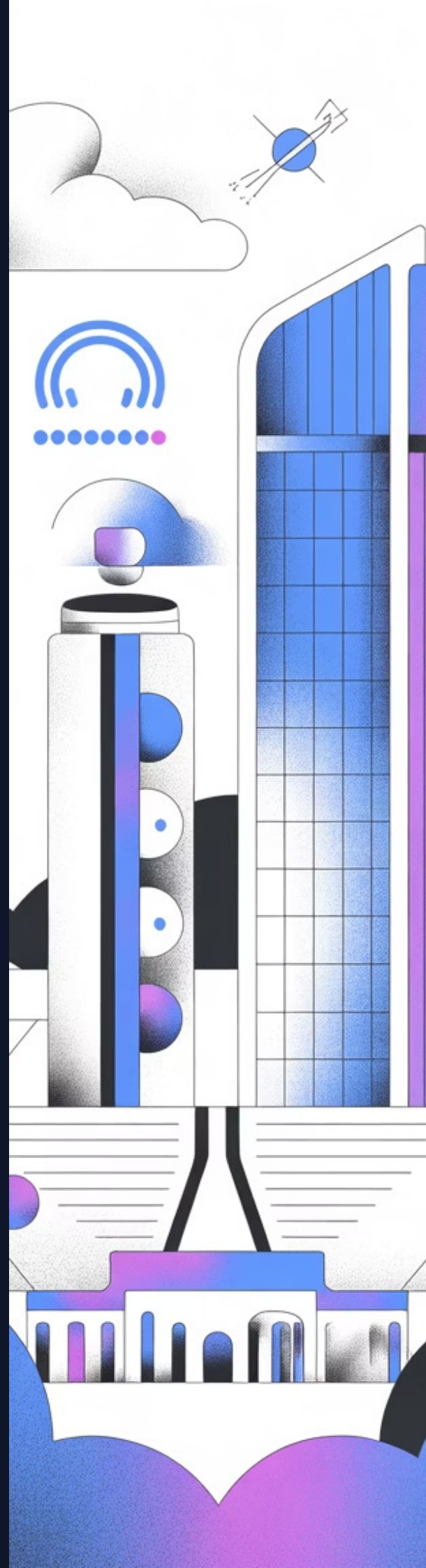


Unlocking Europe's Digital Future: Sovereignty, Geopolitics, and Economic Power

Discover how a resilient, independent European cloud infrastructure is not just a technological ambition, but a strategic necessity, profoundly impacting geopolitical influence, economic competitiveness, and the cultivation of crucial talent across the EU. In an increasingly data-driven world, the control and security of digital infrastructure are paramount to national and regional autonomy.

Europe currently faces significant challenges due to its reliance on non-EU cloud providers, which can expose critical data to foreign jurisdictions and regulatory frameworks, raising concerns about data privacy, security, and digital resilience. This dependence carries substantial geopolitical risks, potentially limiting Europe's capacity to act independently on the global stage, and creating vulnerabilities to cyber threats and economic espionage. The stakes are high: without digital sovereignty, Europe risks ceding control over its industrial data, hindering innovation, and undermining its long-term economic competitiveness.

Achieving digital sovereignty means fostering a robust ecosystem of European cloud solutions that adhere to the highest standards of data protection and cybersecurity. This quest will not only safeguard sensitive information and critical infrastructure but also drive the development of cutting-edge technologies, create high-skilled jobs, and attract investment across the Union. Ultimately, success in this endeavor will empower Europe to shape its own digital destiny, enhance its global leadership in technology and innovation, and ensure a secure and prosperous future for its citizens.





Introduction: The Case for a Sovereign Digital Infrastructure

In a 2021 joint letter to the European Commission, four national leaders — Germany's Angela Merkel, Denmark's Mette Frederiksen, Finland's Sanna Marin, and Estonia's Kaja Kallas — declared, **"Now is the time for Europe to be digitally sovereign."**

Achieving digital sovereignty is not about isolation or autarky; it's about rebalancing control. As the World Economic Forum noted, countries around the world – from the US to China to India – are adopting different approaches to secure their digital futures^[1]. The EU's approach emphasizes rules (like GDPR and the Digital Markets Act) and collaborative initiatives to foster homegrown innovation, whereas the US traditionally relied on market forces and China pursues a state-driven model^[4]. These divergent paths have already heightened geopolitical competition and risk fragmenting global tech ecosystems^[5], but European leaders argue that ensuring sovereignty over critical digital infrastructure is a strategic imperative for the bloc. Below, we explore the key drivers behind Europe's push – from geopolitics and security, to economic growth, to talent retention – and how various European initiatives aim to address them.



Geopolitical and Security Drivers

Strategic autonomy

Europe's leaders increasingly view control over digital infrastructure as akin to control over energy or other strategic resources. Without the ability to "develop its own digital solutions and ensure control over data," a state becomes dependent on foreign tech players, limiting its strategic room for maneuver and potentially subjecting itself to espionage or interference[6].



Supply-chain resilience

Geopolitical tensions and the pandemic-era shocks have also exposed Europe's vulnerability in tech supply chains. From semiconductors to cloud services, reliance on external providers leaves Europe at risk of disruptions or sudden price hikes.



A coordinated response

The EU has marshalled a multi-faceted response to these security challenges. Regulations (GDPR, DSA, DMA, and the EU AI Act, adopted in 2024 and entering phased implementation starting in early 2025) assert Europe's right to set rules on data and technology used within its single market.

