Monthly Review

Cybersecurity news from around the world

ARTICLE

Threat actors and their recent methods

Read article →

SECTRA

Newsletter introduction

The sun is finally starting to bring warmth back to Europe, much needed given the escalations and conflicts happening around the world.

For this March edition, we've compiled a mix of topics for you: how to set up a secure workplace and key measures to consider, Sweden's nationwide roaming function designed to activate during a crisis, the recent attacks on Signal and WhatsApp users, and a short threat assessment outlining what China, Iran, and Russia are targeting and the methods they use.

Stay resilient. Stay secure.

General cybersecurity news

1 How to ensure a safe remote workplace

Remote access enables employees, contractors, and partners to reach organizational resources from outside the corporate network using VPNs, secure access service edge (SASE), or zero-trust network access (ZTNA), according to a TechTarget article on secure remote access best practices. While essential for hybrid work, it increases cybersecurity risk, as compromised endpoints, weak authentication, or unmonitored activity can expose sensitive systems.

Organizations address these risks with remote access policies that define allowed devices, access methods, acceptable use, and consequences for violations. Providing organization-issued devices ensures endpoints meet security standards. Devices undergo cyber health checks for updated operating systems, active antimalware, configured firewalls, and absence of malware. Multi-factor authentication (MFA) strengthens login security, and network communications are encrypted. Zero-trust principles restrict access based on verified users and devices. Users receive training on secure practices, access is limited to those who require it, and accounts are revoked when no longer necessary. Continuous monitoring of servers and user activity identifies anomalies and potential breaches.

These practices protect company data, maintain reliable access for authorized users, and reduce the chance that remote work introduces vulnerabilities into critical systems.

2 Sweden keeps phones ON

Sweden has implemented a national roaming function for mobile networks to ensure communication continues during crises or war.

The government can trigger this "heightened preparedness" measure if national security is threatened. When activated, users of 4G and 5G networks—including Telia, Tele2, Telenor, Tre, and their resellers—can manually switch to another operator's network if their usual one fails, maintaining calls, texts, and data.

This system is unique in the EU, as most countries have no comparable nationwide contingency roaming. It is part of Sweden's broader strategy to strengthen resilience in critical infrastructure and ensure access to vital information for all citizens during emergencies.

3 China-linked hackers target telecom networks

Researchers at Cisco Talos recently disclosed a cyber-espionage campaign attributed to a China-linked threat actor tracked as UAT-9244. The activity, publicly reported in March 2026, shows attackers targeting telecommunications providers in South America since at least 2024.

Investigators identified three previously undocumented malware tools—TernDoor, PeerTime, and BruteEntry—capable of compromising Windows, Linux, and network-edge devices while maintaining persistent access across telecom infrastructure.

The findings reinforce the need to reduce exposure across communication environments. Organizations should prioritize rapid patching, strong credential management, network segmentation, and continuous monitoring for indicators of compromise. Equally important is ensuring that sensitive coordination and decision-making occur over trusted, encrypted channels that remain separate from widely exposed digital platforms, limiting adversaries' ability to observe or intercept critical communications.

ARTICLE

Signal and WhatsApp targeted by phishing campaigne

You get a message with a QR code or link, seemingly from Signal or WhatsApp support. You scan it, and without realizing it, an attacker can pair their device with yours. Authorities across Europe report that these phishing and social engineering campaigns are affecting two of the most popular messaging apps.

In early 2026, Dutch intelligence agencies AIVD and MIVD, Germany's BfV and BSI, and Sweden's CERT-SE reported campaigns targeting Signal and WhatsApp accounts used by high-value individuals, including government officials, military personnel, diplomats, and journalists.

The campaigns rely on social engineering and phishing rather than technical vulnerabilities or malware. Attackers impersonate support channels or chatbots, requesting verification codes, PINs, or asking users to scan QR codes to link accounts to devices they control. Through these methods, actors can gain access to one-to-one and group chats, as well as contact lists. Both full account takeovers and pairing with attacker-controlled devices have been observed. The campaigns exploit legitimate features, such as Signal and WhatsApp's linked-device functionality, rather than flaws in the encryption itself.

Dutch authorities note that Signal's reputation for reliability and end-to-end encryption makes it a target for these operations. While the apps themselves remain technically secure, individual accounts are compromised when users provide sensitive authentication information. →

Similarly, German authorities highlight that phishing messages often create a sense of urgency, misleading users into sharing codes or approving new devices. CERT-SE also reports comparable attacks and emphasizes that phishing can involve QR codes, fake support messages, or other manipulations of app functionality.

