The Impact of AI-Driven Cybersecurity

Trends, Technological Landscapes, and Innovations in Europe

Author: Amir Aghaei Anvigh
Partner: Université de Rennes

Artificial intelligence has moved from being a supporting technology in cybersecurity to becoming one of the main forces shaping both defense and attack. Across Europe, modern cyber defense is being rebuilt around models that learn, adapt, and act faster than any human team can. At the same time, attackers are using the same technology to industrialize fraud, impersonation, and intrusion.

This creates a difficult situation for security teams: AI is being used by defenders and attackers at the same time. Regulations such as NIS2, DORA, the EU AI Act, and the Cyber Resilience Act are pushing European organizations to take this seriously, not only because it looks innovative, but because resilience, traceability, and faster response are becoming legal and operational obligations.

A Threat Landscape Born of AI

Many traditional assumptions in cybersecurity are becoming less reliable. We can no longer rely on slow attackers, recognizable malware, or badly written phishing emails. AI-powered attacks move at machine speed, mutate to evade detection, and impersonate trusted humans with unsettling accuracy.

The Arup deepfake fraud case in 2024 was a clear warning: criminals used deepfake video and audio to impersonate senior executives during a live call and convinced an employee to authorize transfers worth roughly 25 million dollars. Malicious LLMs such as WormGPT show how the barrier to entry is falling. Low-skilled actors can now generate convincing phishing, business email compromise messages, and malware scaffolding in minutes. Combined with polymorphic malware, this shows the limits of traditional rule-based detection, especially when threats constantly change their form.

This project has received funding from the European Union's Digital Europe Programme under grant agreement no. 101123118

Co-funded by the European Union

The Technologies Changing Cyber Defense

The strongest AI security platforms combine several layers: machine learning to detect patterns without signatures, deep learning to find complex behaviors in massive datasets, NLP to analyze phishing and threat intelligence, reinforcement learning to test response scenarios, and explainable AI to make decisions understandable for analysts, auditors, and regulators.

Together, these power three capabilities now standard in mature SOCs: anomaly detection, User and Entity Behavior Analytics (UEBA), and SOAR-driven automated containment. The economic case is strong. IBM reports that organizations using security AI and automation extensively saved an average of 2.2 million dollars per breach and shortened the breach lifecycle by about 100 days.

European Innovation Is Not Theoretical

Europe has become serious ground for AI-driven cybersecurity innovation, partly because of its focus on digital sovereignty. Darktrace, founded in Cambridge, popularized the "Enterprise Immune System," using self-learning AI to model users, devices, and workloads and detect anomalies without prior threat knowledge.

In France, the DGA plays a central role in defense innovation; its cyber expertise in Rennes feeds research, state capability, and startup creation. GLIMPS, founded by former DGA engineers in Rennes, uses deep learning to analyze binary code at a conceptual level, detecting unknown malware variants when signatures fail. TEHTRIS, based in Bordeaux, illustrates another European path: its sovereign XDR platform combines EDR, SIEM, mobile threat defense, honeypots, DNS firewall, and AI-driven orchestration, built with GDPR, NIS2, DORA, and the EU AI Act in mind from day one.

This project has received funding from the European Union's Digital Europe Programme under grant agreement no. 101123118

The Next Frontier: Cyber-Physical Systems and Identity

Some of the most interesting innovation is happening beyond classic IT. In automotive and industrial environments, AI-driven digital twins create virtual replicas of vehicles, factories, or connected devices, letting defenders simulate attacks and detect abnormal sensor behavior before real systems are compromised. For European OEMs facing UNECE R155, this is moving from "nice to have" to operational necessity.

Healthcare is another critical domain: hospitals rely on connected medical devices that cannot be treated like normal laptops, and AI can monitor their behavior continuously to detect compromise much faster than manual processes. Identity is being reshaped too. As voice cloning and deepfake video become cheap, liveness detection (blink patterns, micro-expressions, lighting, movement) is becoming foundational, especially as digital identity wallets expand across Europe.

The Road Ahead

The most important shift is this: AI-driven cybersecurity is not only about detecting threats faster. It is about changing the operating model of security. AI gives defenders autonomous speed, 24/7 scale, predictive capability, and relief for overwhelmed analysts. But it creates a new responsibility: we must secure the AI itself, because models can be poisoned, manipulated, stolen, or tricked with adversarial inputs.

The next five years will be shaped by three forces: explainable and auditable AI, because security decisions must be trusted; digital sovereignty, because European organizations care where their data, models and infrastructure are

This project has received funding from the European Union's Digital Europe Programme under grant agreement no. 101123118

hosted; and autonomous SOCs, where AI handles routine triage and humans focus on strategy, ethics, and adversarial thinking.

AI-driven cybersecurity is already part of today's security operations, and its role will continue to grow. The organizations that treat it as a core capability, not a bolt-on feature, will be the ones best prepared for the next generation of AI-powered threats. What is your organization doing to keep pace?

References

1. IBM. (2024). Cost of a Data Breach Report 2024. (IBM)
2. European Commission. (2024). EU AI Act: Regulatory Framework for AI. (Stratégie numérique Europe)
3. ENISA. (2024). NIS2 Directive: Guidance and Information Campaign. (ENISA)
4. CNN Business. (2024). Arup revealed as victim of $25 million deepfake scam involving Hong Kong employee.
5. Darktrace. Self-learning AI for cyber defense.
6. Direction générale de l'armement. French defense innovation.
7. TEHTRIS. European sovereign XDR platform.
8. GLIMPS. Deep learning malware analysis, Rennes, France.
9. OWASP. (2025). OWASP Top 10 for Large Language Model Applications. (OWASP)
10. MITRE. (2025). MITRE ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems. (atlas.mitre.org)
11. NIST. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST AI 600-1. (NIST Publications)
12. ANSSI. (2024). Security Recommendations for a Generative AI System.
13. NCSC, CISA, NSA, and international partners. (2023). Guidelines for Secure AI System Development. (ncsc.gov.uk)

This project has received funding from the European Union's Digital Europe Programme under grant agreement no. 101123118