SECTRA NEWSLETTER – SEPTEMBER 2025

Monthly Review

Cybersecurity news from around the world

ARTICLE

SWEN — The new Swedish Emergency Network

Read article →

SECTRA

Newsletter introduction

In 2025, Sweden is taking bold steps to strengthen its resilience. Rising regional tensions, growing cyber threats, and Europe's shifting security landscape leave no room for complacency.

From reinforcing military capabilities to improving civil defense, cybersecurity, and emergency communications, the focus is clear: Sweden must be ready to safeguard essential functions when they are needed most.

At the same time, global advances like quantum computing and the surge in cyber espionage remind us that resilience is not just about defense—it's about staying one step ahead. That requires coordination, modern technology, and shared preparedness across societies, businesses, and governments.

Stay resilient. Stay secure!

General cybersecurity news

1

50 billion to strengthen Sweden’s total defense

In 2026, Sweden is proposed to make one of its largest investments in national resilience in decades. Rising regional tensions and escalating cyber threats have pushed the government to strengthen both military readiness and civil protection through Swedens autumn budget.

Civil defense is set to receive around SEK 12 billion between 2026 and 2028, with targeted investments in healthcare capacity, food and water security, and municipal preparedness. Annual funding will increase steadily, ensuring a long-term build-up of resilience across society.

On the military side, the 2026 budget adds SEK 26.6 billion for personnel, equipment, and infrastructure, with defense spending projected to reach 3.5% of GDP by 2030. Combined with civil measures, this represents close to SEK 50 billion in new resources, reflecting Sweden’s determination to meet NATO commitments and adapt to a shifting security landscape. Alongside physical and military capabilities, strengthening digital resilience is becoming equally critical.

The Swedish defense budget for 2026 is set at SEK 175 billion. This reflects a deliberate strategy to strengthen Sweden’s resilience across multiple dimensions, ensuring readiness through training and exercises, and reinforcing critical societal infrastructure. The scale of the investment signals a recognition that contemporary security threats, including regional military pressure and hybrid threats such as cyberattacks, require both robust military capabilities and comprehensive civil preparedness, rather than isolated measures.

2 Chinese APT group targets Dutch ISPs

Dutch intelligence agencies have confirmed that Salt Typhoon, a Chinese-state backed hacking group, targeted smaller internet and hosting providers (ISPs) in the Netherlands. The group, linked to global cyber espionage against telecom and critical infrastructure, exploited known vulnerabilities to access routers and edge devices, occasionally leveraging commercial technology infrastructure. According to the Dutch General Intelligence and Security Service (AIVD), the hackers gained access to routers but as far as known, did not infiltrate internal networks. These findings align with earlier U.S. investigations by the FBI and CISA, which identified Salt Typhoon as responsible for a broad espionage campaign targeting the United States.

The report highlights a wider trend in cyber threats: increasingly sophisticated operations require continuous monitoring, timely patching, and close collaboration with national cybersecurity authorities.

3 Cyberattacks — a national threat

Sweden now identifies cyberattacks as a central threat to national security, according to the report Foundations for total defense 2025–2030 (Utgångspunkter för totalförsvaret 2025–2030). Alongside conventional military threats, sabotage, and information operations, cyberattacks can disrupt decision-making, divert resources, and undermine public trust. Critical infrastructure, including energy, communications, healthcare, and food supply, is particularly vulnerable.

The report was developed by the Swedish Civil Contingencies Agency (MSB) and the Armed Forces to provide a common framework for total defense planning. It responds to a rapidly changing security environment, including lessons from recent conflicts such as the war in Ukraine. Its purpose is to guide municipalities, authorities, and businesses in assessing risks, preparing for potential crises, and ensuring that Sweden can maintain essential societal functions under hybrid and cyber threats.

ARTICLE

The challenger to encryption — Quantum tech

From boardrooms to research labs, one term has been surfacing repeatedly in recent years: Quantum Computers. Touted as the “encryption killer” by some and as a far-off experiment by others, it raises the question—how real is the threat, and who’s actually driving the innovation?

Quantum computing has attracted particular attention in encryption. Today’s cryptography relies on complex mathematical problems that classical computers cannot solve efficiently. Quantum algorithms, such as Shor’s algorithm, often cited as an example of how quantum computing could undermine current encryption.

