SECTRA NEWSLETTER — NOVEMBER 2025

Monthly Review

Cybersecurity news from around the world

ARTICLE

Sensitive data exposed via GEO satellites

Read article →

SECTRA

Newsletter introduction

As November unfolds, Europe's cybersecurity landscape continues to shift, bringing both challenges and opportunities for stronger defenses.

From new insights into Sweden's national electricity transmission operators' data breach, to Denmark halting CSAM scanning plan, and the EU's ongoing support for Ukraine's cyber defenses. This month's edition underscores the importance of staying informed and proactive.

These developments, along with emerging risks from small drones and recent research on unencrypted satellite communications, reminds us that protecting critical infrastructure is an ongoing challenge.

Stay resilient. Stay secure.

General cybersecurity news

1 New details on the data breach of Svenska Kraftnät

New information has clarified the scope of the October 25 data breach at Svenska Kraftnät, Sweden’s national electricity transmission operator. The intrusion targeted an external file transfer service, exposing mostly non-confidential information such as system updates, drivers, support files, historical records, and contact details of individuals attending meetings and trainings. Some sensitive information about the power grid was also accessed, but nothing was classified as critical to national security, according to Chief Information Security Officer, Cem Göcgören.

He emphasized: “It is not surprising that an incident like this attracts interest and curiosity from the media, the industry, and the public. But we hope for understanding from others as we prioritize security first.”

Given the widespread interest in the breach, authorities have confirmed that electricity transmission and grid operations were not affected. Investigations are ongoing to determine how the intrusion occurred and to strengthen processes against future threats. The incident has been reported to the Swedish Authority for Privacy Protection (IMY) as a personal data breach. Officials are also reviewing internal procedures to prevent similar incidents in the future.

2 Denmark drops CSAM scanning plan

Denmark has withdrawn its plan to require online services to scan user devices for child sexual abuse material (CSAM) after domestic and EU opposition. The governing Moderates parties in Germany and Denmark opposed the measure, and the EU vote planned for October 2025 was postponed. Privacy advocates and apps like Signal and Threema criticized the 2022 Chat Control proposal, introduced by the European Commission, for enabling arbitrary surveillance. Denmark's Justice Minister, Peter Hummelgaard, emphasized that the EU must establish a permanent CSAM framework before the current temporary system, which allows only voluntary scanning, expires in 2026.

Opposition remains from the Netherlands and Poland, while France and Ireland support the initiative. The withdrawal underscores ongoing debates on client-side scanning, privacy, and regulatory compliance in the EU.

3 €60.9M to strengthen Ukraine's cyber defenses

The EU and its international partners have strengthened their coordinated cyber assistance to Ukraine, committing €60.9 million for 2025 through the Tallinn Mechanism — the joint platform created in 2023 to organize and deliver civilian cyber support to Ukraine across governments, donors and technical experts. The new pledge brings total coordinated support to €241.7 million.

The announcement followed the Paris meeting on 30–31 October, where EU member states and allies reaffirmed that Russia's increasingly sophisticated cyberattacks form part of a broader hybrid campaign aimed at destabilizing democratic institutions far beyond Ukraine. The EU, together with partners such as the UK, US and Nordic countries, underlined that bolstering Ukraine's digital defenses is directly linked to strengthening Europe's own resilience.

With expanded membership and continued cooperation with observers including the EU, NATO and the World Bank, the Tallinn Mechanism has become the central hub for channeling timely, needs-driven support to Ukraine — and a key instrument in Europe's wider security posture.

ARTICLE

Small drones — Big consequences for airports

Drones are cheap, easy to build — and capable of shutting down Europe's busiest airports. Recent incidents show how little it takes to paralyze critical infrastructure. These disruptions do not only delay flights, but also impose significant operational and financial costs for society.

Over recent months, Europe has seen multiple drone incidents disrupting airports and military installations, exposing vulnerabilities in both civilian and military airspace management. As highlighted by the Financial Times, even small, inexpensive drones can create outsized effects on critical infrastructure.

On November 22, 2025, Eindhoven Airport temporarily suspended all civilian and military flights after several drones entered restricted airspace. The nearby Volkel Air Base, home to Dutch F-35 jets and a U.S. NATO squadron, was also affected. Dutch authorities deployed ground units to respond, but, as reported by the Financial Times, no wreckage was recovered, and the operators remain unidentified. The closure lasted several hours, forcing flight rerouting and emergency airspace protocols, demonstrating how even small unmanned aerial vehicles (UAVs) can disrupt operations.

Earlier in November, Brussels Airport, Zaventem, experienced a similar disruption. →

According to BBC, drones were spotted over both the airport and nearby military facilities, affecting about 3,000 passengers of Brussels Airlines and causing significant operational costs.

