Association des avocats en droit boursier

Paris, 9 September 2026

–

Speech by Denis Beau

First Deputy Governor of the Banque de France

and Delegated Chairman of the ACPR

For several years now, the financial sector has been pushing ahead with a profound digital transformation to maintain and enhance its competitiveness. This can be seen in the amounts allocated to IT budgets, for example: an ECB study estimated the allocation for European banks at nearly 3% of net banking income in 2024[i].

And new digital tools do indeed help institutions to attract new customers by offering them new or improved services, while also enabling them to rationalise costs. However, digital transformation has a downside: **it increases the attack surface for malicious actors**. A successful attack can result in significant costs, both direct and indirect due to reputational effects. Institutions – while continuing to innovate – must therefore ensure they maintain a high level of cybersecurity.

To meet both these objectives simultaneously and "stay in the race" for innovation, **the most obvious solution is often to turn to hyperscalers**, which offer high-performance infrastructure and services – particularly in the areas of cloud computing and AI – while providing state-of-the-art security guarantees. However, this choice leaves users **exposed to a new risk: technological dependence**. This can be potentially costly in the long term: a study commissioned by CIGREF (the association of major French companies focused on information systems) estimates that Europeans spend EUR 264 billion each year on US software and cloud services[ii]. It is also operationally dangerous, and it is telling that the scenario of a **"kill switch"** on US digital services, which for so long was unthinkable, is now contemplated by the French government[iii]. **So, the question is whether the European financial sector can allow itself to be locked into new dependencies in order to realise its innovation and security objectives more quickly.** Clearly, the situation is not straightforward and institutions must navigate an array of complex technological and operational trade-offs. I would like to take this opportunity to consider the main ones (I) before discussing the solutions available to both institutions and public authorities (II).

*

I/ **Cyber risks and sovereignty risks are two sides of the same problem: maintaining control over critical digital infrastructure**. By "handing over the keys" to a few indispensable service providers over which they have little leverage, financial organisations are putting themselves in a vulnerable position, for at least three reasons.

The concentration of providers is in itself a new operational risk: last year, a 14-hour outage at AWS was enough to bring a large part of the online economy to a standstill. These concentration risks can also be directly linked to the use of the same cybersecurity solutions: for instance, the CrowdStrike incident in July 2024 led to 8.5 million systems crashing worldwide due to a faulty security software update.

Next, dependence reduces institutions' capacity to manage operational – and therefore cyber – risk. By entrusting certain activities to third parties, **institutions can lose the ability to carry them out themselves and, above all, to make a proper assessment of the quality of the service provided**. The loss of expertise also makes exercising effective control over IT service providers more difficult. During his hearing before the French parliamentary commission of inquiry into digital dependencies, Henri Verdier, the former Interministerial Digital Director, spoke of the "culture, very widespread in information system departments in both the private and public sectors, which essentially consists of buying solutions rather than knowing how to code yourself"; and, he added, "when an organisation no longer knows how to produce, it no longer knows how to buy".

Lastly, by outsourcing certain critical services, institutions are exposing themselves to a phenomenon of **"vendor lock-in"**, which can manifest itself in very concrete ways through substantial cost increases once a dependency has been created, or the obligation to pay for unwanted functionalities (a practice known as **"bundling"**).

Nonetheless, despite these risks, avoiding dependencies is not easy, particularly as they are often already well entrenched – we can think of the Microsoft software used on work computers, for example – in a context of heightened cyber threats, amid geopolitical tensions. In France, however, the financial sector has perhaps been more cautious than elsewhere, and has generally retained control over its most critical systems.

The case of **frontier AI models**, such as Claude Mythos, provides a particularly revealing example of the difficulties involved in striking a balance between the different solutions. On the one hand, it is increasingly clear that these models will become an indispensable tool for cybersecurity: alongside the offensive capabilities that they unfortunately offer to attackers, they provide security teams with new possibilities both in terms of the identification of vulnerabilities and for the automated generation of corrective measures. It would therefore seem common sense to use these models to "up our game" in terms of cybersecurity. **But leveraging these solutions to their fullest often means granting them very extensive access to the institution's information system, which in turn creates new risks**: the risk of compromise, but also the risk that information capital could be transferred from the financial sector to a few major non-European technology providers.

