Monthly Review

Cybersecurity news from around the world

ARTICLE

MUST: "The threats to Sweden are very serious"

Read article →

SECTRA

Newsletter introduction

The security environment has evolved across all sectors.

This month's newsletter highlights how attacks are sometimes designed not to break systems, but to simply observe them—whether through persistent monitoring of everyday communications or targeted intrusions like the recent incident in Poland's energy sector.

Across Europe, intelligence services report the same pattern that adversaries no longer need to breach your perimeter if they can quietly track how you communicate and make decisions.

Stay resilient. Stay secure.

General cybersecurity news

1 When internal communication stops being internal

Most organizations still treat internal communication as a protected space. That isn't always the case.

Your daily discussions flow across cloud services, external partners, consultants, personal devices, and unofficial chat groups. From an intelligence perspective, this creates a rich, and usually unprotected, map of how your organization thinks and decides. Attackers don't need to break critical systems if they can sit quietly inside email threads and watch decisions form over time.

Ask yourself this: If someone had full visibility into our channels for six months, what would they learn about us?

Organizations that recognize this shift make deliberate choices. They separate routine coordination from sensitive deliberation. They accept that not every tool suits every discussion.

One simple principle helps: ask whether someone needs to know this information, or if it's just nice to know. "Need to know" information is essential, mission-critical, and required immediately for performance, safety, or compliance. "Nice to know" information adds context but isn't necessary to complete the task.

The boundary between internal and external communication has changed significantly. Understanding that shift is the first step toward adapting the way we communicate.

2 Communications as the attack surface

Many cyber operations aren't always aimed at disruption. They're designed for intelligence collection—mapping how you communicate, coordinate, and decide. Organizations that successfully reduce this exposure focus less on perimeter defenses and more on communication habits:

- Separate the channels. Try to keep sensitive discussions off platforms that mix internal, external, and informal messages.
- Verify strategic channels. Make decisions through channels with strict access controls.
- Limit account value. Reduce what any single compromised account can see.
- Grant access by role, not convenience. Restrict unnecessary visibility of sensitive material.

When cyber activity targets information rather than infrastructure, the weakness lies in everyday habits—not technology.

3 Only 1 out of 10 SMEs have mandatory cybersecurity training

New figures from the annual ICT security survey by Statistics Netherlands (CBS), highlighted by the National Cyber Security Centre (NCSC-NL), point to a clear weakness in small and medium-sized enterprises' digital resilience. Just 9% of SMEs require mandatory ICT security training for employees. This stands out in a threat landscape where phishing, credential theft, and social engineering remain common entry points. While 61% of SMEs use multi-factor authentication and 66% maintain off-site backups, far fewer invest in structured awareness programs. However, the data suggests that human-focused measures remain underprioritized. Even with the right technical controls in place, one click on a phishing email can disrupt operations. If your organization has not made security training mandatory, it is not too late to start. Regular, structured training—combined with appropriate technical safeguards—turns digital resilience from a policy into daily practice.

ARTICLE

Poland nearly went dark—here's what it means

Poland's energy sector faced a serious cyber incident, exposing OT vulnerabilities and prompting Nordic authorities to heighten vigilance, highlighting the growing threat to critical infrastructure across Europe.

Poland recently disclosed a serious cyber incident affecting parts of its energy sector. According to the official technical report from CERT Polska, attackers exploited vulnerabilities in perimeter devices, including exposed VPN connections on firewalls, to gain initial access to networks connected to industrial environments.

From there, the intrusion moved beyond traditional IT systems. The threat actor deployed the custom-built wiper malware DYNOWIPER, designed to erase files critical to Windows-based systems. Lateral movement was achieved using scheduled tasks, SMB propagation, and Group Policy Object (GPO) configurations, which enabled broad distribution within the compromised environment. The incident did not result in a nationwide blackout, but the technical findings make clear that the attackers reached deep enough into the environment to create conditions where operational disruption would have been feasible. →

In a subsequent alert, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) cited the Polish case as an example of persistent security gaps in OT and ICS environments, particularly insufficient IT/OT segmentation and limited visibility into industrial protocols.