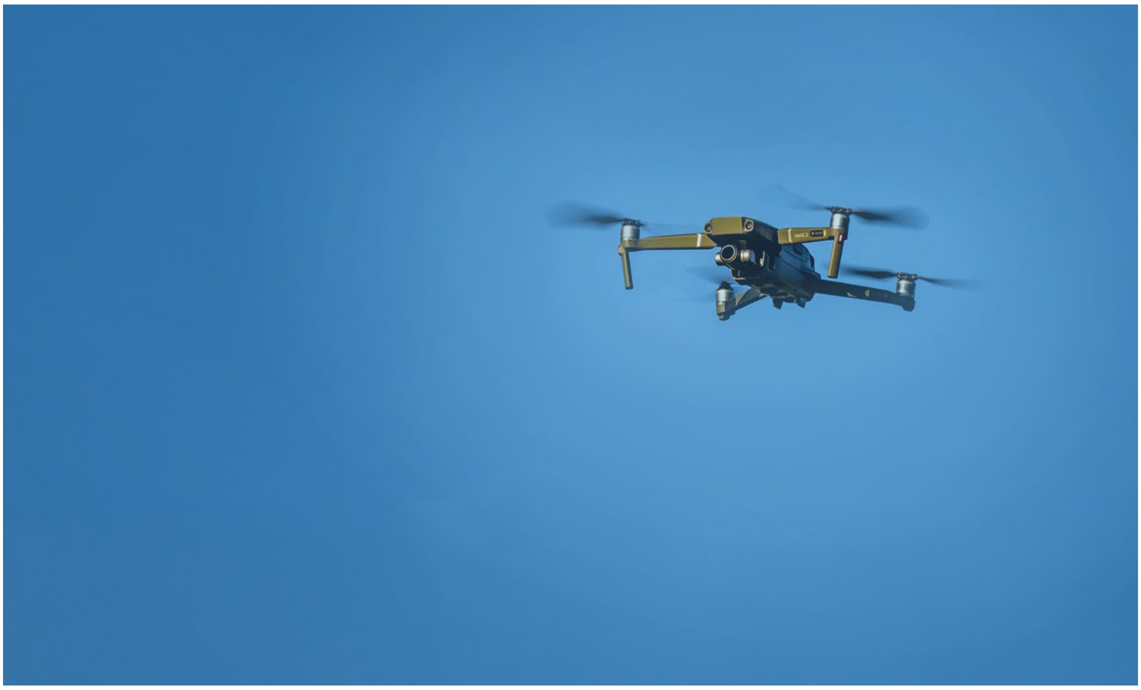
Belgian Defense Minister, Theo Francken, emphasized that what was once considered a purely military problem had become a serious threat to civilian infrastructure across multiple European countries. Assistance from Germany, including anti-drone systems, was accepted to mitigate the risk.

> *“Investment in counter-drone technologies are becoming standard”*

As highlighted by Euronews, comparable incidents have occurred in Denmark, Germany, Poland, Sweden, and Norway, collectively involving several dozen drone sightings linked to airports or military zones. Even a single drone can halt air traffic for tens of minutes, triggering cascading delays and logistical challenges. These events exemplify “low-cost, high impact” disruption: minimal effort produces maximal operational effect.

Speculation over the operators remains high. EU and NATO officials have suggested that the pattern resembles Russian hybrid operations, particularly amid discussions on EU plans to use frozen Russian assets to support Ukraine, as reported by the BBC. However, no concrete evidence has publicly emerged, and as highlighted by Euronews, all drones have disappeared before recovery, leaving authorities with limited forensic material.

The accessibility of drones amplifies the challenge. →



Commercial or improvised models can be built for a few hundred dollars. While their small size makes them difficult to detect, they remain large enough to force significant defensive measures, underscoring a critical gap in European airspace security.

In response, the European Commission has proposed creating an integrated “drone wall” across borders and critical infrastructure, drawing on lessons from Ukraine, as highlighted by the Financial Times. Several member states are accelerating procurement of detection systems, jamming technologies, and rapid-response protocols, according to BBC. These measures illustrate a growing recognition that defending European airspace requires coordinated, cross-border approaches bridging civilian and military capabilities.

While the threat is unlikely to disappear, authorities have highlighted that enhanced detection, coordinated emergency procedures, and investment in counter-drone technologies are becoming standard practice to prevent future disruptions, as reported by multiple sources. ■

ARTICLE

Sensitive data exposed via GEO satellites

New research shows unencrypted satellite traffic leaves telecom, government, and critical infrastructure vulnerable to interception. Sensitive calls, messages, and network data could be accessed by anyone with basic satellite reception gear.

A recent study from the University of California, San Diego and the University of Maryland has revealed significant security gaps in geostationary (GEO) satellites. Sensitive internal network traffic spanning telecommunications, government, defense, utilities, retail, banking, and aviation is being transmitted over satellite links without encryption.

According to the researchers, the scope was "quite shocking," with private voice calls, text messages and internal telemetry accessible to anyone equipped with standard satellite reception gear.

