Cyberdefense

Press release
Paris, 4 December 2025

Security Navigator 2026 reveals cybercrime is industrializing and now sits at the epicenter of geopolitical dynamics. A common battle front is needed.

Orange Cyberdefense, a leading European provider of cybersecurity services, unveils the findings of its latest annual international research report, the Security Navigator 2026. The findings include analysis of more than 139,000 security incidents between October 2024 and September 2025 and a range of research based on its proprietary Cyber Threat Intelligence databank and Open Source Intelligence (OSINT) sources. Key findings include:

- Cyber extortion (Cy-X) has exploded on a global scale, with the number of victims tripling since 2020, reaching up to 19,000 organizations the data reveals.
- The increase in the number of Cy-X victims is striking, particularly for certain segments such as SMEs, which account for two-thirds of the companies affected, particularly as a vector for attacks on the supply chain; but also for critical sectors such as finance and insurance, with a71% increase, and health and transport, with a 69 and 67% increase respectively in the number of organizations affected.
- Cybersecurity is reshaping geopolitical dynamics and manipulating information. The association of states, hacktivists and digital ‘mafia’ organizations with attacks is reinforcing the phenomenon of the ‘balkanization’ of cyberspace. They are working to undermine confidence in democracies, and now economies, through cognitive attacks such as disinformation.
- The industrialization of the cybercrime market is based on a new ‘Crime as-a-service’ model and the growing integration of AI.
- However, international law enforcement co-operation and public-private partnerships are proving effective in dismantling cybercrime networks.

Industrialized cybercrime drives explosion of cyber-extortion

Since 2020, the number of victims of Cy-X has tripled, rising by 44.5% in 2025 worldwide. Small and medium-sized businesses (1-249 employees) suffer two-thirds of attacks, with significant growth in Europe (+91% in Germany, +54% in France). Cy-X extortion is going global, with 35 new countries added to the Security Navigator study this year. The number of victims is increasing, particularly in Africa (+47%), Latin America (+60%) and Asia (+82%), and is impacting critical sectors: +69% in healthcare, +71% in finance and insurance and also distribution (+80%), for example.

The fragmentation of the cybercrime landscape is accelerating. The dissolution of groups such as LockBit or Black Basta has given way to a multitude of players, each operating on a comparable scale. The list of active malicious actors has almost tripled, from 33 to 89.

Cybercrime had been professionalized, but now it has become industrialized, based on a “Crime-as-a-Service” model.

Charl van der Walt, Head of Security Research, Orange Cyberdefense, comments:

“As attackers diversify across geographies and business sizes, what's clear is that the traditional perception of the “supply chain” as linear is obsolete. In reality, we exist within a dense web of interdependence where a single weakness can enable mass compromise. Small businesses and critical services have become prime conduits to amplify economic and social consequences. While traditional defenses and incremental enforcement are necessary, they are not enough to offset agile adversaries that exploit society's interconnectedness."

Converging cybercriminals, state actors and hacktivists reshape modern geopolitics.

The balkanization of cyberspace is manifesting itself in the division of the cyberworld into geopolitical blocs. As revealed in our Security Navigator 2025, the boundaries between these players continue to blur, particularly with the rise of hacktivists, who are often ideologically aligned with complicit states. They carry out destabilization campaigns, DDoS attacks and manipulation of critical systems.

The main objective of these operations is no longer just technical disruption, but also misinformation, manipulation of opinion and psychological destabilization. It is a real strategy of cognitive attacks, demonstrating the interconnectedness of the various players involved. Hacktivists are becoming more professional, exploiting off-the-shelf ‘bot as-a-service’ cybercrime solutions to carry out these destabilization campaigns.

Misinformation completes the threat toolbox and is becoming one of the milestones in the evolution of cybercrime and contemporary geopolitics, with companies in critical sectors also targeted. The dissemination of false information, the manipulation of public opinion through misinformation campaigns, and the staging of spectacular cyber-attacks are fueling a hybrid war in which the boundaries between cybercrime, espionage and propaganda are becoming blurred.

At the same time, state actors continue to invest in cyberspace to carry out their cyber espionage and sabotage operations in a tense geopolitical context. They use criminal groups as proxies or extensions of their geopolitical strategy, in particular to destabilize adversaries or gather sensitive intelligence. For example, the Salt Typhoon campaigns, attributed to China, target critical infrastructure in more than 80 countries, exploiting vulnerabilities in telecommunications equipment and third-party supplier networks. These operations illustrate the integration of cyberattacks into the geopolitical strategies of governments.

Unprecedented global cooperation is the only path forward.

International co-operation is increasing with the active participation of 74 private organizations, under the aegis of Europol, Interpol and the Five Eyes alliance, among others.

An unprecedented analysis of 418 law enforcement actions (2021-2025) shows a steady increase in these operations, the majority resulting in arrests (29%), takedowns (17%) and charges (14%).

Co-operation that works

- Co-operation between public agencies and private players is essential. The majority of operations involve private partners, particularly in deterring and dismantling criminal infrastructure.
- International co-ordination has made it possible to dismantle networks, seize servers, prosecute cybercriminals and strengthen deterrence.
- The success of these operations shows that public-private collaboration is an effective weapon for dealing with the increasing number of attacks and the growing power of cybercriminal groups.

Hugues Foulon, Chief Executive Officer, Orange Cyberdefense, concludes:

"Far from being a tragic fate, the consequences of the balkanization of cyberspace should provide us with an opportunity to strengthen co-operation, transparency and resilience. The fight against organized cybercrime requires a global alliance, both public and private, to confront a threat that knows no borders. Orange Cyberdefense is ready to share the benefits of its Cyber Threat Intelligence to further reinforce our digital shield."

About Orange Cyberdefense

Orange Cyberdefense is the leading European partner for cybersecurity services backed by over 30 years of expertise developed within the Orange Group. The subsidiary independently delivers intelligence-led solutions across managed services, consulting *and systems integration, helping organizations anticipate, prevent and respond to cyber threats at any time. Our service capabilities draw their strength from research and our proprietary cyber threat intelligence capabilities, which allows us to offer our clients unparalleled knowledge of current and emerging threats. With more than 3,200 multi-disciplinary experts across 12 countries and 36 detection centers spread around the world, we know how to address the global and local challenges of our customers thanks to our local anchorage. We consider Cybersecurity as a human journey and a societal issue, so we build a safer digital society by placing people at the core of our actions. https://www.orangecyberdefense.com/*

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.orangecyberdefense.com/global/security-navigator*