While the Polish report focuses on technical remediation rather than attribution, multiple security authorities have linked similar activity clusters to the group commonly known as DragonFly/GhostBlizzard, assessed by Western agencies as associated with Russia's FSB Center 16.

The pattern aligns with earlier campaigns targeting European energy infrastructure.

CISA has repeatedly warned that legacy industrial systems were not designed with modern threat actors in mind. Detection speed now determines whether an intrusion becomes a disruption. The Polish grid remained operational, and that outcome was tied to containment and response, not the absence of capability on the attacker's side.

A Nordic dimension

According to Swedish news outlets, Nordic authorities have recently raised vigilance levels following intelligence of a potential threat directed at energy infrastructure across the region.

Sweden's National Defence Radio Establishment (FRA) confirmed that it has urged the energy sector to increase monitoring and preparedness, explicitly referencing the Polish attacks as part of the background assessment.

Police authorities in Sweden have increased protective presence around critical energy facilities, while national agencies are coordinating through international channels. FRA characterized the measure as precautionary but acknowledged that critical infrastructure remains of consistent interest to foreign adversaries. →

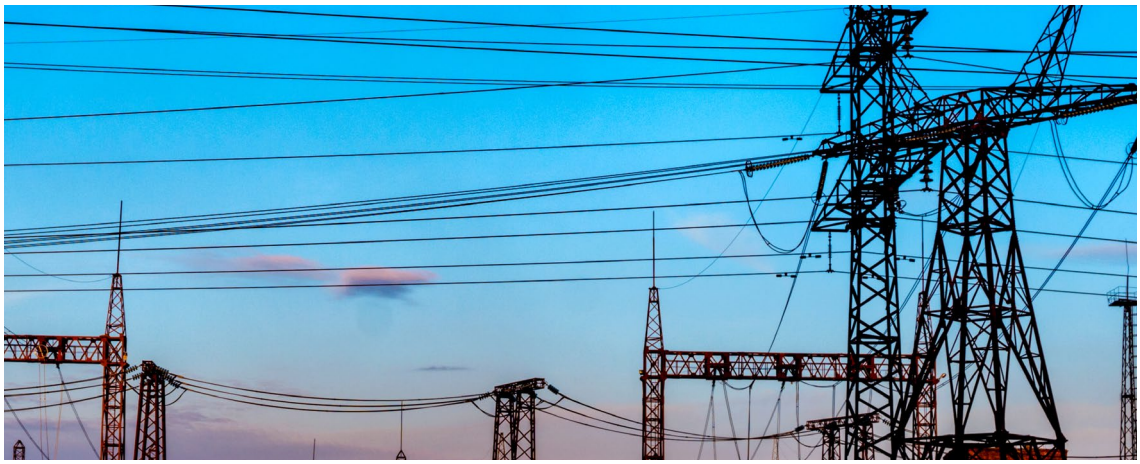
CISA recommends validating IT/OT segmentation, restricting administrative pathways such as GPO distribution across sensitive environments, hardening perimeter devices, and ensuring tested restoration capabilities following destructive malware scenarios. The Polish case illustrates a shift in defensive logic. Resilience is measured less by preventing intrusion altogether and more by detecting, isolating, and restoring before systemic impact occurs.

Three questions worth asking this week:

1. Do we have vulnerability assessments of our energy dependencies?
2. Which systems remain critical if power fails for six or more hours?
3. Do we have backup communication channels that function without internet access?

Across Europe and increasingly in the Nordics, civilian energy infrastructure is no longer treated as a peripheral cyber target. It sits squarely within the scope of geopolitical signaling and operational testing.

