TECHNOLOGICAL SOVEREIGNTY AND CYBER

September 2026

How can we move beyond generic rhetoric and implement concrete solutions?

Jean LANGLOIS-BERTHELOT & Christophe GAIE

Technological sovereignty has established itself as a key focus of the European strategic debate. It underpins industrial policies, shapes public discourse and permeates innovation ecosystems. Yet, behind this ubiquity, ambiguity persists. Technological sovereignty is often invoked as a general framework, sometimes as a rallying cry, but rarely as the subject of rigorous analysis. Yet reality is less conceptual than material. It is reflected in market shares, technological dependencies, digital architectures and substitution capabilities. The shift currently underway is clear. As highlighted in the SKEMA Publika *policy paper*, *Artificial Intelligence and European Sovereignty'*[1] *,* sovereignty is no longer determined solely by the ability to produce, but by the ability to control complex systems whose building blocks are distributed, interlinked and, to a large extent, beyond European control. This shift is also evident in the cyber domain, which today constitutes the focal point of technological dependencies.

A. CYBERSPACE: THE INVISIBLE HEART OF DEPENDENCY

Today, the European economy relies mostly on a digital infrastructure over which it has only partial control of the underlying technology. Indeed, two-thirds of the European cloud market is held by the three major US players: Amazon (with AWS), Microsoft (with Azure) and Google (with GCP)[2] . A

[1] Dibiaggio, L., Nesta, L., Vannuccini, S., Vidal, F., & Scull, S. (2025). Artificial Intelligence and European Sovereignty. SKEMA Publika. https://publika.skema.edu/fr/intelligence-artificielle-et-souverainete-europeenne/

[2] Synergy Research Group. Q1 Cloud Spending Grows by Over $10 Billion from 2022; the Big Three Account for 65% of the Total | Synergy Research Group. https://www.srgresearch.com/articles/q1-cloud-spending-grows-by-over-10-billion-from-2022-the-big-three-account-for-65-of-the-total

substantial proportion of the cybersecurity tools deployed within large organisations also come from non-European vendors such as Palo Alto Networks and CrowdStrike. Furthermore, operating systems, virtualisation environments, monitoring tools and digital identity components are frequently implemented by non-EU players. Examples include the digital giants Microsoft and Google.

This situation has a specific consequence: dependency is not always apparent. In other words, it is insidious in that it does not necessarily lie within the end application, but in the intermediate layers – those that orchestrate, administer and secure the systems[3] . An organisation may host its data within the European Union whilst remaining dependent on architecture over which it has no control. In practical terms, an organisation may secure access whilst remaining dependent on tools over which it has no control, neither in terms of updates nor internal mechanisms. In the military sphere, the example of dependence on the United States regarding the F-35 is a typical case. A country may physically possess a fighter jet without being able to access the content or modify the software essential to its operation. Unless otherwise specified in a contract, this software remains exclusively owned and maintained by the supplier[4]. In such cases, sovereignty is not fully guaranteed.

However, it is often during a crisis that the consequences of a lack of technological sovereignty become clearly apparent. Indeed, the ransomware attacks that have affected local authorities, hospitals and public service providers in recent years have highlighted this technological dependence. Beyond the vulnerability to intrusion, organisations have faced major difficulties in regaining control of their information systems. Due to the lack of alternative solutions for migrating their applications and data, certain digital services had to be shut down and remain unavailable for an extended period. This painful but necessary decision led to significant operational difficulties, which may have required a return to paper-based forms[5] ...

Furthermore, the vulnerability associated with this latent dependency became spectacularly apparent in 2024 during the global outage caused by

[3] Bannerman, S. (2022). Platform imperialism, communications law and relational sovereignty. New Media & Society, 26(4), 1816–1833. https://doi.org/10.1177/14614448221077284

[4] Daniez, C. (2026). 'The US can stifle its allies' use of the F-35 in several ways' – L'Opinion. *L'Opinion*. https://www.lopinion.fr/international/les-etats-unis-peuvent-etouffer-lusage-des-f-35-de-leurs-allies-de-plusieurs-manieres

[5] Richy, W. (25 February 2025). Cyberattack on Versailles Hospital: more than two years on, legislation in the pipeline. Tv78. https://tv78.com/cyberattaque-hopital-versailles-loi-cybersecurite/

a faulty update from the US cybersecurity firm CrowdStrike[6] . This instantly paralysed millions of Windows systems worldwide, bringing airports, hospitals and critical European infrastructure to a standstill. This incident demonstrated that dependence lies not only in accessing and managing data, but also in controlling the update flows of security solutions installed at the heart of IT systems.

