Monthly Review

Cybersecurity news from around the world

ARTICLE

One year with NATO – Sweden's role in cyber defense

Read article →

SECTRA

General cybersecurity news

1 Cyberwarfare in Ukraine: Lessons shaping global security

By the end of February, it marked three years since Russia's full-scale invasion of Ukraine – a conflict that, as highlighted by Cyberwatch, has reshaped the role of cyber warfare. Initially labeled the world's first unrestricted cyber war, predictions of groundbreaking tactics and decisive battlefield impacts have not materialized. Yet, the cyber dimension has significantly influenced Ukraine, Europe, and global security.

Cyber operations impacting Ukraine predate 2022, with attacks like disruptions to the power grid in 2015-16 and the 2017 Petya ransomware attack serving as precursors. Early in the invasion, Russia targeted critical infrastructure like Viasat satellites but failed to deliver lasting results, focusing instead on intelligence gathering. Ukraine demonstrated resilience, mobilizing volunteers for denial-of-service attacks and espionage with international cyber defense aid.

Russia's cyber operations extended into Europe, where pro-Russian groups like Killnet and APT spread propaganda and targeted infrastructure. Although impactful early on, Europe's defenses strengthened over time. Cyberwatch highlights sabotage in the Baltic Sea and the Kapeka malware of 2024 as examples of ongoing hybrid warfare.
As peace talks stall over Russia's demands for lifted sanctions and Swift access, Cyberwatch reports that cyber threats remain a critical concern. Ukraine's strengthened defenses and Russia's shortcomings will shape future cybersecurity strategies, where cyber weapons are key but cannot replace traditional military power.

2 Sweden introduces new cybersecurity strategy

The Swedish government has announced a new national cybersecurity strategy for 2025–2029, replacing the previous strategy from 2017. The strategy aims to strengthen Sweden's resilience against cyber threats and is an integral part of the country's total defense. It focuses on three pillars: systematic cybersecurity efforts, knowledge development, and the ability to handle incidents.

Civil Defense Minister Carl-Oskar Bohlin, highlights the strategy's importance in protecting society, while Education Minister Johan Pehrson stresses the need to train more cybersecurity experts through universities and colleges. The strategy, which also aligns with the EU's NIS 2 Directive, addresses threats from state actors, cybercriminals, and activists, while aiming to enhance infrastructure and competence across society. The government has also adopted an action plan to implement the strategy's goals.

3 Cybersecurity begins with organizational cultures

While IT solutions, cybersecurity policies, and employee cyber hygiene are vital, an organization's operating culture often has an even greater impact on cybersecurity. Employee well-being, being valued, opportunities to participate in decisions, and clear communication from management directly influence how workers approach security practices. A positive culture fosters vigilance and adherence to guidelines, while negativity can lead to negligence.

High employee turnover is a significant risk factor. Poor working conditions, conflicts, or a challenging culture can result in departures, creating security gaps during transitions. Unfulfilled tasks and added stress on remaining employees increase the likelihood of mistakes or negligence, leaving systems vulnerable to threats.

Ultimately, people – not technology – make an organization secure. While strong tools and systems are essential, human error can override them. Organizations must foster supportive environments that encourage security-conscious behavior and align HR strategies with cyber risk management.

ARTICLE

Europe's reliance on US clouds: A risky dependence

Europe's dependence on US cloud providers threatens its digital sovereignty. With concerns over data access, legal conflicts, and geopolitical instability, the question arises: can Europe afford to entrust its future to foreign-controlled infrastructure?

Europe currently finds itself at a crossroads regarding its digital sovereignty. For decades, European governments, industries, and businesses have become increasingly reliant on major American cloud providers. These platforms underpin essential services ranging from email and data storage to sensitive government operations and critical infrastructure. However, this dependence comes with risks far beyond technical concerns. Legal vulnerabilities, geopolitical instability, and the loss of control over critical data highlight the dangers of entrusting so much of Europe's digital backbone to foreign-controlled providers. European reliance on US tech giants raises pressing questions about sovereignty and security, as American laws continue to apply to data stored within EU borders.

The US CLOUD Act has created direct conflicts with European data protection laws like GDPR, undermining confidence in American providers. Measures by American cloud providers to address these issues remain insufficient to guarantee full protections. →

Trump's prior weakening of EU-US data oversight mechanisms further eroded trust in transatlantic agreements, reports Computer Sweden. As The Register notes, data stored with American-owned platforms remains vulnerable, potentially exploited in geopolitical disputes.

Bert Hubert – an entrepreneur software developer, and part-time technical advisor to the Dutch Electoral Council – a vocal critic of this imbalance, highlights that the problem extends beyond legal concerns into operational risks. With many European governments and businesses deeply integrated into American platforms, a sudden disruption in service could have catastrophic consequences.

"However, solving the issue requires Europe-wide coordination and funding"

The Schrems II ruling emphasized these vulnerabilities, as the European Court of Justice struck down Privacy Shield – a framework for EU-US data transfers – for failing to meet GDPR standards. The case exposed how dependence on US platforms compromises both sovereignty and compliance with European laws.