Here are some practical measures to consider

- Do not share verification codes or PINs with anyone.
- Regularly review linked devices and remove any unrecognized or suspicious devices.
- Enable Signal's Registration Lock (or equivalent), which requires a PIN for account registration on new devices.
- Verify suspicious messages through independent channels, such as email or telephone, rather than relying on the messaging app itself.
- Keep apps updated, ideally using automatic updates.
- Adjust privacy settings where possible, both in mobile and web applications.
- Monitor group chats for duplicate or unfamiliar accounts.
- Report potential compromises to your organization's information security team.

The combined observations from multiple European authorities illustrate that these campaigns focus on the misuse of account features and social manipulation. Awareness of account activity, careful handling of authentication information, and vigilance regarding unusual requests or linked devices are highlighted as key elements for maintaining account integrity. ■

ARTICLE

Threat actors and their recent methods

European intelligence agencies note that China, Iran, and Russia have enhanced their threat intelligence methods. Amid regional tensions and U.S. actions, Iranian linked cyber activity is under heightened observation, highlighting why security teams should remain alert to evolving Iranian cyber activity.

In 2025–2026, European security authorities have reported elevated activities by foreign state actors targeting Western countries. Operations ranged from intelligence collection and cyber intrusions to influence campaigns and illicit technology acquisition. Coordination between hostile states is increasing, amplifying the complexity of threats across Europe.

The EU's cybersecurity authority, CERT-EU, analyzed over 300 open-source reports in February 2026, identifying ongoing cyberespionage, cybercrime, and influence operations across Europe. Highlighted is the phishing campaign—stated in article four—that focused on high-profile Signal users, including politicians, military personnel, and journalists.
At the same time, the Russia-linked group APT28 exploited a newly disclosed Microsoft Office vulnerability to target users in Central and Eastern Europe. And China-linked actors conducted multiple campaigns, including supply chain compromises and intrusions targeting telecom and government entities globally. →

Other incidents included distributed denial-of-service attacks on German transport infrastructure and a large-scale data breach affecting a Dutch telecom provider, exposing millions of customer records.

These cases illustrate the range of ongoing activity, from espionage to disruption and data exploitation.

In late 2025, the EU Council sanctioned twelve individuals and two entities linked to Russian hybrid threats, including interference and cyber operations targeting member states.

"Coordination between hostile states is increasing, amplifying the complexity of threats across Europe"

The Swedish Security Service, SÄPO, reports that Russia, China, and Iran are actively targeting Sweden. Russia is the most immediate threat, with a focus on political decision-making, NATO cooperation, and the defense industry. Since the invasion of Ukraine, Russian operations have become more risk-tolerant and opportunistic, extending beyond traditional conflict zones.

Influence campaigns aim to weaken Western support for Ukraine and increase societal polarization. Methods include espionage, hybrid tactics, and sabotage.

China represents a long-term strategic challenge, particularly in economic and technological domains. Its intelligence services target Swedish companies, universities, and research institutions to acquire sensitive knowledge and advanced technology. Methods range from cyber intrusions to investments and intermediary structures designed to bypass regulatory scrutiny. Chinese operations also include monitoring diaspora communities and opposition groups, reflecting a sustained and systematic approach. →

Iran's activities are more variable but remain significant. Intelligence operations have included surveillance, intimidation, and coercion targeting opposition groups, alongside efforts to acquire technology related to weapons development. In some cases, criminal networks have been used as proxies for violent acts.

Cyber operations are increasingly integrated into broader security dynamics. Within NATO, cyber is recognized as a distinct operational domain alongside land, air, sea, and space. Cyberattacks are used to gather intelligence, disrupt societal functions, and target critical infrastructure. Russia's war in Ukraine has demonstrated how cyber operations are embedded in modern warfare, while China continues to conduct activities that challenge allied security.

Elsewhere in Europe, Finland's security service, SUPO, reports Russian actors exploiting supply chain vulnerabilities and using proxies to gather intelligence on NATO and infrastructure. Germany's domestic intelligence service, BfV, identifies Russia and China as leading espionage threats, with Iran involved in targeted cyber and influence operations.

Across Europe, state-backed activities by Russia, China, and Iran remain persistent, coordinated, and multifaceted. ■

Key takeaways

1. Remote work security requires zero-trust architecture, MFA, and continuous monitoring to protect organizational systems.

2. Sweden's national roaming system lets citizens manually switch mobile operators during crises, ensuring communication continuity.

3. China-linked groups embed malware in telecom infrastructure, emphasizing the need for rapid patching and network segmentation.

4. Phishing campaigns exploit Signal and WhatsApp's device-linking features by tricking users into sharing codes or scanning malicious QR codes.

5. Russia, China, and Iran intensify coordinated cyber operations across Europe using supply chain attacks 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