In a context of technological dependence, cybersecurity ceases to be merely a protective function and becomes a prerequisite for business continuity. Consequently, technological sovereignty can no longer be conceived without incorporating this dimension: who controls access, who administers the systems, who deploys updates, and who can, as a last resort, interrupt or alter a service. This intangible dimension of sovereignty must, moreover, be considered from the very moment new digital solutions are integrated (such as artificial intelligence, particularly with the emergence of agent-based solutions). Indeed, if an organisation relies on non-sovereign AI to sort its data or optimise its production lines, its operational continuity is at the mercy of the model's publisher[7]. This is why the deployment of solutions based on open or local models, such as those from the European firm Mistral AI, integrated within secure infrastructures, represents a promising avenue for reducing dependence and enhancing technological sovereignty.

B. INNOVATION AND REGIONS: A FRAGMENTED LANDSCAPE

Faced with this dependence, Europe is not starting from scratch. It has a solid scientific foundation, accounting for around one-fifth of global output. It is home to high-performing technology clusters and dynamic regional ecosystems. In France, hubs (French Tech Capitales) such as Rennes in the fields of cyber security, e-health and deep tech[8], Grenoble for semiconductors (with STMicroelectronics and CEA LETI)[9], and Toulouse for aeronautical and embedded systems (notably with Airbus and Thales Alenia

[6] CrowdStrike / European Union Agency for Cybersecurity (ENISA) incident report, 'Falcon Sensor Content Update Incident and its implications for European critical infrastructures', 2024.

[7] European Commission, 'European AI Strategy and the role of open-source foundational models in industrial autonomy', Policy Report, 2025.

[8] Le Poool. (2026). FrenchTech Rennes St Malo Annual Report 2025. https://www.lepoool.fr/LePoool_RA2025_WEB.pdf

[9] Court of Auditors. (April 2026). Public support for the semiconductor sector: Summary of the thematic public report. https://www.ccomptes.fr/sites/default/files/2026-04/20260421-synthese-Soutien-filiere-des-semi-conducteurs.pdf

Space)[10] bring together high-level expertise, combining research, industry and public sector players. At European level, we can cite the example of 'Silicon Valhalla', referring to the extremely dynamic start-up ecosystem (Sana AI, Lovable, etc.) in Northern Europe[11] .

However, this capacity for innovation faces a structural constraint: the difficulty in scaling up. The number of European cybersecurity start-ups is significant, but very few reach a critical mass comparable to that of their American counterparts. Funding for *deep tech* remains low, and industrial trajectories are often cut short by takeovers or difficulties with industrialisation[12] . In France, the Brittany region has established the 'Cyber Pôle Bretagne' (bringing together academic stakeholders, the DGA and industry players in Rennes) to create a unique innovation ecosystem. However, the findings of the Court of Auditors highlight the chronic difficulties faced by these regional initiatives in transforming their local gems into industrial champions of European stature, due to a lack of unified public procurement contracts and substantial funding during the post-seed phase[13] . Start-ups there remain highly vulnerable to takeovers by foreign capital.

This situation creates a genuine paradox. Innovation exists, but it does not systematically translate into national capacity. Regions produce relevant solutions, test applications and experiment with technological. Yet these innovations often remain confined to local areas or pilot phases. Their scaling up to large-scale deployments remains limited. The regionalisation of innovation is both a strength and a weakness. It enables proximity to needs, the capacity for rapid experimentation and sector-specific specialisation. But it also leads to fragmentation. Without integration mechanisms, initiatives coexist side by side without producing a mass effect. This observation is also made in the SKEMA Publika *policy paper 'Artificial Intelligence and European Sovereignty*': at European level, in the field of AI, a logic of intra-European competition between actors predominates, rather than an ability to mobilise complementary resources and generate opportunities for innovation

[10] Toulouse Haute-Garonne Chamber of Commerce and Industry. (February 2023). Toulouse Aerospace. https://www.toulouse.cci.fr/sites/g/files/mwbcuj1576/files/2023-03/210x297-3v-TOULOUSE-AEROSPACE_fe%CC%81v2023_BD.pdf

Ministry of the Economy and Finance, European Institute of Business Administration, & World Intellectual Property Organisation. (2016). RE-INDUSTRIALISATION THROUGH INNOVATION. https://www.vie-publique.fr/files/rapport/pdf/174000256.pdf

[11] SiliconValhalla. (2026). https://www.siliconvalhalla.no/about

[12] See the SKEMA Publika policy paper: Growth of start-ups and SMEs – Why are current models reaching their limits? https://publika.skema.edu/fr/croissance-des-start-ups-et-pme/

[13] Court of Auditors, Thematic Report: 'Public support for the cybersecurity sector and the development of regional ecosystems', Documentation française, 2025. https://www.ccomptes.fr/sites/default/files/2025-06/20250616-S2025-0602-Reponse-de-l-Etat-aux-cybermenaces-sur-systemes-d%27information-civils.pdf

throughout the value chain[14] . Technological sovereignty therefore requires a shift in approach. It is no longer simply a matter of supporting innovation, but of organising its transformation into industrial and operational capacity. This involves connecting regions with one another, aligning public and private needs, and structuring sectors capable of moving beyond the experimental stage.

