Monthly Review

Cybersecurity news from around the world

INTRODUCTION 2

GENERAL CYBERSECURITY NEWS 3

ARTICLES

Global spyware threat continues to grow 5

Navigating the threat landscape — 2026 outlook 8

KEY TAKEAWAYS 12

ARTICLE

Navigating the threat landscape — 2026 outlook

Read article →

SECTRA

Newsletter introduction

Welcome to the first Sectra Cybersecurity Newsletter of 2026. We hope you've had a well-earned break and are ready to navigate another year of rapid change in the cyber landscape.

This month, we examine the Pentagon's renewed focus on secure mobile communications, Sweden's new NIS2-aligned cybersecurity legislation, the rise of AI-driven Android malware, and evolving global spyware threats.

Stay resilient. Stay secure.

General cybersecurity news

1 New year — new regulations

On January 15, the Swedish government enforced the new cybersecurity law, aligning national regulations with the EU's NIS2 directive. The law introduces major changes affecting organizations of all sizes.

1. Whole-organization scope

Once an organization falls under the law, everything is in scope — not just critical systems or select services. HR, finance, internal tools, subsidiaries, and support functions all count. It's no longer possible to isolate "regulated" IT. This forces enterprise-wide cybersecurity governance, requiring organizations to secure their entire digital ecosystem.

2. Mandatory, provable security governance

Organizations must register with the relevant authority and implement a documented, systematic cybersecurity program, including risk management, incident handling, business continuity, supply-chain security, and access controls. Regulators now expect evidence and structure, not just intentions.

3. Fast incident reporting and executive liability

Serious incidents must be reported within 24 hours, and top management is explicitly accountable. Cybersecurity is now a board-level responsibility, with potential fines or personal consequences.

2 Pentagon enhances mobile security after Signalgate

Insecure mobile communications remain one of the most operationally consequential cyber risks. The 2026 National Defense Authorization Act (NDAA) — the annual U.S. defense policy law — now mandates that, within 90 days of enactment, the Department of Defense (DoD) must procure mobile devices for senior officials under contracts requiring enhanced cybersecurity protections. These include encrypted data, periodic rotation of device identifiers to prevent tracking, and continuous monitoring capabilities. Within 180 days, the Secretary of Defense must report to Congress on implementation, affected personnel, and associated costs.

The move follows the Signalgate incident, where the DoD head allegedly shared strike details over an unsecure Signal channel, exposing critical operational data. This legislation signals a decisive shift toward hardening mobile endpoints in national security contexts.

3 AI-powered malware is being distributed through Xiaomi's official app store

Researchers at Dr.Web have discovered a new family of Android trojans being spread through GetApps, Xiaomi's official app store. The new malware uses AI-powered visual analysis (via TensorFlow) to perform click-fraud by recognizing and clicking on ads in a hidden browser.

More concerning is a built-in feature that lets attackers manually control the device if the AI fails. This allows them to view the screen and interact with it remotely, opening the door to data theft and other malicious activity. The malware has been found in various apps, including games and pirated versions of popular services like Spotify and Netflix. Legitimate-looking games passed Xiaomi's checks initially, with the malware added later through updates.

Children are a key target, increasing risk — especially when they use a parent's device, which may also be used for work.

ARTICLE

Global spyware threat continues to grow

Commercial spyware and the companies that supply them have once again been in the headlines around the world. Well-known spyware includes, for example, the Predator and Pegasus spyware developed by the Israeli companies Intellexa and NSO Group, which have been used to spy on the political opposition, business executives and journalists in different countries, among other things.

Spyware allows an attacker to gain access to the files, camera, microphone, and other functionalities of the target's smartphone without the victim's knowledge. Spyware can often be delivered to the target devices using the so-called zero-click method, where the malware is installed on the device without the victim noticing and does not require security errors by the victim. In other words, they are effective intelligence gathering tools.

Recent developments in the phenomenon include reports of the spread of spyware to new countries and the removal of those responsible for them from the U.S. sanctions list. On the other hand, case law related to spyware has also begun to appear. →

One notable development is a U.S. federal ruling that prohibits NSO Group from using WhatsApp to deliver spyware after the company targeted up to 1,400 users. The decision, reached after a six-year legal process, also requires NSO to compensate Meta. Similar delivery methods have been linked to other actors, including Intellexa and Paragon Solutions.

"Overall, according to data from the US authorities in 2025, spyware is believed to be in use in almost a hundred countries."

To balance the positive legal developments, there have also been less favourable developments in the spyware landscape. At the end of December, the U.S. administration removed three individuals associated with commercial spyware development from its sanctions list. While the administration described the move as part of routine administrative processes, several observers expressed concern that the decision may complicate ongoing international efforts to limit the spread and misuse of commercial spyware.

A recent report by Recorded Future, a producer of cyber threat intelligence, added more fuel to the fire. It stated that the products of Intellexa, the provider of the Predator spyware, have been detected for the first time in Iraq and Pakistan, among other countries. In addition, Saudi Arabia, Kazakhstan, Angola and Mongolia, among others, are users of this spyware.

Overall, according to data from the US authorities in 2025, spyware is believed to be in use in almost a hundred countries around the world. In authoritarian countries, they pose a clear threat not only to the state's own citizens, but also to diplomats and business representatives operating in the countries. Abuses have also been suspected in Europe, for example, in Italy and Spain.→

A quick solution to the spyware problem is unlikely. At the beginning of December, Google also announced that it had detected that Intellexa was rapidly deploying new zero-day software vulnerabilities to infiltrate devices. The international Pall Mall process, a diplomatic initiative between the UK and France to tackle spyware, has also progressed slowly. In the spring of 2025, a non-binding policy paper "The Pall Mall Process Code of Practice for States" was produced, which reviews the problems and recommendations in the field.

