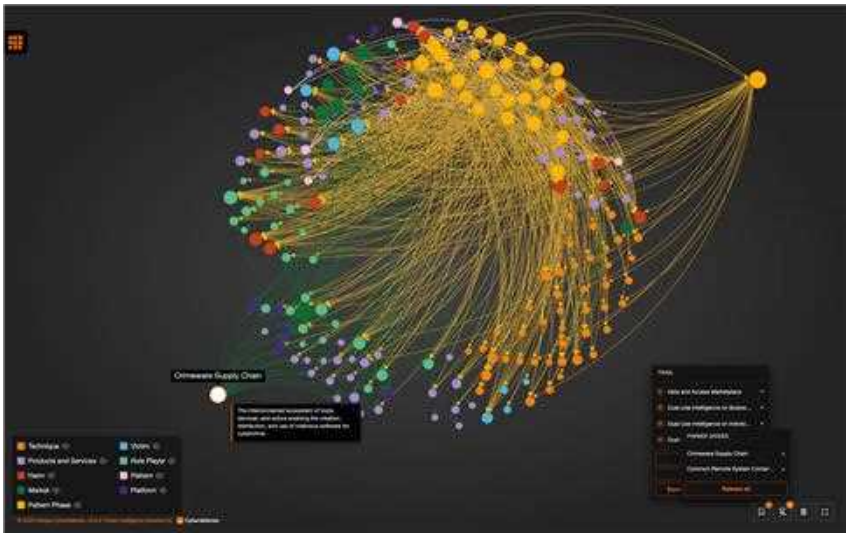
It is built on a formal ontology, with uniform definitions and categories which can be expanded on using open-source principles and community collaboration.

For these reasons, the Cybercrime Atlas has developed and launched what we believe to be the world’s first open-source cybercrime ecosystem knowledge graph, an interactive map that connects cybercriminal groups, tools, infrastructure and their relationships.

This resource was built over several months through a highly collaborative effort by volunteers across the Cybercrime Atlas community, including experts from industry, law enforcement, academia and civil society.

Cosmos currently includes nine core categories, 229 identified elements (such as cybercriminal groups, tools, services and infrastructure) and 849 connections that map how these elements interact and support one another.

Together, this creates a structured view of the cybercrime ecosystem, showing not just who and what is involved, but how they are linked. Importantly, the dataset is designed to be dynamic, expanding and evolving as new intelligence is contributed, and the community’s understanding deepens.



Static snapshot of the interactive Cybercrime Atlas Cosmos map Image: World Economic Forum

It is intended for both specialist and non-specialist users, including researchers, journalists, investigators, policymakers and practitioners from a wide range of fields.

Improving visibility is a first step toward more effective disruption.

The Cybercrime Atlas community and its partners are proud to release the first version of this new initiative. Cosmos provides a map of the cybercrime landscape as we understand it today. It also invites the wider community to help build, refine and use that map in the fight against cybercrime.

We extend our deepest thanks to the researchers, investigators, engineers and experts from the Cybercrime Atlas community who contributed to this report. For reasons of operational security, they cannot be named, but the findings shared here are based on insights developed through collaborative research by experts from the following organisations that participate in the Cybercrime Atlas community. Research led by Orange Cyberdefense with contributions from Universitat de Girona, Scitum and TrendAI.


WORLD
ECONOMIC
FORUM