KPMG

Europe at a crossroads

Europe's coming of age

Bart Groothuis

February 2026

Europe's coming of age

When technology becomes the frontline of democracy

Bart Groothuis is a member of the European Parliament (VVD) and has been advocating for digital autonomy in Europe over the past five years. He urges business leaders to play a proactive role towards the cyber resilience goals of NIS2 because it matters for their business, not because of the need to comply. He also outlines how Europe should embrace a new geopolitical reality dominated by hard power rather than soft power and with digital technology in the heart of the matter.

"We're not a partner. We're a client."
Bart Groothuis, Member of the European Parliament

The longstanding love affair between Europe and the United States is under severe pressure and a recent series of decisions by President Donald Trump have made this utterly clear. However, a sharp-eyed analyst should have seen this coming much earlier. Groothuis points to a decision under the former Biden administration that showed the cracks in the relationship: new US export controls on advanced AI chips divided Europe into two trade zones, east and west, implying that part of Europe will find itself cutoff from the most advanced AI chips. At that moment, this decision didn't get much media coverage. Groothuis: "But in itself, it was a big decision. It was not just a trade restriction. It was a message: we want you to be dependent on us. If the US can unilaterally decide who in Europe gets access to key technology, then we're not a partner. We're a client."

This is just one of many examples of the new anatomy of geopolitics. Once upon a time, geopolitics was about geography: borders, pipelines and armies. Today, it is about chips, data and code. Countries can be colonised digitally. And once a country is colonised, it is no longer in charge of their own rules. Groothuis points to the 'CIA triad', a standard model in information security that stands for Confidentiality, Integrity and Availability. For many years, focus was on the C and the I. "A has now become top of mind in Europe. This runs like a current through many conversations in Brussels these days."

Buy European

The global power struggle is about who controls the technologies that shape our societies. The US dominate advanced AI chips through NVIDIA. The Chinese hold critical positions in solar panels and industrial components. But what about Europe? Part of the answer, according to Groothuis, lies in 'Buy European', not as a fancy slogan, but as a strategy. Europe needs to create demand for its own technology in order to be able to produce it. "Markets can be created through regulation. If you want chip factories in Europe, you first need a market that buys European chips for the European cloud, and governments should be the first customers of that cloud." That logic already drives parts of the EU's green and digital industrial policies. Just as the energy transition led to local requirements for wind turbines and batteries, digital sovereignty should demand similar measures for chips, AI, and cloud infrastructure.

Indispensability

But this discussion isn't about autarky. Sovereignty doesn't mean doing everything yourself. It also means making sure you can produce what others cannot. That's indispensability. If Europe can master a handful of critical technologies, e.g. lithography or industrial robotics, it will be relevant to others again.

The shift also carries an important message about cybersecurity: it is a key prerequisite for such digital autonomy. The new European NIS2 directive requires thousands of European companies to meet stricter security standards. It is clear that the 'A' of 'Availability' of the earlier mentioned CIA triad is a leading argument behind this set of rules which are vital to maintaining digital autonomy. For many CEOs, NIS2 feels like yet another compliance burden. But Groothuis insists it's something else entirely: a moment to regain control.

Companies should stop seeing cybersecurity as cost and start treating it as an opportunity to be as resilient as possible. "Cyber is not about being in control for 100%, as this is simply impossible. It's about reaching a state of always in beta, always eager to improve. And about being in control after an incident. A recent report of credit rating agency Moody's was very clear on this: the NIS2 is 'credit positive for doing business in Europe'. This underscores why NIS2 is not a compliance project and why it's vital to embrace it wholeheartedly. And as a CEO you don't need to wait for the final text of the law to do that: the rationale behind it is clear."

Ransomware as a service

Groothuis also points out how the nature of the cyber arena has evolved dramatically. "Most attacks today are industrialised. You're not hacked because someone hates you. You're hacked because you fit well in the business model of the hacker. They simply assess how much money you will be willing to pay. And with a few mouse clicks on the dark web, they order professional attacks. Ransomware as a service. No expertise needed."

We must fight these industrial-scale attacks with industrial-scale defence. If the private sector needs urgency, governments need discipline and proactive sharing of intelligence and monitoring information between private and public sector. That means central monitoring, public-private intelligence sharing, and clear accountability. "The Netherlands is a soup of small agencies," Groothuis says, "Every letter of the alphabet seems to have its own cybersecurity office. When these agencies have to decide something together, it simply takes too long. The less letters in the soup, the more effective a country is in cybersecurity"

Ukraine

Countries such as the UK, Canada, and Norway have more centralised structures. Some therefore suggest a stronger EU-level authority; a European Cyber Command for the civilian domain. Others also argue for national digital ministries. Groothuis advises against this and uses Ukraine as a good case: "Ukraine has a deputy minister for digital affairs in every department. Health, defence, education. Because everything is digital nowadays." In other words: it would be wrong to perceive digitalisation as a separate sector. It's the operating system of modern governance. Despite some frustration about the European speed on this topic, Groothuis spots progress. Export controls on high-end chipmaking equipment, once decided in The Hague under U.S. pressure, are now handled at EU level. "Brussels is slowly growing shoulders."