Adding to these challenges is the centralization of Europe's digital operations. Nearly half of European enterprises rely on US-based cloud providers, writes The Register. The integration of foreign platforms into Europe's digital infrastructure makes it difficult to disentangle critical operations and leaves entire sectors exposed. This dependence also raises the specter of geopolitical risk. Strained relations between the EU and US or shifts in American policy could abruptly revoke access to vital data, as Computer Sweden notes. Such risks undermine the foundation of public service delivery, from healthcare to national security. →

The urgency to reduce this dependence has sparked calls for action across Europe. An open letter to EU leadership in 2025 highlighted the threat posed by reliance on foreign technologies to European sovereignty and growth, reports EuroStack. Signed by diverse businesses, the letter advocated for proactive strategies such as prioritizing sovereign cloud development, industry resource pooling, and procurement obligations for public institutions to “Buy European.” Leveraging open-source frameworks and interoperability standards, the EuroStack initiative emphasized reshaping Europe’s digital landscape to foster autonomy and resilience.

Several European governments have already demonstrated viable approaches. According to The Register, open-source solutions adopted in Germany and Spain showcase alternatives at smaller scales. However, solving the issue requires Europe-wide coordination and funding to create systems capable of rivaling US cloud providers. Investments in local infrastructure and technology are critical, along with fostering transition strategies to help both public and private sectors break reliance on foreign platforms. As Computer Sweden argues, entrenched habits – not technological superiority – drive much of this dependence. Bert Hubert however continues to call for bold government action to innovate at home and build a sustainable, independent digital future for Europe. ■

ARTICLE

One year with NATO – Sweden's role in cyber defense

Sweden has played a vital role in strengthening the alliance's cyber defense. With a focus on innovation and digital resilience, Sweden is helping NATO tackle emerging cyber threats and secure critical infrastructure.

Since joining NATO in 2024, Sweden has emerged as a key player in the alliance's cyber defense and information security efforts. Amid growing threats from cyberattacks, hybrid warfare, and digital espionage, Sweden is applying its technological expertise to strengthen NATO's digital resilience, reports the Swedish government. These efforts reinforce Sweden's dedication to collective defense while addressing rapidly evolving challenges in the digital domain.

Central to Sweden's strategy is its integration with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia, a hub for cybersecurity innovation. Participation in global exercises such as Locked Shields – one of the largest simulations of cyberattacks – highlights the importance of interoperability and rapid response capabilities within NATO. Sweden's contributions ensure the alliance can effectively handle emerging threats to critical infrastructure across member states. →

In 2025, Sweden will amplify its involvement by aligning its national cybersecurity efforts with NATO's broader goals. The establishment of a National Cybersecurity Center demonstrates this commitment, creating a platform to counter advanced cyber threats. Investments in digital infrastructure will enhance NATO's Integrated Air and Missile Defense (IAMD) systems, where Sweden plays a crucial role in mitigating airspace vulnerabilities from cyber disruptions. These initiatives underline Sweden's focus on cyber resilience as an integral part of NATO's deterrence and defense.

"Sweden strengthens NATO's current capabilities while laying the groundwork for future security"

Sweden is also prioritizing cybersecurity within its civil defense strategy by protecting essential societal functions like transportation, communication, and healthcare from cyberattacks. Collaborations with NATO allies ensure expertise sharing in cyber-resilient systems and secure communication. Exercises like Cyber Coalition highlight Sweden's contributions to preventing data breaches, improving network security, and ensuring digital infrastructure can withstand ransomware and disinformation campaigns.

Technological innovation further strengthens Sweden's role within NATO. Partnerships with leaders in the tech sector advance secure communications and satellite-based surveillance. These innovations bolster NATO's capabilities to detect, deter, and respond to hybrid threats, creating a more robust defense against digital aggression. Sweden's focus on cybersecurity research is evident in an over 50 percent increase in funding for technology development by 2027, according to the Swedish Ministry of Defense. →

Psychological defense is another pillar of Sweden's cyber strategy. Proactively countering disinformation campaigns ensures public trust and resilience during crises. As a NATO member, Sweden aims to expand these measures, supporting collective resilience across the alliance.

Sweden's integration into NATO underscores the growing importance of cyber defense in modern security strategies. By prioritizing digital resilience, secure communication systems, and technological innovation, Sweden strengthens NATO's current capabilities while laying the groundwork for future security. Amid NATO's 75th anniversary celebrations in 2024, Sweden's contributions in the digital sphere exemplify the alliance's commitment to adapting to an ever-changing security landscape. ■

Key takeaways

1. Ukraine's cyber resilience reshapes the landscape of modern digital warfare.
2. Sweden launches 2025–2029 cybersecurity strategy to boost resilience, knowledge, and incident preparedness.
3. Cybersecurity hinges not just on tech, but on healthy workplace culture and engaged employees.
4. Experts call for Europe to reduce reliance on US clouds to protect it's digital sovereignty.
5. Sweden help strengthens NATO cyber defense through innovation and resilience.

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