The looming threat of “Q-Day”, said to be the day where quantum computers will be powerful enough to break current encryption systems, has already pushed governments, defense organizations and companies to prepare for a post-quantum era with quantum-resilient encryption and long-term digital security strategies.

However, investment in quantum computing is accelerating worldwide. Analysts at the Mercator Institute for China Studies (MERICS) note that China advances through state-driven programs, combining large-scale funding with commercial projects. The country publishes extensively and operates machines with several hundred qubits, reports The Quantum Insider. →

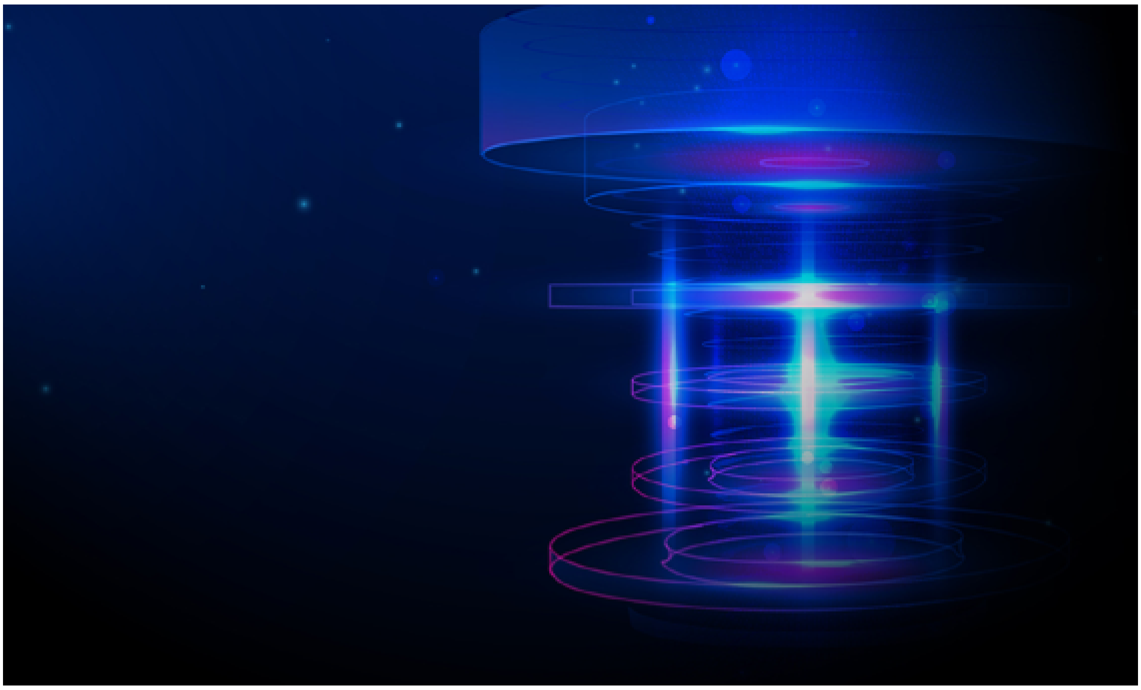
The United States on the other hand follows a different model, pairing federal support with private-sector leadership. Companies like IBM and Atom Computing already run quantum computers exceeding 1,000 qubits, according to HPCwire, placing the U.S. at the technological forefront.

In Europe, the Quantum Flagship program and the 2025 EU Quantum Strategy aim to connect research with real-world applications. Germany plays a prominent role, but officials stress collaboration across member states to build competitive capability by 2030, even while trailing China and the U.S.

> *“Future capabilities explain why governments, companies, and research institutions are investing in quantum-resilient technologies”*

Other countries, including Canada, Japan, and the United Kingdom, have advanced programs, though not at the same scale. Analysts at Cyberwatch note that Russia and India face economic, technical, and political challenges that limit their progress.

Currently, quantum computers remain largely experimental, accessible mainly to large research institutions, major companies, and select government actors. Their immediate impact on everyday digital systems is therefore limited. Although today’s quantum computers cannot yet break current encryption, their potential future capabilities explain why governments, companies, and research institutions are investing in quantum-resilient technologies. →



In early 2025, The European Commission published a coordinated roadmap for the transition to post-quantum cryptography, specifying that Member States should start implementing national strategies by 2026, secure high-risk systems by 2030, and complete the transition as far as possible by 2035.

