Monthly Review

Cybersecurity news from around the world

INTRODUCTION 2

GENERAL CYBERSECURITY NEWS 3

ARTICLES

A rising trend — persistent access, not disruption 5

CERT-EU: A year defined by endurance 8

KEY TAKEAWAYS 11

ARTICLE

CERT-EU: A year defined by endurance

Read article →

SECTRA

Newsletter introduction

In this month's newsletter, we highlight developments that shape how security risk is changing over time.

From the transition to post quantum cryptography (PQC), to persistent access in critical infrastructure and the growing role of AI in vulnerability discovery, the common theme is long term resilience. The articles below offer context on what to watch, why it matters, and how today's decisions influence future exposure.

Stay resilient. Stay secure.

General cybersecurity news

1 Googles shift to post-quantum cryptography

Google has set an early 2030 target for its transition to post quantum cryptography, describing the shift as a gradual engineering effort rather than a single upgrade. The company outlines a phased approach in which quantum resilient algorithms are introduced incrementally across core services over several years.

The motivation is tied to data longevity. Google notes that encrypted data intercepted today can be stored and decrypted later, once potential quantum capabilities emerge. This so called “harvest now, decrypt later” risk is less about immediate system compromise and more about long term exposure of sensitive information. To address this, Google emphasizes the need to inventory existing cryptographic use, understand dependencies, and enable gradual replacement over time. These steps reflect the reality that modern systems rely on layered and interdependent cryptographic components, making sudden transitions impractical. When investing in new systems, the key question is therefore not only how secure they are today, but whether they are designed to adapt as cryptographic assumptions change.

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

2 What does post-quantum cryptography mean?

The term “quantum safe” refers to cryptographic solutions designed to withstand attacks from both classical and quantum computers. It does not imply absolute or provable security. Instead, it means the solution relies on cryptographic algorithms and methods that, based on current scientific knowledge, have no known weaknesses even if a large scale quantum computer was available.

Modern cryptography depend on assumptions about computational difficulty rather than guarantees. Quantum computing challenges some of those assumptions, but not all. While quantum computers excel at solving certain specific problems, they offer no universal advantage. Post-quantum cryptography (PQC) is built on problems widely believed to remain hard even in a quantum scenario. The claim is therefore grounded in current research and the absence of known quantum attacks, not certainty about the future.

3 Mythos — a new wave of AI-driven risk

A new experimental AI model called Mythos, developed by the AI giant Anthropic, has rapidly changed how cybersecurity is understood.

Instead of detecting known weaknesses, Mythos is designed to actively search for unknown vulnerabilities, reason about them and in some cases even generate code to exploit them. The model has made the Swedish National Cyber Security Center coordinate, together with AI Sweden and the Swedish defense, among others, to see how this development can be translated into operational readiness. The focus is on whether critical systems can remain resilient in an environment where vulnerabilities can be discovered autonomously.

The core question here is who can control systems that can both secure and destabilize digital infrastructure.

ARTICLE

A rising trend — persistent access, not disruption

The attacks making headlines are becoming less representative. Reporting shows state-linked cyber operations moving from visible disruption toward persistent access embedded deep inside network infrastructure. Access itself is treated as a strategic asset, enabling long-term intelligence collection without drawing attention.

Recent reporting highlights a consistent approach in state linked cyber operations. Rather than prioritizing immediate disruption, actors increasingly focus on establishing durable access positioned deep within network infrastructure. In practical terms, this means gaining a foothold in systems that quietly handle traffic for many users, instead of attacking individual devices directly. Access itself is treated as a long term asset, enabling selective intelligence collection with limited visibility.

This pattern is described in detail by the UK National Cyber Security Centre (NCSC) in its advisory on APT28's exploitation of routers to enable Domain Name System (DNS), hijacking. The NCSC explains how the Russian state linked actor has compromised vulnerable routers to overwrite Dynamic Host Configuration Protocol (DHCP) and DNS settings, redirecting traffic through attacker controlled DNS servers.

DNS normally acts as the internet's address book, so altering it allows an attacker to quietly steer users to malicious infrastructure without changing what the user typed or clicked. →

According to the advisory, this manipulation enables man in the middle activity that allows the harvesting of passwords, Open Authorization (OAuth) tokens, and other authentication material from web and email services, creating sustained exposure rather than immediate impact.

The NCSC further notes that the operation is opportunistic. Rather than targeting a narrow set of victims from the outset, APT28 is described as affecting a wide pool of exposed devices before narrowing focus to users and networks of likely intelligence value. Routers are particularly attractive for this purpose because they sit directly on the data path for all connected devices and are often lightly monitored once deployed.