If you operate in adjacent sectors—logistics, healthcare, communications, finance — proximity alone makes resilience part of your mandate. ■



ARTICLE

MUST: “The threats to Sweden are very serious”

Sweden’s MUST released its annual threat assessment. The message: pressure below armed conflict is increasing, and communication systems are now contested space.

In its latest overview, Sweden’s Military Intelligence and Security Service (MUST) describes a security environment that has continued to deteriorate and will likely remain unstable through 2026. The report emphasizes that pressure against Sweden and its allies is increasingly applied below the threshold of armed conflict—through cyber operations, influence campaigns, sabotage, intelligence collection, and economic pressure.

“The threats to Sweden are very serious, and the situation may worsen further.”

Russia remains the primary military threat in MUST’s assessment, but much of the report focuses on how modern conflict is actually conducted in practice. Hybrid activities are described as integrated instruments used to shape outcomes over time, not as alternatives to traditional warfare.

For secure communication, this shift carries real implications. MUST repeatedly highlight that hostile activities increasingly target systems, information flows, and decision-making processes rather than territory alone. →

Communication systems are therefore not only enablers of daily operations, but part of the contested space itself.

One pattern stands out across the report—the use of intermediaries. Sabotage, cyber activity, and intelligence collection are increasingly carried out through criminal networks, loosely affiliated actors, or individuals recruited online. This makes it harder to determine who is behind an operation and complicates both response and deterrence.

"The broadening use of unqualified executors and proxies makes sabotage activities difficult to prevent, detect, and link to specific actors."

In such an environment, the ability to communicate securely, across organizational boundaries, between civil and military actors, and with international partners, becomes a practical necessity rather than a theoretical safeguard.

Similar observations appear in reports from other European intelligence services. Finland's SUPO has pointed to the growing use of proxies and deniable operations, noting that these methods increase the risk of misinterpretation and unintended escalation. SUPO has also highlighted that intelligence and security cooperation increasingly relies on trusted channels, often outside public or open communication structures.

The Dutch intelligence service AIVD approaches the issue from a different national position but reaches comparable conclusions. As a logistics, transport, and data hub, the Netherlands has seen how cyber operations, sabotage, and organized crime can intersect with state interests. AIVD has described how criminal networks develop capabilities comparable to those of intelligence services, and how these capabilities can be leveraged by state actors seeking plausible deniability. →

MUST's assessment places particular emphasis on persistence. Hybrid pressure is not framed as episodic or crisis-driven, but as continuous and adaptive.

"The security-threatening activities affect a broad range of societal functions and actors."

Across the MUST, SUPO, and AIVD reports, a common thread emerges, communication systems are increasingly exposed to intelligence collection, manipulation, or disruption, while the need for secure and reliable channels continues to grow. The challenge is not only about protecting information, but about ensuring that decision-makers, operators, and partners can communicate without interference in an environment where pressure is sustained and attribution remains unclear.

Organizations working with sensitive information are beginning to ask different questions. Not just whether a channel is encrypted, but who can see the metadata around it. Not just whether they have secure email, but whether they can continue making decisions if their primary communication infrastructure is compromised or under observation. Not just whether they are compliant, but what an adversary would learn by quietly monitoring their communications over an extended period.

The environment these intelligence services describe is not temporary. It represents a baseline shift in how pressure is applied and how security must be understood. ■

Key takeaways

1. Organizations still treat internal communication as protected environment—attackers know it isn't and use it to map decision-making over time.

2. When attacks target information rather than infrastructure, the weakness lies in communication habits, not technology.

3. With only 9% of SMEs requiring mandatory cybersecurity training, human behavior remains the most underprotected part of digital resilience.

4. The Polish energy incident shows that resilience today depends less on stopping intrusions entirely and more on detecting, isolating, and restoring before operational disruption occurs.

5. MUST, SUPO, and AIVD agree, hybrid pressure is persistent, communication systems are contested, and organizations must assume their channels are being monitored.

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