TOP 5 CYBERSECURITY TRENDS FOR 2025

GILLES DAGUET

Head of the Private Equity
Cybersecurity Strategy

FRANÇOIS LAVASTE

Executive Director,
Private Equity Cybersecurity Strategy

TIKEHAU
CAPITAL

Top 5 Cybersecurity Trends for 2025

Since launching its dedicated **cybersecurity private equity investment strategy in 2019**[1], Tikehau Capital has been at the forefront of identifying and supporting solutions to one of today's most pressing challenges: cybersecurity.

Cybersecurity has evolved into a global megatrend, driven by the rapid digitalisation of economies, the explosion of data generation, and the increasing frequency and sophistication of cyberattacks. Adding to this momentum, **regulatory frameworks** such as the **NIS2 Directive**, **Cyber Resilience Act**, and **DORA** are transforming the landscape, especially in Europe, creating new challenges and opportunities for businesses.

Looking ahead, we have identified our '**Top 5 Cyber Trends for 2025'** — predictions that reflect the sector's dynamic evolution. These predictions will be revisited in 12 months to evaluate their accuracy and impact.

Key Milestones

OF TIKEHAU CAPITAL'S CYBERSECURITY STRATEGY

Guiding innovation and resilience in the digital economy.

LAUNCH YEAR: 2019

ASSETS UNDER MANAGEMENT:

€500 million

dedicated to cybersecurity[2] (as of September 2024)

[1] Each investment involves risks, including but not limited to loss of capital.

[2] The cybersecurity strategy includes a vehicle managed by Tikehau Investment Management, reserved for qualified investors and no longer open to commercialisation and subscription.

DEMOCRATISATION OF CYBERSECURITY: no one is safe

In 2025, every connected device and network — whether Information Technology[3] (IT) or OT (Operational Technology[4]) — becomes a potential target for cyberattacks.

- Large organisations remain at risk due to human error and their attractiveness to cybercriminals.
- Small and medium-sized enterprises (SMEs) and individual professionals are easier targets, often lacking robust defences.
- Attackers now leverage **automation** and **AI** to industrialise campaigns, increasing the scale and sophistication of phishing and ransomware attacks.

This universal threat drives a surge in **cybersecurity mergers and acquisitions (M&A)**, with non-cyber companies entering the space. Notable examples from 2024 include MasterCard's acquisition of Recorded Future and Salesforce's acquisition of Own Company.

The full impact OF AI

AI is transforming cybersecurity—but also empowering attackers.

- **Attackers**: AI is enabling sophisticated tactics like deepfake-based campaigns, CAPTCHA bypasses, and targeted phishing. Predictions suggest that by 2025, 17% of attacks and data leaks will involve generative AI (Source: *Gartner, August 2024*).
- **Defenders**: AI enhances data management, productivity, and automated threat response while creating a new challenge: defending AI itself.
- **AI Governance**: Transparent and explainable AI becomes critical to maintain trust and regulatory compliance, much like data governance has evolved.

CRYPTOJACKING makes a comeback

The rise of cryptocurrency prices makes cryptojacking — a form of illegal cryptocurrency mining — an attractive alternative for attackers.

- Unlike ransomware, cryptojacking silently drains resources without dramatic disruption, making it harder to detect.
- With high ROI and less visibility, cryptojacking malware is expected to grow significantly as a threat in 2025.

[3] Information Technology is the use of computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data.

[4] Operational Technology is the practice of using hardware and software to control industrial equipment, and it primarily interacts with the physical world

Intensification
OF CYBERPHYSICAL HYBRID WARFARE

Global geopolitical tensions and conflicts continue to inspire **cyberphysical hybrid war tactics**:

- Attacks on physical infrastructure (e.g., telecoms, electric grids and satellites) can disrupt essential services and create cyber vulnerabilities.
- Cyberattacks, in turn, can trigger physical consequences, highlighting the interconnectedness of physical and digital threats.
- Hybrid scenarios leveraging critical cyber weaknesses are expected to rise, posing challenges to infrastructure resilience.

The backlash OF PLATFORMISATION

Consolidating cybersecurity tools into unified platforms offers efficiencies but introduces significant risks:

- **Advantages**: Unified platforms reduce blind spots, streamline operations, and enable consistent policy enforcement.
- **Risks**: Relying on a single platform creates potential single points of failure. For example, the flawed July 2024 CrowdStrike Falcon update caused widespread disruption, grounding 42,000 flights and impacting 8 million devices.

In 2025, organisations will prioritise balancing **platform efficiency** with **redundancy and risk management**, avoiding over-reliance on a single solution.

Disclaimer

This document is not an offer of securities for sale or investment advisory services. This document contains general information only and is not intended to represent general or specific investment advice. Past performance is not a reliable indicator of future results and targets are not guaranteed. Certain statements and forecasted data are based on current expectations, current market and economic conditions, estimates, projections, opinions and beliefs of Tikehau Capital and/or its affiliates. Due to various risks and uncertainties, actual results may differ materially from those reflected or contemplated in such forward-looking statements or in any of the case studies or forecasts. All references to Tikehau Capital's advisory activities in the US or with respect to US persons relates to Tikehau Capital North America.