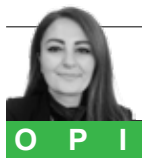
Europe faces faster cyberattacks than ever

Many of solutions long known



By Joyce Hakmeh
Senior expert in int'l cyber and tech policy

OPINION



A woman walks past empty fresh-food refrigerators at an Intermarché supermarket in Névez, western France, on October 12, 2026, a day after cyberattacks on the country's supermarket refrigerators.
FRED TANNEAU/AFP

In October, hackers caused tons of food to be thrown away after hacking into refrigerators in around 700 French supermarkets. Within weeks, similar incidents were reported in Belgium, Luxembourg, Sweden, Ireland and elsewhere. Nobody has claimed responsibility, but France has accused Iran of carrying out the 'unprecedented attack' against it.

The freezer attacks come after a spate of cyber incidents across Europe in the last few years that have repeatedly exposed familiar weaknesses. Russia's war against Ukraine has raised the stakes, putting Europe on the front line of hybrid attacks including through cyber operations.

Four problems stand out: old systems that are never fixed, new technology built without security in mind, increasingly capable attackers aided by AI, and states using cyberattacks as instruments of power, often through proxies.

Each requires its own response, and Europe is doing better on some fronts than on others. None is a European problem alone, and none will be solved by Europe alone.

Vulnerable legacy systems

The first problem lies in the weakness already built into the technology Europe runs on. Much of Europe still relies on legacy systems — technology that has reached the end of its life and no longer receives the security patches it needs. The result is a stock of known vulnerabilities that attackers can exploit.

The freezer attacks show what this looks like in practice. They were not technically complex: most of the hacked temperature controllers in France were reportedly legacy systems that no longer receive updates. Operational technology of this kind, which controls physical equipment, often stays in service for decades, long after anyone is updating it.

This is not just an issue for companies. The UK's National Audit Office found in 2025 that government departments used 'hundreds of ageing legacy IT systems.' Germany's federal audit office found in 2025 that parts of the federal government's networks are so outdated they no longer receive security updates.

Part of the problem is visibility: organizations and governments often lack a clear picture of the technology they own and operate. Even when organizations know where the problems lie, replacing old systems is expensive and disruptive. But leaving them in place is becoming increasingly risky.

Replacing these systems is primarily the responsibility of national governments and companies that operate them. But the EU is also pushing for it. In July, the European Central Bank told Europe's largest banks to replace or update legacy systems as part of planning for AI-enabled threats. The financial sector, however, is far ahead of most other sectors, and replacement will require money, expertise and political commitment.

In the meantime, basic measures, often referred to as 'cyber hygiene', can go a long way. According to ENISA, the EU's cybersecurity agency, two-thirds of the vulnerabilities attackers exploit already have a patch available. Where equipment no longer receives security updates, organizations need to restrict its exposure or replace it.

Europe does not lack information or rules: ENISA maintains a European Vulnerability Database, national agencies issue regular alerts, and the NIS2 Directive makes managing these risks a legal obligation. What is missing is implementation: turning warnings into action, particularly in smaller organizations, and enforcing rules that many member states have been slow to adopt.

Technology built without security

The second problem is that too much technology is still being built without security in mind. This is due to market incentives; manufacturers compete on price, features and speed to market, rather than prioritizing security. The costs of insecurity have mainly fallen on customers and society.

The EU has sought to change this. From December 2027, under the EU's Cyber Resilience Act (CRA), connected products that do not meet basic security requirements will no longer be allowed on the EU market. Manufacturers will be responsible for their security throughout their lifecycle.

However, the CRA has limits. Manufacturers are required to report actively exploited vulnerabilities, including those affecting products already on the market. But reporting a flaw does not fix it.

And for products that manufacturers no longer support, there may be no fix. Someone else then has to act: the shop, hospital or council operating the equipment must know it is affected and have the skills and resources to patch, isolate or replace it.

The underlying problem is poor-quality software. AI could help strengthen the security of software by identifying and fixing flaws faster than people can. But that depends on vendors using AI tools (with human oversight) before their products reach the market.

More attackers, moving faster

The use of AI by attackers is compounding these problems. AI is accelerating the process by which attackers are finding and exploiting vulnerabilities in insecure products and ageing systems. It is lowering the skills and resources needed to launch attacks and compressing the time defenders have to respond.

This year, frontier AI labs made a series of striking disclosures about their latest models' cyber capabilities. These capabilities are real, particularly when it comes to exploiting vulnerabilities including in legacy systems. The labs were right to disclose them. But the disclosures also showcased their products, and the hype and catastrophizing that followed have not always helped clarify where priorities should lie.

AI is not yet changing the nature of the game so much as its speed and scale. ENISA found that attackers in 2025 relied mainly on off-the-shelf AI tools to sharpen skills they already had. Similarly, the UK's National Cyber Security Centre found that among the incidents it handled, AI had not enabled 'a novel class of attack'.

Instead, the greater danger is that AI-assisted vulnerability discovery gives attackers more opportunities to strike before system owners can apply patches. In response, defenders must be able to act at the same speed.

Governments have not yet managed to achieve this. The EU, for example, created the European Cybersecurity Alert System to analyse threat and incident data across member states using AI. However, EU auditors recently found that the system had stalled and was not yet working as intended.

A separate challenge is dependence on external providers. Many of the most capable defensive AI tools are developed in the US. Access can be restricted or withdrawn, as US export controls showed in June 2026. Governments need to establish structured ways of working with these companies on early warning, model testing and making defensive tools available to operators of critical infrastructure.

> Part of the problem is visibility: organizations and governments often lack a clear picture of the technology they own and operate. Even when organizations know where the problems lie, replacing old systems is expensive and disruptive. But leaving them in place is becoming increasingly risky. Replacing these systems is primarily the responsibility of national governments and companies that operate them. But the EU is also pushing for it.



Frozen products are thrown away after freezers were emptied at ICA Kvantum in Sjobo, Sweden, on November 2, 2026, following a "sharp" overnight rise in freezer temperatures at several Swedish supermarkets.
JOHAN NILSSON/ Keystone-sda.ch

Cyber as a tool of state power

The fourth problem is that states are increasingly using cyber operations as a routine instrument of power, often through proxies. The war in Ukraine has exposed an entire ecosystem of proxies. The overlap between these actors blurs responsibility and complicates attribution.

Europe does not lack the tools to respond to state-backed cyber activity. It has mechanisms for public attribution, criminal investigations, sanctions and diplomatic pressure. But these measures have been slow and applied unevenly, which has reduced their collective impact.

The priority is therefore to use existing instruments more quickly and consistently. This requires coordinating responses across Europe and with international partners.

An EU-wide response is only as effective as the national systems underpinning it. Yet all but two member states missed the deadline to adopt the NIS2 Directive, which requires critical sectors to manage risks and report serious incidents. Member states need to improve information sharing, strengthen reporting and practise their responses to attacks.

Internationally, states have already agreed not to attack critical infrastructure or knowingly allow their territory to be used for malicious cyber activity. The