Monthly Review

Cybersecurity news from around the world

INTRODUCTION 2

GENERAL CYBERSECURITY NEWS 3

ARTICLES

At the center of NATO's security agenda 5

How AI is reshaping the cyber threat landscape 8

KEY TAKEAWAYS 11

ARTICLE

How AI is reshaping the cyber threat landscape

Read article →

SECTRA

Newsletter introduction

Cybersecurity continues to evolve at a rapid pace, shaped by new technologies, changing regulations, and increasingly organized threat actors.

This edition highlights developments that affect how organizations manage identity, trust, and resilience in practice. From new fraud enabling services in the criminal eco-system to regulatory shifts around artificial intelligence, and the growing importance of mobile security controls, the focus is on understanding risk early and responding with clarity rather than complexity.

Stay resilient. Stay secure.

General cybersecurity news

1 The new farmers of cybercrime

A new service model is becoming increasingly common in cybercrime, especially in online fraud and scams. It is known as SIM Farm as a Service. In simple terms, it involves systems that manage large numbers of SIM cards at the same time. Each SIM card has its own phone number that criminals can use.

SIM farms allow criminals to create many accounts on social media platforms, email services, and other sites that require phone number verification. The SIM cards can receive one-time codes or send text messages, which makes fake accounts appear legitimate. This also makes it harder to identify who is really behind an account or a message.

These fake accounts are often used for phishing, fraud, extortion, or the spread of false information. SIM farms have also been used in SIM swap attacks, where an attacker takes control of a victim's phone number.

SIM farms are not illegal by default and can be used for legitimate purposes. The risk arises when this infrastructure is used for criminal activity. Authorities have acted in recent years, but demand for these services is expected to continue.

2 EU postpones AI Act implementation

EU member states and the European Parliament have reached a political agreement to delay parts of the EU's AI Act as part of the bloc's regulatory simplification agenda. Under the agreement, rules governing high-risk AI systems will apply from December 2, 2027, instead of August 2026. Requirements for AI systems used as safety components in products are postponed further, until August 2028. Transparency obligations for AI-generated content are also delayed until December 2026.

The changes are intended to reduce administrative burdens for companies and better align the AI Act with existing EU product and sector-specific legislation. At the same time, new prohibitions are introduced, including a ban on AI systems used to create non-consensual sexual or intimate material. Registration obligations in the EU AI database and strict necessity requirements for processing sensitive personal data are also reinstated. Formal approval by the Council and Parliament is still required.

3 What is MDM, and why does it matter?

A Mobile Device Management (MDM) is a set of technologies that allow organizations to centrally manage, secure, and monitor mobile devices, such as smartphones, laptops, and tablets, that access corporate systems. According to IBM, MDM helps balance mobile productivity with protection of enterprise data across both corporate-owned and personal devices.

MDM matters because mobile devices operate outside traditional network boundaries and are frequently lost, stolen, or exposed to insecure networks. NIST notes that centralized device management is critical to reducing risks such as data leakage, malware, and unauthorized access throughout the device lifecycle.

In practice, MDM restores visibility, enforces security policies, and enables secure remote and hybrid work at scale.

ARTICLE

At the center of NATO's security agenda

The Swedish town Helsingborg became a key stage for NATO's evolving security agenda in May 2026. Behind the formal meetings, discussions and agreements reflected a shift toward closer cooperation, stronger defense capabilities, and secure technological collaboration between allied nations.

The coastal city hosted a meeting of NATO's foreign ministers, a milestone for Sweden as a relatively new member of the Alliance. Over two days, senior representatives from across NATO gathered to discuss the state of European and transatlantic security, at a time marked by geopolitical uncertainty and increasing demand for coordination between allies.

The meeting itself was part of the formal NATO decision-making structure, known as the North Atlantic Council at ministerial level. In practice, that means foreign ministers come together to align positions ahead of major summits and to translate political commitments into concrete capability plans. In Helsingborg, much of the discussion focused on defense investment, industrial capacity, and long-term support to Ukraine, issues that continue to shape NATO's operational posture.

