SECTRA NEWSLETTER – JUNE 2025

Monthly Review

Cybersecurity news from around the world

ARTICLE

State-sponsored cyber operations in 2025

Read article →

SECTRA

Newsletter introduction

Europe is accelerating its journey toward digital sovereignty amid rising geopolitical tensions and growing cyber threats. This shift demands not only new policies and infrastructure but also a deep understanding of evolving cyberattacks and state-driven operations targeting critical systems.

In this issue, we explore how Europe's strategic efforts to regain control over its digital future intersect with the realities of modern cyber warfare and daily cyber risks.

This is our last issue before the summer break. We'll be back in August with new updates on cybersecurity trends and threats. Until then, stay secure—and have a great summer!

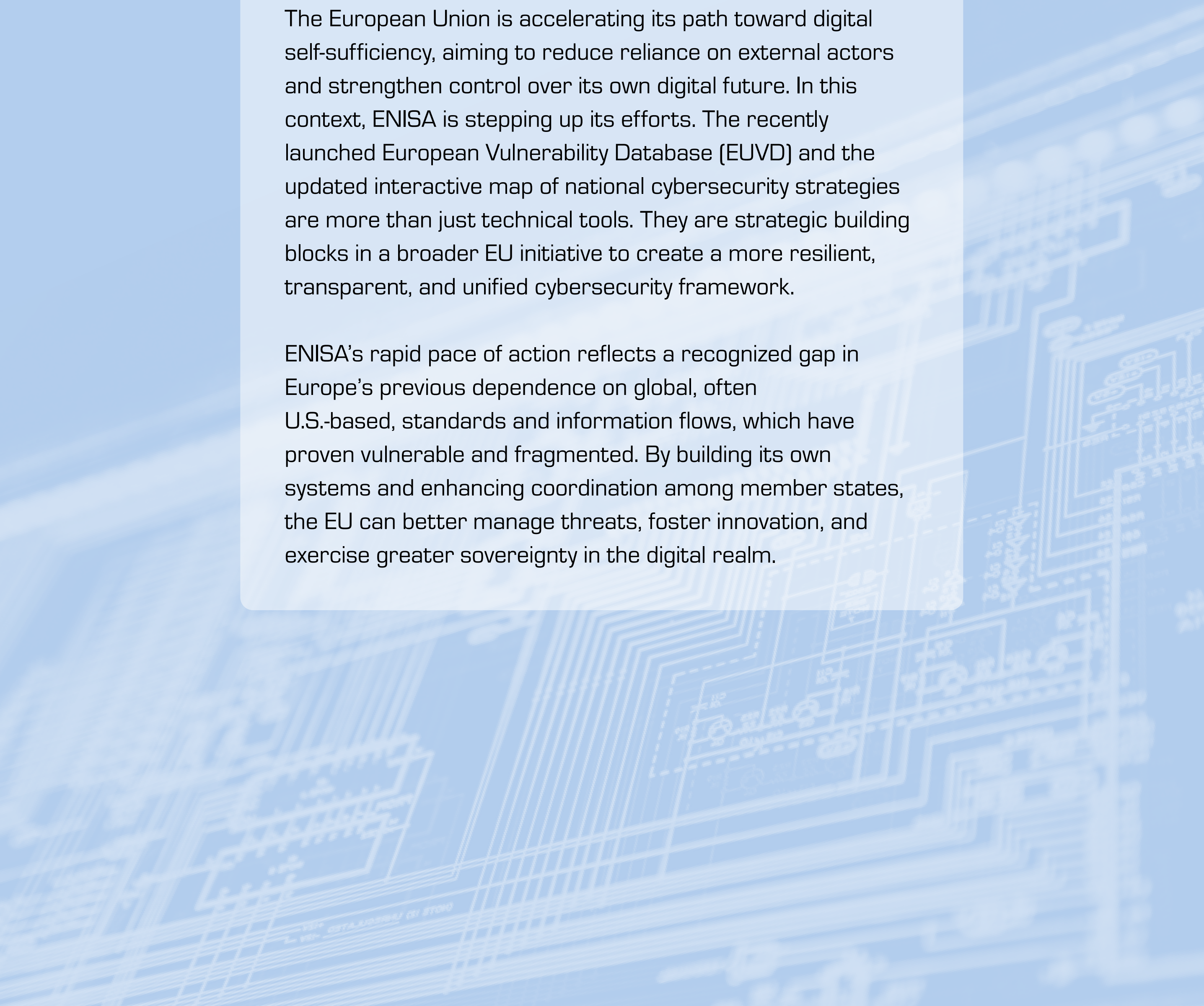
General cybersecurity news

1 Europe’s move toward digital sovereignty with ENISA’s new initiatives

Do you know who controls your data? With rising global tensions and growing digital threats, Europe is pushing for more independence in how it manages cybersecurity. New tools from ENISA signal a shift toward self-reliance, transparency, and shared defenses across EU countries.