Although the study was conducted using satellites visible from southern California, primarily serving U.S. and Mexican networks, the technological implications are global. GEO satellites operate under standard protocols and hardware that are used worldwide, including across Europe. This places EU governments, critical infrastructure operators and private enterprises at potential risk if they rely on comparable unencrypted GEO links. →

The research team, helmed by academics from U.S. institutions, scanned IP traffic across 39 GEO satellites and collected 3.7 terabytes of raw data over seven months. The analyzed satellites represent roughly 15 percent of the global GEO fleet, suggesting that the prevalence of unencrypted transmissions might be far greater than documented.

The exposed data included unprotected backhaul for cellular networks (voice, SMS, metadata), internal communications of large corporations, banking and utility network traffic, and even in-flight WiFi data — all in plain text.

> *“The fact that fundamental encryption is missing in large parts of the GEO-satellite ecosystem indicates a compliance gap for any EU-based operator using such links”*

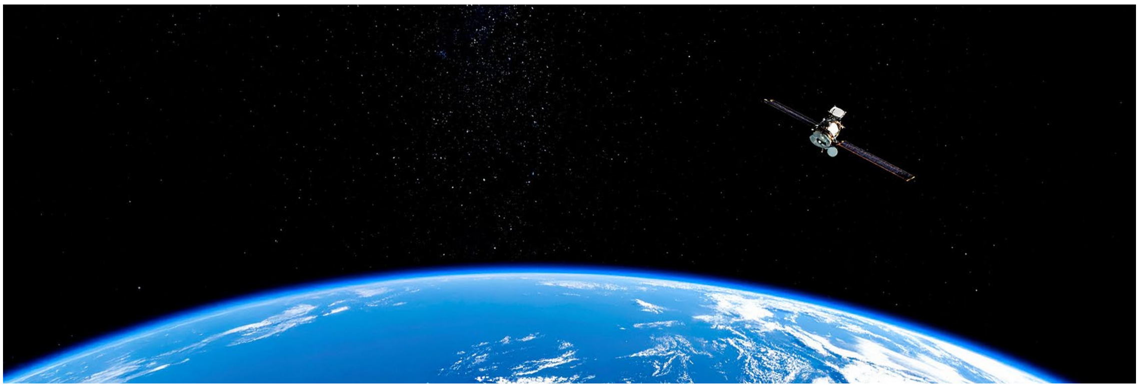
The findings reaffirm concerns previously demonstrated in Europe. The 2022 cyberattack against the satellite broadband network KA-SAT, affecting thousands of modems across multiple EU countries, damaging critical services including renewable-energy operations, underscored how satellite-based systems can be exploited. That incident demonstrated the practical consequences of compromised satellite links. The new study adds technical evidence that many GEO links remain unencrypted by design or default, a vulnerability that may persist across European satellite communications.

The findings reaffirm concerns previously demonstrated in Europe. The 2022 cyberattack against the satellite broadband network KA-SAT, affecting thousands of modems across multiple EU countries, damaging critical services including renewable-energy operations, underscored how satellite-based systems can be exploited. →

That incident demonstrated the practical consequences of compromised satellite links. The new study adds technical evidence that many GEO links remain unencrypted by design or default, a vulnerability that may persist across European satellite communications..

The study's findings highlight gaps in European regulatory and strategic frameworks. Under the NIS2 Directive, organizations in critical sectors must implement "state-of-the-art" security measures, yet many GEO satellite links remain unencrypted, creating a compliance gap.

The EU's planned IRIS² satellite constellation gains added justification, as these vulnerabilities underscore the need for end-to-end encrypted European satellite infrastructure rather than reliance on older GEO services.



In technical terms, the problem is not confined to geography but to the architecture of GEO satellite networks. That underlying architecture is shared globally, including in Europe, meaning that systemically unencrypted backhaul, outdated satellite hardware, and organizational under-awareness are issues that could affect European networks the same way they affect American or Mexican ones.

In conclusion, while the study focused on US and Mexican communications, its findings carry clear relevance for Europe. The demonstrated prevalence of unencrypted traffic over GEO satellites should prompt European operators, in telecom, utilities, transport, defense and beyond, to audit their satellite links. At a time when EU regulation demands robust cyber-resilience, the exposed satellite-link vulnerabilities underscore an urgent need: encryption must become standard across all GEO communications used by European critical infrastructure. ■

Key takeaways

1. Sweden’s national electricity transmission operators’ breach exposed some sensitive information but did not affect critical electricity grid operations.

2. Denmark has withdrawn its plan for CSAM scanning of user devices following privacy and regulatory concerns.

3. The EU and international partners pledged €60.9 million to strengthen Ukraine’s cyber defenses through the Tallinn Mechanism.

4. Small drones have repeatedly disrupted European airports, revealing vulnerabilities in critical infrastructure.

5. A recent study revealed that a significant portion of GEO satellite traffic, including voice, text, and telemetry, is transmitted unencrypted.

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