Questions around the United States' military presence in Europe and expectations on burden-sharing between allies added tension to the discussions. →

At the same time, ministers addressed developments affecting Euro-Atlantic security more widely, including the war in Ukraine and instability in other regions.

Alongside the formal agenda, Helsingborg also became the setting for several bilateral engagements. One of the most visible outcomes was a new agreement between Sweden and the United States, the so-called Technology Prosperity Deal. Formally, this is a memorandum of understanding, meaning it does not create binding obligations but outlines areas of cooperation. These include artificial intelligence, advanced connectivity, defense innovation, and quantum technologies, all fields that are becoming increasingly relevant to national security.

Taken together, the discussions and outcomes in Helsingborg point to a clear direction. Security policy is no longer confined to military capability alone. It now involves the ability to share information securely, coordinate across borders, and build trusted technological ecosystems that can operate under pressure.

For organizations working with secure communications, this development is already visible in day-to-day operations. Cross-border collaboration requires systems that can handle classified information while remaining usable across different environments, authorities, and security levels. Secure communication capabilities therefore play a central role in enabling cooperation between allied nations. The discussions and agreements in Helsingborg underline the importance of trusted infrastructure and reliable information exchange as part of modern defense and security work. ■

ARTICLE

How AI is reshaping the cyber threat landscape

AI is no longer a future risk in cybersecurity. This spring showed how quickly new models, tools, and habits are already reshaping how attacks happen and how organizations are caught off guard.

This spring, analysts at Cyberwatch Finland examined how artificial intelligence is reshaping the cyber threat landscape from three angles: AI as a tool for attackers, AI systems as targets, and the risks introduced by autonomous AI agents. According to Cyberwatch, the volume and pace of AI-related security incidents increased notably, with implications for both attackers and defenders.

One focus area was AI-driven acceleration of cyberattacks. The release of advanced models, including the highly publicized Mythos model from Anthropic, triggered debate about how quickly AI can identify and exploit vulnerabilities. While some claims were likely overstated, multiple studies cited in the review show that the time between vulnerability disclosure and exploitation has dropped dramatically, in some cases to less than a day.

Researchers also documented real-world use of AI-assisted tools in ransomware and large-scale network breaches, including attacks against hundreds of exposed firewall devices across dozens of countries. →

Another area of investigation involved AI systems becoming attack surfaces themselves. Incidents affecting cloud and developer platforms illustrate how third-party AI tools, browser extensions, and open-source libraries can be abused to gain deep access into enterprise environments. The breach disclosed by Vercel demonstrated how a forgotten trial of an AI tool, combined with excessive permissions, enabled attackers to move laterally into sensitive systems. Similar supply chain compromises showed that even short-lived malicious updates can have wide consequences when widely used AI components are involved.

The third theme centered on AI agents. Unlike traditional generative tools, agents can act independently across systems. Reports from Traficom and security researchers highlighted risks such as prompt injection, over-privileged access, and unintended autonomous actions. Real incidents ranged from data leaks to accidental deletion of production environments, underscoring how small configuration errors can scale quickly when agents are involved.

Across these areas, several trends stand out. Attack speed continues to increase, human error remains a central factor, and shadow use of AI tools is a recurring weakness. At the same time, organizations are beginning to apply AI defensively, particularly for detection and vulnerability management.

The likely path forward combines broader AI adoption with tighter governance, clearer boundaries for autonomous systems, and stronger identity and permission controls, as efficiency gains and security risks continue to evolve side by side. ■

Key takeaways

1. SIM farms enable criminals to mass-produce credible fake identities and scale fraud operations.
2. The delay of the AI Act gives organizations more time, but requirements for governance and compliance remain.
3. Without MDM, organizations lack visibility and control over one of their most exposed attack surfaces.
4. Modern security relies on the ability to share information securely across organizations and borders.
5. AI is increasing both the speed of attacks and the number of entry points, making stronger control and visibility essential.

www.communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden,
and operates through offices in Sweden, the Netherlands and Finland.

Linkedin

SECTRA