II/ So, what to do? And how to guard against these risks of dependence? Without claiming to address the subject in full, I would like to mention certain measures that can be implemented by financial organisations, and others that are within the reach of public authorities.

Organisations can – and must – first implement "basic" cyber hygiene measures: reducing attack surfaces, securing access, strengthening detection capabilities and establishing minimum incident response capabilities. They must also adapt to the accelerating pace at which vulnerabilities are exploited, which means regularly upgrading procedures, resources and tools in order to **roll out necessary corrective measures more quickly** than is currently the case. These initial recommendations form the core of an **ACPR official letter sent to industry associations in June of this year**.

Organisations can also improve how dependence is taken into account in their operational risk analysis by carrying out a **systematic inventory of critical dependencies** that covers all their IT assets – workstations, networks, hardware, software, cloud services, security equipment, and so on. The exercise may be complex, but it is vital to gaining a comprehensive picture of risk exposure. Benchmark indicators, such as the Digital Resilience Index developed in France by a group of public sector players, businesses and digital experts, can help with the assessment[iv].

The identification of dependencies must then be used by organisations to develop operational resilience strategies. Taking the cloud as an example, this can involve applying a "multi-cloud" strategy by using multiple providers, employing a "hybrid-cloud" strategy by storing critical data and applications on proprietary servers or on a private cloud, or even preparing for a potential exit by ensuring data and application portability. **Lastly, using open-source technologies is also a promising solution for reducing dependencies.**

And of course, public authorities also have their part to play. In terms of regulation, sovereignty issues have already been clearly identified at the European level: the European Commission recently proposed a **"tech sovereignty package"** [v] which notably features the Cloud and AI Development Act (CADA). The CADA aims to facilitate the deployment of the EU's cloud and AI capabilities. It notably proposes a single assessment framework for grading cloud sovereignty[vi]. The package also includes an Open Source Strategy aimed at **ensuring continued access to the most critical software components**.

As for the supervisory authorities, they can play at least two complementary roles. First, they can act as **watchdogs** through their supervisory mandate. By bringing critical third-party providers (CTPPs) under a common oversight framework, DORA helps financial supervisors better assess the risks of concentration, dependency and technological lock-in, and thus better align operational security and digital sovereignty objectives. Second, supervisors can play the role of **catalysts** by shaping practices in the financial sector. Supervisors can perform this role by highlighting emerging risks, as the Single Supervisory Mechanism (SSM) recently did by alerting major European banks to the risks associated with frontier AI. They can also perform the role by being **exemplary in their choices of technology** for their own needs, as their choices are likely

to influence the decisions of financial institutions. Finally, supervisors can **support a framework that is conducive to industry-wide initiatives that enable financial institutions to strengthen their bargaining position vis-à-vis** major technology providers. One such example is the Collaborative Cloud Audit Group (CCAG), which was set up by several major German financial institutions to conduct pooled audits of the main cloud service providers.

*

Therefore, a balance – albeit a delicate one– can be struck between innovation, cybersecurity and sovereignty. Let us bear in mind that, despite the undeniable pace of technological change at work, **our collective resilience will depend on our ability to retain control over our infrastructures and our operational risks**. Therefore, integrating these issues into our strategies today is essential if we are to limit dependencies before they take lasting hold. Thank you for your attention.

[i] ECB, Digitalisation: Key Assessment Criteria and Collection of Sound Practices

[ii] CIGREF, 2025. Figures extrapolated from the expenditure data of six large "benchmark" companies.

[iii] Report of the French Parliamentary Commission of Inquiry on Structural Dependencies and Systemic Vulnerabilities in the Digital Sector and the Risks to France's Independence; see in particular Chapter 5(B)(2)(a).

[iv] aDRI - Digital Resilience Inititative

[v] Communication on European Technological Sovereignty, accompanied by an EU Open Source Strategy

[vi] Cloud and AI Development Act | Shaping Europe's digital future