Hard power

Perhaps more importantly it's also about a moral shift. The old European self-image, of the merchant and the missionary, trading and preaching, no longer fits the reality of a world defined by hard power. "Soft power only works when it's backed by real power. A legalistic tone and slow bureaucracy won't impress a world of strongmen. Europe definitely has potential. We have scale with 450 million citizens with money, we have world-class researchers, and we have some of the most valuable industrial ecosystems on the planet. If it can act together, if it can find the will, it can compete. We're in the middle of Europe's coming-of-age moment. Every CEO can contribute to making the European agenda and should take ownership over it. It's in the interest of Europe, and in their own interest."

Viewpoint Ronald Heil

For management, it's all about intelligence-led decisions"

Although not every EU member state is ready, the transposition of the EU NIS2 directive in local laws is near, and it is safe to assume that the remainder of the countries will pass local laws this summer at the latest. NIS2 makes cybersecurity a board-level accountability, a business issue, not an IT/OT issue alone. The management body are personally responsible for ensuring risk-based, proportionate security measures are governed and implemented. Moreover, they may face fines on company group level, liability and potential 'career bans' for negligence.

Intelligence-led decisions are more than ever key. It is not about controls (only). It is (also) about prioritised threats on the operational resilience of the company. Focus should not be on paper-based compliance, rather on real adversaries, unlikely but plausible attack paths and operational business impact. Threat intelligence helps to make risk led decisions, with effective guidance on where to invest today (and what today tomorrow and later in the future). In effect such a threat intelligence approach helps organisations explain why and how they spend security money. Which is exactly what NIS2 asks from companies and their eco systems.

ESET threat intelligence

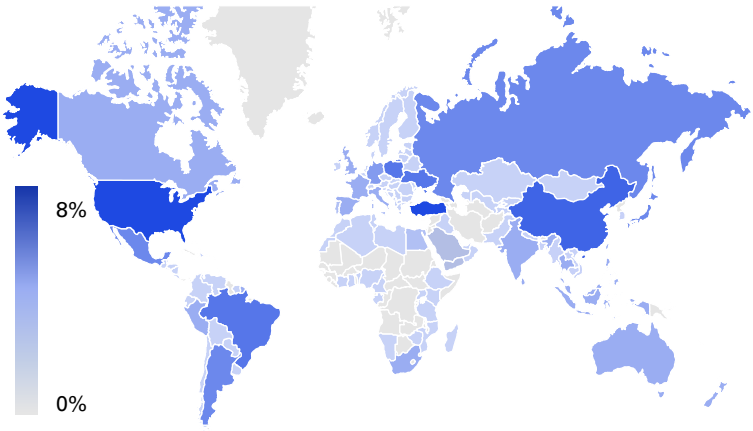
More than 90 percent of all digital systems used in the EU are made or developed abroad. This dependency is risky and calls for European alternatives for systems that are part of critical infrastructure that keep society up and running. In the meantime, criminal ransomware operations are increasingly aligned with or even directed by state actors. This alignment is deliberate, making it more difficult to attribute attacks between cybercrime and state sponsorship.

Stats

Ransomware deployment speed accelerated 48 percent (average 24-hour intrusion), driven by commoditisation of initial access and credential theft at scale.

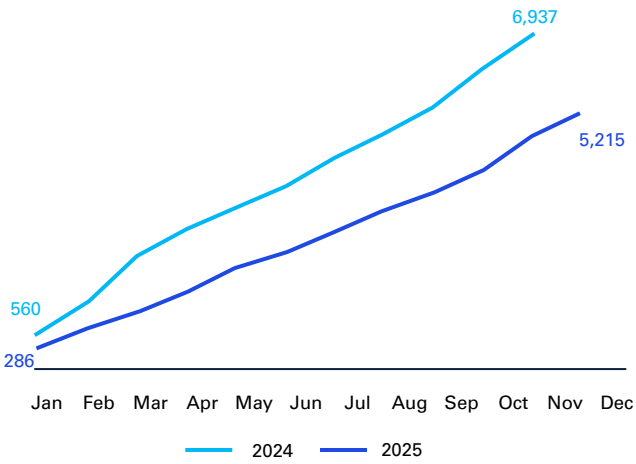
ESET Research projects a 40 percent year-on-year increase in the number of ransomware victims compared to the previous year.

Geographic distribution of ransomware detections in H2 2025



Source: ESET Threat Report H2 2025

Number of publicly reported victims of data leak sites of ransomware gangs



Source: Ecrime.ch

Recommendations

Immediate

Many attacks now escalate from initial access to full disruption within a day. This calls for developing and testing incident response plans tailored to 24-hour ransomware scenarios. Focused playbooks with clear escalation and decision paths help shorten detection and containment time.

Mid-term

Organisations must combine cyber threat intelligence with geopolitical analysis to provide early warning of strategic cyber risks and enable faster, better-informed executive decisions.

Long-term

Boards should reduce reliance on US Five Eyes intelligence by strengthening European cyber intelligence capabilities. This improves strategic autonomy, speeds up decision-making and ensures threat assessments align with European priorities and interests.