Similar reporting illustrates how these mechanics translate into real world operations. Coverage by Politico describes a large scale campaign in which Russia's GRU linked hacking group Fancy Bear, also tracked as APT28, compromised Wi Fi routers across Western countries to spy on military, government, and critical infrastructure targets. By operating at the router level, attackers were able to observe traffic from otherwise well secured laptops and mobile devices, even when endpoint security controls remained intact.

Reducing exposure to this type of risk means limiting implicit trust in underlying networks by enforcing strong authentication, encryption, monitoring, and integrity end to end, even when traffic appears to originate from inside the network. By segmenting secure communication from the transport layer and centralizing control and policy enforcement, compromised routers or DNS paths become far less useful to an attacker over time. ■

ARTICLE

CERT-EU: A year defined by endurance

The 2025 threat landscape shows how state linked cyber activity is increasingly shaped by persistence rather than disruption. Long term access, not visible incidents, defined the most consequential activity of the year.

CERT EU's Threat Landscape Report 2025 describes a year in which the most consequential state linked cyber activity was shaped less by visible disruption and more by the quiet accumulation of access. Rather than drawing attention through high impact attacks, adversaries established footholds in widely deployed systems and maintained them long enough to remain useful. The defining feature was not scale or spectacle, but endurance. →

EXPLAINER — CERT-EU

CERT-EU is the European Unions Computer Emergency Response Team (CERT) for its institutions and agencies. It detects, responds to and coordinates cyber incidents across the EU system. It also shares threat intelligence and supports organizations in improving cyber resilience and managing vulnerabilities.

Within CERT EU's dataset, cyberespionage and prepositioning account for 38 percent of recorded malicious activity. In practical terms, prepositioning refers to establishing access early and preserving it as a standing capability, rather than using that access immediately to disrupt operations. Incident analysis in the report helps explain why this model continues to prevail. In 2025, the most consequential initial access resulted from the exploitation of vulnerable, internet facing software. Edge devices such as firewalls, VPN appliances, and network management solutions featured prominently. CERT EU reports nine significant incidents during the year, with exploitation serving as the initial access vector in seven cases, including two zero day vulnerabilities.

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

These systems sit at the boundary of organizational networks and are operationally critical. As a result, they are difficult to take offline and are typically managed with a focus on availability and continuity rather than on detecting long term hostile presence. Once compromised, they can support extended access with limited interaction with internal systems, reducing the risk of detection while maintaining operational value.

This access first logic becomes clearer when viewed in a geopolitical context. CERT EU notes that events such as summits, elections, armed conflicts, and sanctions repeatedly coincided with increased malicious activity across the EU ecosystem.

Denial of service attacks frequently occurred during these periods, but the report observes that they rarely escalated into incidents with lasting impact on Union entities. →

More durable value instead came from campaigns that used these moments to expand access through credential harvesting, spearphishing, impersonation, and reconnaissance. High profile events created predictable engagement windows, allowing activity to blend into elevated background noise while access opportunities expanded.

The report further emphasizes that strategic cyber interference during such periods does not primarily aim to cause immediate operational failure. Instead, it enables access staging and exposure mapping that remain relevant long after the triggering event has passed. In this context, timing acts as a multiplier for positioning rather than as a driver of short term impact.

Destructive cyber activity represents a smaller share of the threat landscape described by CERT EU, but its presence remains significant. Wiper malware was largely confined to active conflict zones, most notably in connection with Russia's war against Ukraine. At the same time, CERT EU documents an attempted wiper attack against a Polish renewable energy operator. While the incident did not disrupt national energy supply, it is cited as a rare example of potential spillover beyond an active conflict zone.

Overall, the report does not portray a landscape defined by constant disruption. Instead, it points to persistent presence inside systems that are widely deployed, implicitly trusted once installed, and difficult to scrutinize in depth after compromise. ■

Key takeaways

1. Google is treating post-quantum cryptography as a gradual shift, building crypto agility now to reduce future “harvest now, decrypt later” risk.

2. Post-quantum cryptography refers to algorithms believed to remain secure against both classical and quantum attacks, based on current knowledge rather than absolute guarantees.

3. AI model Mythos turns vulnerability discovery into an automated capability that must be governed, not just defended against.

4. Modern cyber operations create impact by maintaining quiet access rather than causing visible disruption.

5. Resilience increasingly depends on detecting and reducing persistent access, not just responding to incidents.

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