This requirement for sovereignty is, moreover, shaped by the physical reality of the digital world. Over 95 per cent of global internet traffic passes through undersea cables[15] . Yet the ability to ensure the security of one's critical infrastructure is the true measure of a territory's sovereignty. The example of Marseille is emblematic, as the city now ranks among the world's top ten connectivity hubs, situated at the junctions where Europe's networks converge with those of Africa, the Middle East and Asia. By integrating these networks into highly secure local data centres, the region is transforming a geographical advantage into an industrial lever and a source of national resilience[16] .

C. SELECTIVE DEPENDENCIES, MEASURED SOVEREIGNTY

The debate on technological sovereignty often comes up against a simplistic dichotomy: dependence or autonomy. This opposition is misleading because, in a globalised technological system, no economy can claim complete autonomy. The real issue is that of chosen dependence.

Some dependencies are acceptable because they are managed, diversified or easily substitutable. Others are critical because they concentrate on essential functions for which there are no credible alternatives. The distinction between these two categories must become explicit and operational.

The case of telecoms infrastructure illustrates this logic. Players such as Huawei have offered high-performing and competitive solutions,

[14] Dibiaggio, L., Nesta, L., Vannuccini, S., Vidal, F., & Scull, S. (2025). Artificial Intelligence and European Sovereignty. SKEMA Publika. https://publika.skema.edu/fr/intelligence-artificielle-et-souverainete-europeenne/

[15] General Secretariat for Maritime Affairs. (2022). Submarine Communication Cables. In The Blue Economy in France – 2022 Edition (pp. 397–412). French Government. https://www.info.gouv.fr/upload/media/content/0001/10/ca2753fbe56d94423b50ccf54efb30d5f4e75672.pdf

[16] Morel, C. (2020). The State and the Global Network of Submarine Communications Cables (PhD thesis in public law). Jean-Moulin Lyon 3 University. https://doi.org/10.70675/4c76d5acz07e0z4242z8830zecd385cc73ea

accompanied by local investment and job creation. Yet several European states have restricted their access to critical 5G networks. This decision is not driven by economic considerations, but by an assessment of control. In a network infrastructure, the supplier retains influence over updates, architecture and certain technical parameters. This position confers on structural power that goes beyond a mere commercial relationship.

This case highlights a key point: territorial or fiscal ties are not sufficient to guarantee sovereignty. Sovereignty depends on the ability to control, audit, replace and maintain a system in operational condition. This requirement for control lies at the heart of intangible infrastructure. The implementation of the French government's 'Cloud at the Centre' doctrine perfectly illustrates the complexity of this chosen dependency. This is the aim of the S3NS consortium, an alliance between Thales and Google Cloud, designed to meet the sovereignty requirements of ANSSI's SecNumCloud label. The operational challenge here is not technological self-sufficiency but rather ensuring technical reversibility and immunity from extraterritorial regulations such as the US *FISA* or *Cloud Act*. This enables institutions to retain the encryption keys and exclusive operational control over their data[17] .

This reasoning also applies to all digital technologies. The cloud, identity systems, critical software and data chains must be assessed not only in terms of performance but also in terms of control and reversibility. The apparent cost of a solution does not reflect its strategic cost. Low-cost technology may create long-term dependency. More demanding technology may offer decision-making capacity and continuity. In this context, technological sovereignty becomes measurable. It is reflected in the ability to identify critical points, organise alternatives and maintain continuity of action in degraded situations. Cybersecurity serves as a barometer of this, as it concentrates invisible dependencies and control capabilities. It requires reliance on well-calibrated and enforceable legislation that fulfils its protective role without hindering innovation.

Technological sovereignty is therefore neither a slogan nor a category of actors. It represents a more profound transformation in the way states and economies approach technology. The available data reveal significant dependence on critical digital infrastructure, a genuine capacity for innovation that is, however, insufficiently industrialised, and territorial fragmentation that limits economies of scale.

[17] National Agency for the Security of Information Systems (ANSSI). (2022). Security requirements framework for trusted cloud service providers (SecNumCloud) (Version 3.2). General Secretariat for Defence and National Security. https://cyber.gouv.fr/documents/388/secnumcloud-referentiel-exigences-v3.2.pdf

The challenge is not to reduce these observations to an ideological dichotomy. It is to treat them as operational variables. Technological sovereignty cannot be decreed. It is built through the interplay between cyber security, regulation, innovation and territories, and is demonstrated by the ability to continue functioning when conditions become unfavourable.

It is precisely at this point that technological sovereignty ceases to be a generic term and becomes an analytical tool that seeks solutions to protect citizens.