The European Union is accelerating its path toward digital self-sufficiency, aiming to reduce reliance on external actors and strengthen control over its own digital future. In this context, ENISA is stepping up its efforts. The recently launched European Vulnerability Database (EUVD) and the updated interactive map of national cybersecurity strategies are more than just technical tools. They are strategic building blocks in a broader EU initiative to create a more resilient, transparent, and unified cybersecurity framework.

ENISA’s rapid pace of action reflects a recognized gap in Europe’s previous dependence on global, often U.S.-based, standards and information flows, which have proven vulnerable and fragmented. By building its own systems and enhancing coordination among member states, the EU can better manage threats, foster innovation, and exercise greater sovereignty in the digital realm.



2 Danish cities break with Microsoft—signals broader EU shift

Copenhagen and Aarhus are phasing out Microsoft products to boost digital sovereignty and reduce reliance on U.S. technology amid growing concerns over the CLOUD Act, which grants U.S. authorities the right to access data stored abroad by American companies. Denmark's Ministry of Digitalization emphasizes that this move is about ensuring control and resilience, not rejecting global firms. However, experts warn the transition is complex—Microsoft is deeply embedded in municipal systems, and switching may lead to temporary drops in user experience and increased costs. Supporters argue that reducing dependence on foreign tech is crucial to limit external risks and foster European innovation.

For users, the change brings both uncertainty and opportunities to develop IT systems better aligned with local needs and regulations. Denmark's shift mirrors a broader European debate on balancing security, control, and practicality in an interconnected digital landscape.

3 Amazon establishes German parent company for EU sovereign cloud

Amazon Web Services (AWS) is strengthening its EU presence by establishing a standalone parent company in Germany to manage its new AWS European Sovereign Cloud. Launching its first region in Brandenburg by the end of 2025, this cloud service will operate all technical support, customer service, and data processing entirely within the EU. A "sovereign cloud" means all data and operations stay within EU jurisdiction, ensuring tighter control over privacy and compliance. This setup ensures compliance with strict EU data laws, including GDPR, German federal data protection, and the new NIS2 Directive on cybersecurity regulations.

For organizations seeking NIS2-compliant providers, AWS's move offers enhanced legal certainty and data control, easing their own regulatory compliance. The initiative represents an investment of around €7.8 billion through 2040 and is expected to create nearly 3,000 jobs annually in Germany. AWS's move addresses growing demand for cloud solutions that offer full control over data and security—a key factor in Europe's drive for digital sovereignty and stronger cybersecurity.

ARTICLE

Awareness is your first defense

Cyberattacks don't just hit states or IT—they target everyday habits. And when routines slow down, like in summer, attackers strike. Here are five common methods that exploit trust, curiosity, and human behavior.

Phishing: deception at scale
An email that looks like it's from your CEO, asking you to review an urgent invoice. A message from your bank about a suspicious login. These are classic phishing lures, crafted to trick you into clicking, downloading, or revealing sensitive information.

Phishing remains one of the most widespread and effective cyberattack methods. Fraudulent emails, texts, or messages often appear to come from trusted sources like banks, colleagues, or service providers. The goal is to trick recipients into clicking malicious links, downloading malware, or revealing login details, card numbers, or internal documents. Its success relies on social engineering—exploiting human trust and urgency. Many phishing campaigns are now personalized through leaked data or social media profiling, making them even harder to detect. This more targeted version is known as spear phishing.

USB drops: physical vectors for digital infiltration
Not all cyberattacks happen online. Some start in the real world, with a USB drive left in a parking lot, lobby, or café. →

Attackers exploit human curiosity, hoping someone will plug in the device without suspicion. Once connected, the infected USB can silently execute malware, infecting the system, stealing data, or installing backdoors for future access. One well-known case involved attackers scattering USBs outside corporate offices, each one armed with code that activated instantly. This tactic preys on instinct—our tendency to explore the unknown or ignore security warnings

Ransomware: digital hostage-taking
Hospitals, schools, city governments, even small businesses, have all been hit by ransomware. This type of malware encrypts systems and files, locking out users until a ransom is paid, often in cryptocurrency. Ransomware can spread through phishing emails, exploit known vulnerabilities, or arrive via compromised websites. Its impact is severe: halted operations, data loss, financial damage, and reputational fallout.

Today, ransomware-as-a-service platforms have made these attacks more accessible than ever. Criminals don't need advanced skills—just access to the right tools.

Man-in-the-middle (MITM): intercepting communication
A man-in-the-middle attack occurs when a third party secretly intercepts communication between two others, often without either side knowing.

This can happen on unsecured public Wi-Fi, through compromised routers, or malware-infected devices. For example, attackers on a coffee shop network could intercept your logins, messages, or banking details in real time.
More advanced MITM attacks may also alter content during transmission—changing data, redirecting users, or injecting malicious code. →

Cross-site scripting (XSS): exploiting web application flaws
Cross-site scripting is a web vulnerability that lets attackers inject malicious code into trusted websites. When a user visits the site, that code runs in their browser, often without them noticing. This can allow attackers to steal cookies, session tokens, or login credentials. In other cases, they might redirect users to fake pages or spread malware.

