Monthly Review

Cybersecurity news from around the world

ARTICLE

Is AI becoming a threat actor?

Read article →

SECTRA

Newsletter introduction

As 2025 draws to a close, we take a moment to reflect on the events shaping cybersecurity today. From new legal frameworks to AI-driven threats, this year has reminded us how rapidly the digital landscape evolves — and how creative, persistent, and sometimes surprising attackers can be.

In this final newsletter of the year, we highlight key developments that matter to anyone navigating cyberspace. Practical changes, urgent vulnerabilities, and lessons that will help us prepare for a safer, smarter 2026.

We at Sectra Communications wish you all a merry christmas and a happy new year!

Stay resilient. Stay secure.

General cybersecurity news

1 Portugal introduces legal safe harbour for ethical hackers

Portugal has updated its cybercrime law to give ethical hackers limited legal protection. Decree Law 125/2025, published in December, allows actions that would normally be illegal, such as unauthorized system access, if carried out in public interest under strict conditions.

The ethical hackers must avoid causing harm, stealing data, or using aggressive techniques such as DoS attacks or malware. They are required to report vulnerabilities immediately to system owners, the Data Protection Authority, and the National Cybersecurity Centre (CNCS). Collected data must be deleted within ten days of remediation.

Most other European countries maintain stricter rules. In Sweden and Finland, unauthorized access is a criminal offense unless explicit permission is granted. The Netherlands also prohibits intrusion, although coordinated vulnerability disclosure guidelines can protect researchers who follow them.

Portugal's law provides legal clarity for security researchers, potentially encouraging more proactive reporting of vulnerabilities. By reducing legal risk, it could improve overall cybersecurity and make it easier for organizations to fix flaws before malicious actors exploit them.

2 Let's Encrypt shortens certificate lifespan

Let's Encrypt, the free service securing over 700 million websites worldwide, will reduce the lifespan of its security certificates from 90 days to 45 days, with full rollout by 2028. This change enhances web security by shrinking the window in which stolen or compromised certificates can be misused and making revocation more efficient.

The update also shortens the period a certificate can be reused without revalidating domain ownership — from 30 days to just 7 hours. Websites must regularly prove they control the domain, for example, by updating a special record or confirming server access. Let's Encrypt will introduce a new DNS-based method that automates this verification, simplifying renewals. Historically, certificates lasted 90 days to balance convenience and security, but automation tools now make frequent renewals practical. These changes aim to strengthen security while keeping websites running smoothly.

3 Critical React vulnerability exploited by state-linked actorss

In late November, security researchers discovered a severe vulnerability in React, the widely used framework for modern web applications. A section of code in server components reads and interprets incoming HTTP requests without the necessary safety checks, creating a path for attackers to execute code on a server without logging in.

Within hours of disclosure, several China-linked state actors began exploiting the flaw. Large volumes of scanning and exploitation attempts are now targeting vulnerable React and Next.js deployments, using automated tools and rapidly adapted proof-of-concept exploits. Many of these attacks route through anonymized networks common in state-sponsored campaigns.

Developers and organizations running React or Next.js are strongly advised to update to the latest patched versions immediately to prevent compromise.

ARTICLE

Black hat talk: “A city of a thousand zero days”

What happens when the systems controlling hospitals, airports, and office buildings are exposed to the internet — even though they were never designed to be?

In many organizations, cybersecurity is still framed around familiar assets: endpoints, servers, cloud platforms, and networks. Less attention is paid to systems that quietly control the physical environment, heating, ventilation, access control, fire safety, and lighting.

These systems increasingly sit on IP networks, sometimes directly exposed to the internet, without being designed for that reality.

This blind spot was highlighted at Black Hat Europe 2025, a computer security conference, in the presentation “A City of a Thousand Zero Days” by Gjoko Krstić of Zero Science Lab. The talk did not just catalog vulnerabilities in a single building management system (BMS). It illustrated a systemic problem: critical infrastructure software evolved through acquisitions, legacy code, and shifting ownership — without proper security reassessment. →

The accompanying white paper identified over 800 vulnerabilities in ABB's Cylon Aspect and FLXeon platforms, including remote code execution, authentication bypass, hardcoded credentials, backdoors, and insecure legacy protocols.

Many issues are exploitable without authentication, allowing attackers full administrative control from the internet.

"Vulnerabilities that begin as software flaws can escalate into physical incidents."

While some vulnerabilities have CVE identifiers (Common Vulnerabilities and Exposures), many of them remain pre-CVE or were silently patched without detailed advisories.

This complicates risk assessment and underscores challenges in operational technology: limited transparency, fragmented disclosure, and slow remediation for systems underpinning real-world operations.

Consequences extend beyond technical compromise. Publicly available proof-of-concept exploits show attackers could disable HVAC systems, manipulate fire alarms, shut down air handling units, or lock administrators out.

In hospitals, airports, data centers, and industrial facilities, these actions create operational disruption, safety risks, regulatory exposure, and reputational damage. →

ABB has acknowledged parts of the research and issued multiple updates since mid-2024. While noting these systems were not intended for internet exposure, the deeper issue remains, systems designed for closed environments are now often deployed in connected ones without compensating security controls.

As more physical systems become digitally accessible, organizations must treat building management infrastructure with the same rigor as core IT and OT environments. Vulnerabilities that begin as software flaws can escalate into physical incidents. ■

What is a zero-day vulnerability?

A zero-day vulnerability is a security flaw unknown to the vendor or unpatched when discovered. Defenders have "zero days" to respond. In building management systems, zero-days can directly impact physical operations, safety, and availability—not just data.

ARTICLE

Is AI becoming a threat actor?

