

Steven Maijor: Europe's digital autonomy - between fault lines and vault lines

Speech by Mr Steven Maijor, Executive Board Member and Chair of Supervision of De Nederlandsche Bank, at the 10th Annual FinTech and Regulation Conference, Brussels, 3 February 2026.

* * *

Good afternoon, everyone.

Before we dive into the issue of digital dependence in Europe, let me start with a confession: I spent part of last weekend practicing my English pronunciation: fault lines versus vault lines. The first one with an 'F', the second one with a 'V'.

Well-known examples of the first one are the San Andreas fault line in California, or the North Anatolian fault line in Turkey.

And the thing about these fault lines, these often-unseen cracks, is that we know they are there, we know they can shake foundations and shatter lives, but we don't know when these powerful forces will strike.

On the other hand, you have vault lines – with a V.

When I'm talking about vaults, today, I'm not talking about the place we keep our gold, but about vaults as in arches of resilience.

Whenever you visit the Notre Dame cathedral in Paris, or the chapel of King's College in Cambridge, or any great chapel or church in Europe, and look up to the ceiling, you'll probably see them: those stone arches that carry the weight and absorb the strain. Those visible lines of strength, deliberately built, stone on stone, to withstand pressure. Those are the vault lines I'm talking about. They keep things together – prevent the roof from falling on our heads. And provide shelter and safety.

Now, the reason I practiced these two words, similar in sound, but very different in meaning, is that the one – with an F – describes our current world, and the second – with a V – our future world, ideally, at least.

How so?

Well, let me start with our current world. Our financial system also has fault lines – cracks.

And those cracks have a capacity, similar to any tectonic fault line, to cause crises.

Today, I want to talk about one of those fault lines: Europe's digital dependence.

Together with the Dutch Authority for the Financial Markets – the AFM – we wrote a report on this topic. We did this because, currently, many European financial institutions are entrusting more and more of their IT stack to a limited number of IT service providers.

Cloud services are dominated by a few IT companies, the so-called hyperscalers. And, as you well know, many IT applications are built on these services. Often also for specialized services, for instance in cyber security, many financial institutions turn to a few smaller service providers.

For sure, relying on one IT provider for cloud services has efficiency benefits and gives access to innovative service, but it also makes institutions vulnerable. Because if that one hyperscaler were to fail - or become the victim of a cyber-attack - the effects would be immediate. And if it were ordered by its government to halt services for certain customers, stability could be severely jeopardised.

This concentration risk exposes a fault line in the financial sector. Because what seems stable today, might suddenly start to quiver and quake.

And it is not just about concentration risk. Because reliance on the same few large IT providers has also created systemic risks. Meaning that in a system as interconnected as our financial system, the lights going off at one hyperscaler, could very possibly affect the entire financial system.

It is undeniable that the fault lines under our European financial system have become far more prone to cracking in recent years. Right on Europe's borders, a ruthless aggressor is waging hybrid warfare. At the same time, some of our longstanding global relationships have soured. Values once thought common, like privacy and the rule of law, are no longer self-evident. And when once-partners diverge on fundamental values, fissures appear, following decades of trust. And this puts our financial system at risk.

Looking beyond these immediate threats, the DNB/AFM report sketches four directions that can shape Europe's digital footing:

One – in a world with increasing geopolitical pressures, and a digital stand-still in Europe, we become a digital colony dominated by external forces.

Two – in a world with increasing geopolitical pressures, but with a Europe that finds its own digital strength, we live in a fragmented world of separate technology spheres.

Three – in a world with DE-creasing geopolitical tensions, but still with a digital stand-still in Europa, we remain digitally dependent on non-European IT providers.

And four – in a world with DE-creasing geopolitical tensions AND with a Europe that finds its own digital strength, we succeed in creating a human-centred path of digitalisation, meaning that European IT capabilities grow, our digital dependence declines, and all of this happens in sync with European values such as privacy, and the rule of law.

Obviously, now that we are aware of the risks of the fault line that our digital dependence represents, the fourth scenario is the one to prefer. But since this is also the hardest one of the four to achieve, action is urgent.

So, where to start?

Indeed, as I said at the outset, looking ahead requires a shift in perspective. From what breaks to what endures. From what threatens to what protects. From the fault lines with an F to the vault lines with a V.

That is what we need in our financial system: strong structures and stable partnerships, built on shared values, to protect our system from shocks caused by the cracks beneath the surface.