In addition, several national security agencies such as Sweden's MUST and Germany's BSI, among others, have issued guidance aligned with these objectives, reflecting national steps to adapt cryptographic systems to future quantum capabilities.

Quantum computing is already pushing innovation in research, industry, and cybersecurity.

Understanding the underlying principles, the leading actors, and today's state of development provides a clear picture of where the technology stands and how it may shape encryption and data management in the coming decade. ■

ARTICLE

SWEN — The new Swedish Emergency Network

By the end of this decade, Sweden will retire a national communications system that has served as the backbone of crisis response for nearly 20 years. Its successor promises stronger resilience, higher capacity, and new ways of securing society.

2030 marks the shutdown of Rakel. Today, Sweden's national communications network that enables coordination between emergency services, government authorities, and vital community functions. It has been in use for almost two decades, providing secure voice communication to police, fire and rescue services, ambulance operators, the armed forces, and every municipality and region in the country. Its successor? **SWEN – the Swedish Emergency Network**.

Rakel was built on TETRA technology, which has proven robust and reliable, but also increasingly outdated. It was designed for secure voice calls, not for the demands of modern emergency management. As the digital environment has evolved, the needs of users have changed dramatically.

Responders today require not only encrypted voice but also real-time video from drones and body cameras, secure access to patient data at accident sites, and the ability to exchange situational information instantly. →

Rakel’s limited capacity means it cannot deliver these functions, which are now critical for operational efficiency and safety.

This gap has become even more pressing in light of Europe’s deteriorating security environment. A resilient society depends on the ability to maintain command and control in crisis, conflict, and war. Sweden’s Civil Contingencies Agency (MSB) has therefore been tasked with developing a system that can meet both everyday and extraordinary demands. The outcome is SWEN, a 5G-based network built as a hybrid solution. It combines a dedicated, government-controlled core with commercial mobile infrastructure, ensuring both flexibility and state oversight.

“It equips responders with the tools to share information quickly and securely, even under pressure”

SWEN is more than an upgrade of Rakel. It is a transformation of how emergency communication is conceived. By leveraging modern mobile standards, it enables advanced features such as secure multimedia services, prioritized traffic for critical users during network congestion, and interoperability across national borders.

Finland and Norway are also developing similar solutions, opening opportunities for cross-border collaboration in emergencies.

For municipalities and regions, the transition to SWEN is not optional. Secure communication is a prerequisite for delivering health care, social services, public safety, and crisis management. Every organization currently using Rakel must plan to adapt or replace equipment, update network infrastructures, and prepare staff for new ways of working. →

While this involves costs and effort, it also unlocks new capabilities. The system's design ensures that the fundamental functions of Rakel will remain, but it gradually adds new layers of functionality that improve both response time and decision-making.

The migration from Rakel to SWEN will take place between 2028 and 2029, during which the two systems will run in parallel. This phased approach allows for testing, adaptation, and training before Rakel is fully decommissioned in 2030. All devices and applications connected to the new network must be approved by MSB, ensuring compliance with strict security requirements.

Ultimately, SWEN is about strengthening total defense and crisis preparedness in Sweden. It equips responders with the tools to share information quickly and securely, even under pressure, and it ensures that communication capacity keeps pace with technological and geopolitical realities. For Europe as a whole, it reflects a broader shift toward resilient, digital, and interoperable emergency networks. Sweden is taking an important step, one that will define how critical communication is handled for decades to come. ■

Key takeaways

1. Sweden's 2026–2028 budget allocates billions to strengthen civil and military defense.

2. Global cyber threats, like China's Salt Typhoon, highlight the need for monitoring, patching, and collaboration.

3. Cybersecurity is now central to Sweden's total defense, with new laws, reporting systems, and an expanded National Cybersecurity Center.

4. Quantum computing threatens encryption, prompting investment in quantum-resilient technologies.

5. SWEN will replace Rakel by 2030, providing modern, resilient, and interoperable emergency communications.

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