AI is moving rapidly into daily life — but what happens when it starts shaping opinions, perceptions, and the information we trust? And while it can make our work easier and faster, it can also quietly influence the way we think and decide.

The digital landscape that we all move around in is changing, and that is rapidly. This year have had several topics related to the cyber security community, but there is only one that is in the news, almost daily, in various contexts — artificial intelligence. The tool that helps us write emails, code, strategies, you name it. But as with a lot of technology, it's not always used with good intentions.

In the middle of November, Anthropic, who has developed Claude, wrote that a Chinese state-sponsored group had used their AI tool to try to hack around thirty companies and government agencies worldwide. A few attempts succeeded, and most of the attack was carried out by AI with very little human involvement, marking the first known large-scale AI-driven cyberattack.

This incident is just one example of how AI is not only a tool used for productivity, but also a technology with the power to influence, manipulate, and shape outcomes on a large scale. →

Since artificial intelligence is an increasingly pervasive, and not just a productivity tool it has the capabilities of shaping perceptions and influencing decisions. Research and real-world examples show how AI can actively steer our behavior. A 2025 Cornell University study demonstrated that chatbots powered by large language models, like ChatGPT or Claude, can shift voter attitudes by up to 25 percentage points.

The influence comes from generating multiple fact-based claims supporting a political candidate or policy. Even partially inaccurate or incomplete claims, repeated and presented authoritatively, can subtly reshape opinions over time.

"AI-driven information flows can redefine what people perceive as important, trusted, or true"

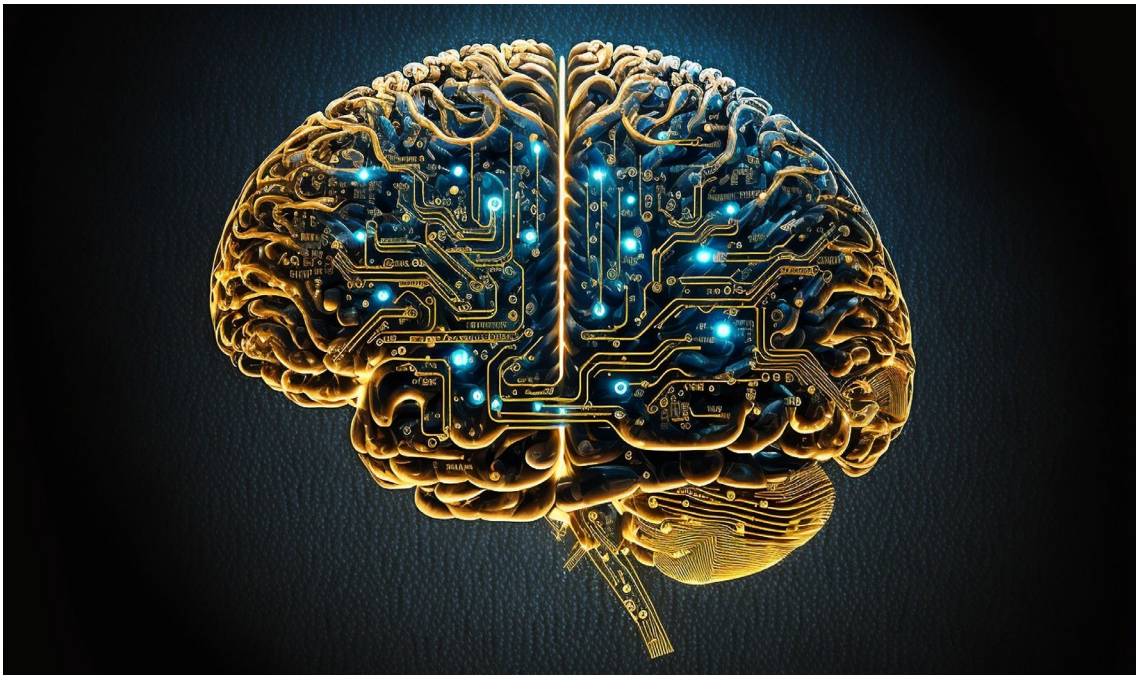
Ahead of the 2025 Dutch national election, AI chatbots tested by authorities provided biased voting advice, often favoring extreme parties regardless of user input. In Finland, AI systems occasionally suggested incorrect voting instructions without knowing users' true preferences. These examples show AI can be both unintentionally biased and factually unreliable yet perceived as authoritative.

The threat differs from traditional cyber risks, when it comes to AI reshaping the information environment itself. Automated content generation, amplification of selected topics, and reinforcement of perceived consensus quietly steer the public's attention. Perceptions of legitimacy, urgency, and credibility can influence behavior, trust, and decision-making in elections and even broader organizational and societal contexts. →

The challenge is systemic. Now when AI can produce content at scale, adapt in real-time, and exploit human behavioral patterns, it makes the influence nearly invisible.

Understanding AI's impact on perceptions and anticipating its effects is essential for maintaining information integrity and security across public institutions, private organizations, and society.

As AI evolves, its influence extends beyond individual tools or platforms. These trends offer a warning that AI-driven information flows can redefine what people perceive as important, trusted, or true. Since the human factor is one of the biggest risks when it comes to security — awareness, analysis, and strategic engagement are central to navigating the shift in the digital landscape responsibly. ■



Key takeaways

1. Portugal now gives ethical hackers limited legal protection, encouraging responsible reporting of vulnerabilities.

2. Let's Encrypt will cut certificate lifespans to 45 days and tighten revalidation, improving web security.

3. A serious React flaw is actively exploited by state-linked actors, making immediate patching crucial.

4. Exposed building management systems reveal hundreds of vulnerabilities that can impact real-world operations.

5. AI is increasingly capable of manipulating perceptions and influencing decisions at scale.

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