In the near term, these vault lines – with a V – will consist of preparing ourselves the best we can – given our state of dependence. Today, independence is not on the table, because it is simply not available. It is not yet attainable. No European alternative is adequate to take the place of one of the big non-European IT providers.

And so, preparation is key – for instance by developing and rehearsing actual threat scenarios. In doing so, two fast-moving situations should receive special emphasis:

- hybrid attacks – meaning a combination of physical and digital attacks – that disrupt shared infrastructure, and
- sanctions that force key third-party suppliers to suspend services.

Financial institutions are already working together closely on this by sharing vital information. In our report, we urge them to also test whole chains of systems with their main suppliers, and as such learn how disruptions might spread. This helps to spot weak points early and to contain problems before they can shake the entire system. The AFM and DNB stand ready to facilitate this work wherever we can be of assistance.

A good practice we found at a few financial institutions, is investing in more flexibility – wherever possible. As such, they redesign applications to improve portability, adopt open standards and use container technologies to reduce dependency.

Procurement practices are also shifting in this direction. We see that financial institutions are broadening their vendor base and exploring multi-vendor strategies. These steps do not eliminate dependency risks, but they do provide institutions with more options when conditions change.

One essential vault line – with a V – which the European financial sector needs to construct or strengthen, is control over its data.

In this regard, it is promising that financial institutions are looking more and more often at European IT providers. They are also reassessing the European variants offered by global hyperscalers – the so-called EU sovereign cloud offerings. In that last scenario, the central question remains, of course, whether any of these arrangements truly strengthens control and resilience when circumstances become difficult, and a foreign government starts threatening.

In our report, we suggest that financial institutions increasingly retain their own encryption keys. This would ensure, in the near term, that the protection of critical information remains firmly under their stewardship.

All in all, financial institutions must assess all available options carefully and plan for continuity. Of course, switching providers is never simple – it is costly and time-consuming, even if we expect or eventually even compel providers to facilitate this when asked to. But preparation matters. It shows institutions what can realistically be done when disruption strikes and where additional work is still needed.

In this way, they strengthen the vault lines that help the system hold firm when the ground begins to shake.

Now, turning to the longer term, the goal is pretty straightforward: we need to reduce our reliance on non-European providers. And we need to do this by reinforcing Europe's digital capabilities and addressing the causes of our current dependency.

This long-term goal is a joint project of the European tech industry, the financial sector and public authorities.

And yes, policy is already moving in the right direction.

We already see protective vault lines emerging in legislation like DORA – the European Digital Operational Resilience Act, which entered into force in January 2025.

But truth be told, even with DORA in place, vulnerabilities persist – especially those that are linked to geopolitical developments and to the location of critical data. DORA provides a good start, but we must continue to focus on key vulnerabilities, like

- concentration risks,
- who has jurisdiction over critical data and applications, and
- how far supervisory powers extend.

In order to develop European IT capabilities, we must get to work.

Earlier, I described four possible scenarios for our digital future. To realise the preferred fourth scenario, the one in which Europe leads the way in promoting human-centred digitalisation, will demand time, determination and sustained investment in European IT.

As such, where possible, financial institutions should work more closely with European IT providers for critical services. By aligning specifications, running coordinated tests, and offering purchase guarantees, they can help create the scale needed for viable and competitive European cloud providers to emerge.

But scale alone is not enough. To truly strengthen Europe's digital footing, we also need joined testing. For instance, when it comes to the security of the entire chain of operations, from primary IT providers to every subcontractor involved. Joint testing helps us spot vulnerabilities early, before they can spread through the system.

And even that is only part of the answer. To genuinely build Europe's digital strength, we must also invest in the companies capable of delivering it. That means strengthening the savings and investment union, so that more European capital flows to innovative European firms - the firms that can build the digital services we will rely on tomorrow.

And yes, where necessary we must also improve regulation - making oversight more enforceable, clarifying expectations on geopolitical risk and data location, and, in due course, considering a cross-sector European cloud supervisor.

By continuing to work together – financial institutions, policy makers, and the European tech industry – we can gradually reduce our digital dependencies and strengthen the resilience of our financial sector. Step by step, we can shift from merely spotting the fault lines that may fracture beneath us to actively reinforcing the vault lines that keep Europe's financial system safe and secure.

And if you still can't hear the difference between fault with and F and vault with a V, don't worry. Just remember: the first one cracks, the second one endures.

Thank you.