

Security Navigator 2026: Data points

Cy-X is exploding:

- The Security Navigator 2026 found that Cy-X attacks have surged, with a 44.5% increase in victims observed between October 2024 and September 2025, as compared to the previous period.
- This continues a multi-year trend, with the total number of victims more than tripling since 2020 reaching 19,000 victims
- Cy-X actors' operational efficiency has also grown by 18%, with the victims-per-actor ratio rising from approximately 45 in 2020 to 53 in 2025.

The cybercrime landscape is fragmenting

- Previously, a single dominant group defined the landscape. Now, several actors sustain large-scale operations, with the number of distinct actors nearly tripling from 33 to 89 since 2020.
- In Europe, victims of Qilin and Akira have risen by 324% and 168% respectively.
- This is in some part due to the commoditisation of cybercrime “as a service”, which has drastically lowered the entry costs for attackers - allowing them to multiply and thrive.
- In addition to lowered entry costs, we are seeing the industrialisation of cyber crime with specialised expertise that democratise criminal activity through shared infrastructure, affiliate programmes and tool reuse.

Attackers are diversifying, targeting the vulnerable

- Two-thirds of Cy-X victims were Small-medium-sized-businesses (SMBs), a +9% increase from the previous year.
- In the US, small business victims surged by a dramatic 91%, showing attackers' preference for perceived ‘weaker links’ within societies' economies.
- In Europe, Germany ranks first in Europe in terms of victim count and is the country with the biggest growth in terms of Cy-X victims at 57.7%. Victims classified as large grew by 110.0%.
- 35 new countries see Cy-X emerging in our study, among them 10 new countries in Africa.

Hacktivists: Arm of states in modern geopolitics

- Hacktivism has evolved into a complex ecosystem aligned with state interests and geopolitical conflicts, moving beyond simple protests to real-world disruption and cognitive influence.
- Major incidents in 2025 include impacts on businesses: large-scale DDoS campaigns, cyber-physical attacks, and targeted disinformation efforts –
 - For example, on 7th April 2025, attackers remotely opened a valve at the Bremanger dam in Norway for several hours before operators intervened.

- On 29th October 2025, The Canadian Center for Cyber Security alerted that hacktivist groups had breached water, energy and agricultural OT/ICS systems in Canada, manipulating water pressure and manipulating temperature and humidity levels
- The goals have shifted from technical disruption to cognitive influence, aiming to erode trust in institutions and to influence public perception: in October 2025, pro-Russian hacktivist groups launched a disinformation campaign by claiming that they had accessed and manipulated water supply systems in several European countries, including Norway and Belgium.
- With Law Enforcement operations to interrupt their activities like Europol [Eastwood](#)

Global law enforcement (LE) cooperation is on the rise

For the first time, Security Navigator 2026 includes a systematically constructed dataset of 418 publicly announced LE activities conducted between 2021 and mid-2025. The data, collected by Orange Cyberdefense research teams, confirms a clear and steady annual increase in LE activity from 2021 to mid-2025:

- Actions taken include arrests (29%), takedowns (17%), charges (14%), sentences (11%), sanctions (7%), and seizures (4%).
- Cy-X is the most targeted criminal act by LE, with 59 cases, and it is also the most likely to lead to arrest, demonstrating that LE activity is scaling to meet the spiralling threat posed by Cy-X.
- The data also highlights a strong public-private partnership, with private organisations ranking as the third-most prominent institution type supporting law enforcement disruption efforts:
 - 40% of cases involves private actor contribution
 - At the country level, the United States remains the central enforcement hub, with US institutions and agencies driving 43% of LE actions.
 - The US also led nearly half of all actions (45%) and was a secondary participant in 17%.
- However, grey-zone actors can rebuild faster than bureaucracies respond, leaving significant ground for global law enforcement initiatives to cover.

About the Security Navigator

The Security Navigator is an international and multi-industry investigative research report and a strategic guide to understanding changes in the cyber threat landscape and sharing recommendations for risk management, by anticipating, responding to attacks and building the resilience of our societies. It combines rigorous analysis of first-hand global cyber research data with experts' advice and actionable recommendations to guide public and private decision-makers through an ever-changing threat landscape.

For its seventh edition in a row, it draws on the intelligence capabilities of Orange Cyberdefense, its Cyber Threat Intelligence. This year the analysis includes:

- 11 months' worth of Managed Threat Detection Services data, from 1st October 2024 to 31st August 2025, detecting and analysing over 139,000 security incidents.
- Since 2020, the team has observed and investigated 18,943 cases of cyber-extortion, including 6,142 in the last 11 months (October 2024 and September 2025).
- 1,289,451 unique findings and 60,837 unique assets via Orange Cyberdefense vulnerability operations centers (October 2024 and September 2025).
- 413 World Watch advisories delivered (October 2024 and September 2025).
- A new dataset of 418 publicly announced law enforcement activities conducted between 2021 and mid-2025.

Security Navigator 2026 is more than just a snapshot of the threats. It provides practical tools for action: methods for detecting attacks in their early stages, assessing their impact and organising a coordinated and effective response. By combining expertise and in-depth threat analysis with actionable recommendations, it enables organisations to strengthen their resilience in the face of cyber-risks, while anticipating tomorrow's challenges.

The full Security Navigator 2026 report can be downloaded here: <https://www.orange cyberdefense.com/global/security-navigator>