

Monthly Review

Cybersecurity news from around the world

INTRODUCTION.....	2
GENERAL CYBERSECURITY NEWS.....	3
ARTICLE	
Germany expands cyber intelligence powers	5
KEY TAKEAWAYS	7

ARTICLE

Germany expands cyber intelligence powers

[Read article →](#)



Newsletter introduction

Welcome back, and we hope you had a wonderful summer. As always, plenty happened across the cybersecurity landscape since our last newsletter, and this issue is an overview..

This month, we look at Germany's sweeping intelligence law reform, the growing abuse of trusted cloud services as attack infrastructure, the risks of unpatched consumer devices, and how the Coupang data breach turned into a trade policy dispute between allies.

Stay resilient. Stay secure.

General cybersecurity news

1 When “normal” traffic isn’t normal

Security researchers have tracked a growing pattern of attackers hijacking everyday cloud services to run their operations. In July, Zscaler linked an East Asian threat actor to malware named TELESIM, which used Telegram as its command channel against Middle Eastern government targets. China-linked APT41 has used Google Calendar entries the same way, until Google shut down the abused accounts. Russia’s APT29 did something similar back in 2022, using Dropbox and Google Drive to smuggle malware, and later Cobalt Strike, into diplomatic networks.

What ties these cases together isn’t the malware itself, but rather the logic behind it: why build risky infrastructure when you can borrow Google’s or Telegram’s instead? The traffic is encrypted, the domains are trusted, and most organizations wave it straight through the firewall. It’s the cloud-era sibling of living-off-the-land attacks, where intruders use a system’s own built-in tools to stay invisible, except that here, the “land” is the internet’s most popular platforms.

The uncomfortable conclusion for defenders is this: a known-good service is no longer a safe signal on its own. Spotting these attacks means watching how a connection behaves, meaning the timing, account and follow-up actions involved, rather than simply where it goes.

2 Unpatched consumer devices create cyber risks

Manufacturers don't always fix reported vulnerabilities. A flaw in a popular gaming speaker let anyone nearby hijack it as a keyboard over Bluetooth, without pairing or a password, yet the manufacturer dismissed it as a non-issue. More commonly, vendors invoke "end-of-life" status to dodge fixes, and a 2024 FTC study found 89% of smart device makers don't even disclose how long support will last.

New EU-driven rules aim to fix this by requiring manufacturers to guarantee updates for a device's expected lifespan and disclose support end-dates at purchase, but that won't help the millions of devices already sold without such guarantees. For those, owners should disconnect unsupported devices, disable risky features like Bluetooth, or replace them, since leaving them connected risks botnets, data theft, or giving attackers a way into the wider network.

3 When data breaches become trade policy

CA data breach is no longer just a technical matter, it can trigger trade policy consequences even between allies. Attacks can prompt sanctions, espionage fears can spark retaliatory tariffs, and cyber-enabled industrial espionage or perceived discriminatory regulation can escalate into full trade disputes. South Korean e-commerce giant Coupang illustrates this well. After a former employee exploited an unrevoked cryptographic key to access 33.7 million users' data undetected for months, regulators fined the company a record \$409 million. Because Coupang's parent is US-listed, American shareholders bore the cost. Investors pushed for a US Section 301 investigation, a US trade tool used to investigate and respond to foreign practices deemed unfair to American businesses, while Korean lawmakers accused Washington of political interference, turning a security failure into a dispute between allies.

The case shows how data breach response can no longer stop at technical recovery, it must also account for geopolitical risk.

ARTICLE

Germany expands cyber intelligence powers

A new German bill would give the country's intelligence services offensive cyber powers for the first time — a historic policy change that lines up with Germany's rising defense spending and a broader Western trend toward more proactive cyber capabilities.

Germany's cabinet approved legislation this week that would let its intelligence agencies hack foreign systems, sabotage supply chains, and feed false information to extremists at home. As reported by Recorded Future News, it is the biggest overhaul of the country's spy laws since the postwar era.

The Federal Government's own announcement of the cabinet decision frames the reform around a fast-changing threat picture: rising espionage, sabotage and hybrid attacks, alongside a string of drone incidents and terrorist threats in recent years.

Interior Minister Alexander Dobrindt, quoted by Recorded Future News, said the agencies were being granted "active, operational powers," framing the bill around acting against attackers rather than simply monitoring them. Chancellery chief Nina Warken, per the same report, said the new authority could include substituting faulty components into deliveries, sabotaging drone factories or chemical weapons labs, and disabling servers run by state-backed hackers. →

The foreign intelligence service (BND), according to the government's statement, would need to formally declare a named foreign power a persistent threat before conducting disruption operations, a declaration that expires after 12 months and must be reviewed every six. The domestic service (BfV) gains narrower but still unprecedented powers: blocking or rerouting data traffic, corrupting stored data tied to a plot, and disabling equipment before an attack occurs.

Oversight is being consolidated rather than left to individual agencies. A new Independent Oversight Council will take over the fragmented responsibilities of the former G10 Commission and must approve any particularly intrusive measure in advance, the government notes, giving the reform a single, court-like check across both services.



The bill also regulates AI use in analysis, permitting self-learning systems while requiring higher-risk outputs, such as movement profiles or behavioral assessments, to clear an additional threshold before an analyst can access them, Recorded Future News' review of the draft found.

The reform's timing tracks closely with Germany's sharp increase in defense spending following Russia's invasion of Ukraine. For organizations with infrastructure or supply-chain exposure in Germany, the practical implication is that the state is signaling a lower threshold for direct intervention against foreign threats, a posture other states, allied and adversarial alike, are likely to weigh in their own planning. ■

Key takeaways

1. A trusted service is no longer a safe signal on its own, defenders must watch how connections behave, not just where they go.
2. When manufacturers don't patch a vulnerability, the burden of security falls on the device owner.
3. A data breach's real cost may not be the attack itself, but the trade policy fallout from how it's regulated.
4. Offensive cyber powers are now spreading to core EU states, meaning direct state intervention in cyber incidents is becoming more likely, not just defensive support.

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