The spyware problem affects several groups of people. Diplomats have been reported to have been targeted, in addition to which journalists, political decision-makers and key personnel of significant companies belong to risk groups. Preparing for spyware is challenging, as it is almost impossible for the user to detect. There is a constant race between spyware companies and the companies that develop the software they target between finding vulnerabilities and fixing them.

Both Google and Apple have at least some kind of capabilities for detecting spyware. Both have made it a practice to send notifications and instructions to users' devices if indicators of spyware are detected. These include, among other things, timely updates to the operating system and the introduction of multi-factor authentication. ■

ARTICLE

Navigating the threat landscape — 2026 outlook

Nation-state cyber operations are evolving beyond short-term battlefield support into long-range strategic tools. Russia, China, Iran, and North Korea are expanding espionage, influence, and disruption efforts — raising the stakes for governments and critical infrastructure operators in 2026.

Nation-state cyber operations are entering a more strategic phase, with leading threat actors broadening their objectives beyond immediate tactical gains. According to the Google Cloud Security team's annual threat report, Russia, China, Iran, and North Korea are increasingly using cyber capabilities to secure long-term political, economic, and military advantage, while laying groundwork for future crises.

Russia: from battlefield support to global positioning

Russia's cyber activity continues to support its war against Ukraine, but the scope is widening. Espionage against Ukrainian government and defense institutions remains a priority, largely to inform kinetic operations and political negotiations. However, as noted by Google Cloud researchers, Russian intelligence collection expanded significantly across Europe and North America during 2025, signaling a shift toward broader strategic positioning. →

This expansion has been accompanied by the adoption of new tactics, techniques, and procedures, suggesting sustained investment in advanced cyber capabilities. While destructive attacks have declined since their 2022 peak, the report highlights continued risks to operational technology environments. An April 2025 compromise of a Norwegian dam underscores the potential for OT-focused disruption against critical infrastructure. In parallel, pro-Russian information operations are expected to intensify, particularly around Western elections, amplifying narratives of foreign interference and undermining trust in democratic processes.

"As geopolitical friction intensifies, organizations should expect cyber operations to become more sophisticated."

China: scale, stealth, and supply chains

China remains the most active cyber power by volume and reach. The Google Cloud Security Team reports that Beijing's operations are increasingly characterized by stealth and scalability, with frequent use of zero-day vulnerabilities and a strong focus on edge devices that lack robust endpoint detection.

Supply-chain compromise continues to be a preferred access vector, exploiting trusted third-party relationships to gain downstream access into high-value targets. The semiconductor industry is identified as a key focus area, reflecting both geopolitical competition and the accelerating demand driven by artificial intelligence. Alongside cyber espionage, pro-PRC (People's Republic of China) information operations aim to shape global narratives, portraying China as a stabilizing force while discrediting the United States and regional competitors. →

Iran: agility across domains

Iranian cyber operations remain diverse, blending espionage, disruption, hacktivism, and financially motivated activity. According to the report, regional tensions—particularly those involving Israel and the United States—are sustaining aggressive campaigns, including elevated risks of wiper malware.

Iranian information operations are also evolving. Google Cloud analysts highlight growing use of AI-generated content and coordinated inauthentic behavior, especially on platforms such as Telegram, to influence elections and amplify geopolitical messaging. Tehran's rapid adaptation following global events, including the April 2025 Pahalgam terror attack, demonstrates its ability to exploit periods of heightened international tension. Political organizations, regime critics, and technologies with military relevance remain consistent targets.

North Korea: cybercrime as state revenue

North Korea continues to pair traditional espionage with large-scale financial theft. Following a record cryptocurrency heist in 2025, estimated at $1.5 billion, the report indicates that Pyongyang's operators are refining their techniques, combining sophisticated social engineering with deep reconnaissance of cloud environments.

These operations pose significant risks to digital asset platforms and financial services providers, reinforcing the need for advanced fraud detection, identity controls, and cloud security hardening. →

Operational considerations for 2026

As nation-state cyber operations grow more sophisticated, organizations handling sensitive information or critical infrastructure should take the following into account:

- Ensure confidentiality and integrity of sensitive communications, particularly for leadership and mission-critical operations, as adversaries increasingly target interception points and weak encryption.
- Validate the security posture of partners and service providers to reduce the risk of cascading supply-chain compromises.
- Implement defense-in-depth measures, including strong endpoint protection, network segmentation, and hardened edge devices to counter zero-day exploitation.
- Review isolation strategies and contingency planning for operational technology environments to limit the impact of disruptive attacks.
- Monitor for influence operations and validate information sources to maintain resilience against disinformation.
- Begin assessing cryptographic agility to protect long-term data confidentiality as quantum computing advances.

As geopolitical friction intensifies, organizations should expect cyber operations to become more sophisticated, persistent, and tightly linked to national policy objectives. ■

Key takeaways

1. Sweden's new NIS2-based law demands full-scope cybersecurity, proof of governance, and rapid incident reporting with executive accountability.

2. U.S. law requires senior officials to adopt more secure mobile devices after the Signalgate incident.

3. A new Android trojan in Xiaomi's app store uses AI for click-fraud and can let attackers remotely control infected devices.

4. Global spyware is expanding worldwide as legal and diplomatic efforts struggle to contain its misuse.

5. Nation-state cyber operations are expected to intensify in 2026 as major powers expand long-term espionage, disruption, and influence campaigns.

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