Monthly Review

Cybersecurity news from around the world

ARTICLE

CISA's challenges test global cyber coordination

Read article →

SECTRA

Newsletter introduction

As summer approaches, the threat landscape and cyber domain remain just as active. This month's developments all point in the same direction, Europe is accelerating efforts to strengthen its resilience.

The EU is simplifying defense investments, Sweden is reinforcing its digital defense through cryptography and secure cloud, cyberattacks are increasingly reaching operational technology, and changes within CISA highlight the importance of strengthening regional cyber capabilities. Before signing off for the holidays, we also share a practical checklist to help reduce cyber risk while you're away.

Stay resilient. Stay secure.

General cybersecurity news

1 EU clears pats for faster defense investment

The European Commission has unveiled the Defence Readiness Omnibus, a legislative package designed to remove obstacles that have slowed defense investment across Europe.

The proposal simplifies defense procurement rules, shortens permitting processes for defense-related projects, streamlines transfers of defense products between Member States, and introduces greater flexibility within the European Defence Fund (EDF). It also clarifies how existing EU legislation, including rules covering finance, competition and chemicals, applies to defense activities.

For governments, defense suppliers and technology providers, the changes could mean faster project approvals, more predictable procurement processes and shorter time from investment to delivery.

The initiative supports the EU's broader ambition to enable up to EUR 800 billion in defense investments over the coming years by reducing administrative delays and strengthening Europe's defense industrial base. As security challenges continue to evolve, the Commission aims to ensure that funding, industrial capacity and regulatory processes can move at the pace required to support European defense readiness.

2 Cryptography and secure cloude strengthen Sweden's digital defense

Sweden is strengthening its digital defense through a SEK 5 billion investment package that includes expanded cryptographic capabilities and a national cloud for sensitive defense information. The initiative also covers secure communications infrastructure and AI-enabled command systems designed to improve information sharing and operational decision-making across military units and NATO allies.

As defense organizations become increasingly data-driven, protecting sensitive information throughout its lifecycle is critical. Strong cryptography safeguards communications, identities and classified information, while isolated cloud environments help maintain national control over critical data. Together, these technologies provide a trusted foundation for secure collaboration, operational resilience and defense readiness in increasingly connected environments.

3 Cyberattacks are increasingly targeting OT systems

Cyberattacks targeting water and wastewater systems have increased significantly over the past year, highlighting growing risks to critical infrastructure. According to Cyberwatch Finland, geopolitical tensions, coordinated hacktivist activity and weaknesses in operational technology (OT) security continue to drive the trend.

Recent incidents demonstrate that attackers are no longer focusing solely on IT environments. In one case, in 2024, a Danish water utility experienced physical equipment damage after attackers manipulated pump pressure through industrial control systems.

For organizations operating critical infrastructure and industrial environments, these developments indicate that cyber threats increasingly have the potential to disrupt physical operations. Reducing external exposure, strengthening authentication and improving visibility across OT environments remain essential steps for lowering operational risk.

ARTICLE

CISA's challenges test global cyber coordination

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has long been a cornerstone of international cyber defense, coordinating threat intelligence and supporting critical infrastructure. Recent organizational challenges are prompting many organizations to consider how dependent they are on a single source of cyber coordination.

CISA continues to perform its core mission, including publishing threat advisories, coordinating responses and supporting critical infrastructure. However, according to Cyberwatch Finland, prolonged leadership instability, workforce reductions and budget pressure have affected several areas of the agency's operations, including intelligence sharing and coordination.

The agency is also prioritizing resources more narrowly toward the most critical systems. While this approach may strengthen protection where risks are highest, it could reduce visibility and support for lower-priority sectors.

The implications extend beyond the United States. For years, CISA has played an important role in sharing threat intelligence across governments, critical infrastructure operators and international partners. Any reduction in coordination capacity could affect how quickly cyber threat information reaches organizations during complex or large-scale incidents. →

These developments reinforce Europe's ongoing efforts to strengthen its own cybersecurity capabilities. Alongside NIS2, the European Commission and ENISA have introduced the European Vulnerability Database (EUVD), providing organizations with a European source of curated vulnerability intelligence to support risk assessment and vulnerability management.

For organizations operating within critical infrastructure, defense or international supply chains, the lesson is not to replace one intelligence source with another, but to diversify. Combining intelligence from international partners, European initiatives and internal analysis helps improve resilience if individual sources become less available during major cyber events. ■

CHECKLIST

Before you log off for the holidays

Cybercriminals don't take holidays, and neither do their phishing campaigns and efforts. Before heading off for a well-earned break, take a few minutes to make sure the basics are covered.

- ☐ Install any pending security updates on your devices.
- ☐ Make sure multi-factor authentication is enabled on both your work and private accounts.
- ☐ Be extra cautious of unexpected emails about deliveries, invoices or holiday offers.
- ☐ Store important files in approved company locations—not just on your laptop.
- ☐ Lock your computer and secure your workspace before you leave.
- ☐ Check that you know who to contact if you notice suspicious activity.
- ☐ Avoid using public Wi-Fi without your organization's approved security tools.
- ☐ If you're traveling, keep work devices with you and never leave them unattended.

A few simple precautions before you log off can make a meaningful difference in protecting both your organization and your own information while you're away.

Have a safe and relaxing summer, we'll be back in August.

Key takeaways

1. The EU aims to accelerate defense investments by simplifying procurement and reducing regulatory barriers.

2. Sweden is strengthening its digital defense through investments in cryptography and secure cloud infrastructure.

3. Cyberattacks are increasingly reaching operational technology, with incidents showing potential impact on physical processes.

4. Challenges within CISA raise concerns about future cyber coordination and the need to diversify threat intelligence sources.

5. Before the holidays, a few simple security checks can significantly reduce avoidable cyber risk.

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