XSS typically results from poor input validation and weak output handling. Developers can prevent it by sanitizing user input and following secure coding practices.

Why understanding these attacks matters
Cyberattacks succeed when we underestimate how creative and varied they can be. By recognizing these five methods, organizations can better train staff, detect intrusions, and reduce risk.

Could your team spot a phishing attempt or think twice before plugging in a found USB? Awareness is the first step—then comes action. ■

ARTICLE

State-sponsored cyber operations in 2025

Cyberattacks today aren't just about stealing secrets—they're tools of statecraft. In early 2025, operations linked to Russia, China, and Iran exposed how digital tactics are now used to disrupt societies, send political signals, and prepare for conflict.

Over the first half of 2025, cyber operations attributed to Russia, China, and Iran have surged in sophistication and tempo. These are not isolated incidents, but part of coordinated geopolitical strategies—testing resilience, gathering intelligence, and establishing digital footholds. While some campaigns began earlier, they became strategically significant or publicly disclosed this year, reflecting evolving motives in global cyber conflict.

Russia has driven much of this shift. In June 2025, Germany's Federal Criminal Police Office (Bundeskriminalamt, BKA) reported that cybercrime caused a record €178.6 billion in economic damage during 2024—an increase of €30.4 billion from the year before. According to the BKA, nearly 950 public and federal institutions were affected, primarily by Russian-linked ransomware and distributed denial-of-service (DDoS) campaigns. Although these attacks occurred last year, the full extent and attribution only became clear in mid-2025, highlighting a strategic use of cyber tools to weaken institutions and extract value. →

In March 2025, the cybersecurity firm Cyble, which specializes in monitoring underground threat actors and global cyber activity, reported a 50% increase in attacks on industrial control systems (ICS) and operational technology (OT) environments. Many of these attacks were linked to Russian-aligned hacktivist groups such as NoName057(16) and Sandworm. These campaigns appeared designed to test critical infrastructure and gauge European defensive readiness, signaling a shift from opportunistic activity to strategic pressure.

In the United Kingdom, the National Cyber Security Centre (NCSC), part of the intelligence agency GCHQ, stated that the number of “nationally significant” cyber incidents had doubled since September 2024, with many linked to Russian-backed actors. This trend, publicly disclosed in spring 2025, reflects a persistent effort to intrude, disrupt, and erode trust in national systems.

> *“Amid recent U.S. and Israeli military escalations, many analysts warn Iran’s cyber retaliation may intensify in both scale and precision, raising concerns in Western defense circles”*

Meanwhile, on May 28, 2025, Czech authorities formally accused APT31 (also known as Judgment Panda), a group backed by China’s Ministry of State Security, of conducting sustained cyber espionage against the Czech Ministry of Foreign Affairs’ unclassified network. The intrusion reportedly began in 2022, but its strategic significance increased this year due to Prague’s diplomatic positions. The attack drew swift condemnation from both the European Union (EU) and NATO. The attack underlined the seriousness of the intrusion.

In parallel, U.S. intelligence briefings released in late spring indicated a 150% increase in China-linked operations targeting telecommunications, water utilities, and energy systems. Analysts believe groups like Volt Typhoon are “pre-positioning” within critical infrastructure, ensuring potential leverage in future conflict scenarios. →

Iran, though less prolific, has shown renewed intent. In June 2025, cybersecurity company ESET, known for its malware research and expertise in threat intelligence, reported new activity by BladedFeline, a subgroup within the Iran-aligned OilRig cluster. OilRig has been active since at least 2014, evolving its tools and targeting strategy consistently. The recent expansion and public attribution point to a wider strategic push by Tehran to assert digital influence in its neighboring region. The operations in June targeted Kurdish and Iraqi governmental networks and continue Iran's long-standing focus on regional espionage.

In light of recent military escalations involving the U.S. and Israel against Iran, many analysts warn that Iran's cyber retaliation may increase in both scale and precision—raising concerns across Western defense circles.

These trends show a shift: cyber operations are no longer just about data theft—they serve foreign policy goals. Russia disrupts to punish, China embeds for future gain, and Iran expands influence via targeted surveillance. Often publicized for political impact, these actions underline that in 2025, cyber warfare is integral to state strategies. With critical infrastructure and governments targeted, strong national cyber resilience is now crucial across democracies. ■

Key takeaways

1. The EU's new cybersecurity tools signal a shift toward digital sovereignty and shared European resilience.

2. Denmark's largest cities are replacing U.S. tech with European alternatives, reflecting growing concerns over geopolitical risks.

3. Amazon's new EU-based sovereign cloud enhances legal certainty and data control for organizations navigating NIS2 compliance.

4. Five common cyberattacks—from phishing to ransomware—exploit human behavior as much as technology.

5. Russia, China, and Iran increasingly use cyber operations as strategic tools in geopolitical competition.

www.communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden,
and operates through offices in Sweden, the Netherlands and Finland.

in
Linkedin

SECTRA