Today, Europe is uncomfortably over-reliant on non-European technology in areas like cloud computing, processors, and AI. This dependency has stark security implications. European governments and companies know that data stored on U.S.-based cloud platforms could be accessed under extraterritorial laws such as the American CLOUD Act, while data on Chinese systems might be subject to state surveillance. Indeed, the data of European firms – whether "military, industrial, commercial or political" – can be exposed to foreign legal jurisdiction, "compromising security, competitiveness and strategic autonomy" in sensitive sectors[7]. For example, France's experience with its national Health Data Hub underlined these concerns: regulators argued that given U.S. disclosure laws, it was essentially illegal for a U.S.-based company to host French health records, even if the data resided on EU soil[8]. This ultimately forced the platform to seek a Europe-only cloud solution. The lesson is clear: **control over data infrastructure is now seen as a national security issue.**



EU officials point to recent cases where critical components saw prices soar, in some cases by several hundred percent — and even higher in isolated components, due to supply crunches. Such fragility strengthens the argument that Europe needs local, resilient digital infrastructure under its own governance. A culture of sovereignty is emerging in policy circles, emphasizing that decisions on innovation and IT procurement must weigh geopolitical risk alongside cost or performance. This doesn't mean banning foreign tech outright, but it does mean Europe wants the option to operate independently if needed. Initiatives like the EU Cybersecurity Certification Scheme (EUCC) and draft Cyber Resilience Act aim to ensure that critical hardware and software meet security standards and are free of backdoors. Some policymakers even debate whether to introduce procurement preferences or quotas for European tech solutions to bootstrap "digital sovereignty," reflecting the urgency of the moment.

Massive R&D investments are being funneled into areas like cybersecurity, cloud, quantum computing and AI – over €7.3 billion via Horizon Europe 2021–2027, including €1.6 billion earmarked for advancing artificial intelligence. Crucially, member states are beginning to collaborate on shared infrastructure. Rather than each country depending solely on U.S. hyperscalers, pan-European efforts like GAIA-X (discussed below) seek to create federated networks under collective European governance. As one cybersecurity executive summarized, "in the face of growing technological dependency and extraterritorial laws, developing digital sovereignty calls for practical action – from control over encryption to legal supervision of data transfers and support for certified European infrastructures." In short, geopolitical realities have made digital sovereignty not just a buzzword, but a prerequisite for national security and strategic autonomy in the 21st century.

Economic and Growth Considerations

Beyond security, Europe's push for its own digital infrastructure is fueled by economic motivations. Critics of "tech sovereignty" often claim Europe's preference for local or open-source solutions will raise costs and slow innovation. However, many European experts counter that this view ignores the hidden costs of the status quo – what some call the "**dependency tax**" Europe currently pays to foreign tech monopolies[\[20\]](#)[\[21\]](#).

The dependency tax

A recent in-depth study by consulting firm Asterès, commissioned by the Cigref association of IT users, quantified just how much Europe spends on non-EU cloud and software providers. The findings are striking: roughly 80% of Europe's enterprise cloud and software spending goes to U.S.-based companies, amounting to an estimated **€264 billion** every year[\[22\]](#). This is money European businesses pay to the likes of Amazon, Microsoft, and Google for cloud infrastructure or SaaS – an enormous outflow of capital. That €264 billion/year can be thought of as a direct drain on the European economy[\[23\]](#). It's supporting jobs and innovation overseas rather than in the EU. Indeed, the study calculated that European cloud dependence effectively sustains about 1.9 million jobs in the United States. If even a portion of this demand were served by European providers, it could create hundreds of thousands of high-skilled jobs in Europe. For example, if Europe managed to recapture just 15% of the cloud/software services it imports by 2035, it would mean an estimated **463,000 additional tech jobs** within the EU[\[24\]](#). The opportunity cost of inaction – in lost jobs, lost tax revenue, and lost industrial know-how – is enormous[\[25\]](#).

Local innovation and competitiveness

There's also the cost of stifled innovation to consider. When European companies large and small all rely on the same handful of external platforms, it becomes very difficult for European tech firms to compete or for homegrown alternatives to gain traction. Dominant foreign providers enjoy economies of scale and often lock-in customers with integrated services and punitive exit fees (for instance, high data egress charges)[\[26\]](#). This dominance can impose "unfavorable licensing terms" and leave European customers with little bargaining power[\[26\]](#). More insidiously, it discourages European entrepreneurs from building new solutions – why build the next collaboration platform or cloud service if the market is already sewn up by a global giant? The result is a brain drain and innovation drain: talent and venture capital gravitate to Silicon Valley or other hubs where these tech giants operate, and Europe loses out on cultivating its own digital champions[\[27\]](#). By investing in sovereign infrastructure and "strategic autonomy," Europe aims to "shift this paradigm, fostering sustainable, European-rooted growth" that keeps value creation within Europe[\[28\]](#). In the long run, a robust local tech ecosystem means more resilient growth – growth that isn't beholden to decisions made in Seattle or Shenzhen, and that aligns with Europe's stringent standards on data protection, privacy, and consumer rights[\[29\]](#).



Counting the true costs

When weighing costs, European advocates of sovereignty argue one must include the long-term risks of dependency. These include security risks (breaches or surveillance incidents can cost billions and erode public trust), geopolitical risks (sanctions or political disputes could abruptly cut off crucial services), and the negotiating disadvantage Europe faces when a few companies hold outsized market power. All of these are effectively a "price of inaction" that doesn't show up on a procurement spreadsheet, but is paid in lost sovereignty and agility. The debate is no longer framed as "protectionism vs. free market," but rather as investment in resilience. As one analysis put it, As one policy blog framed it, Europe's digital sovereignty drive is a **'strategic moonshot'** – "not because it's easy, but because it's hard" and necessary. The upfront investments in European cloud infrastructure, open-source software, or semiconductor fabs may be high, but they are seen as essential investments in Europe's future capacity and bargaining power – a far better alternative than continuing to pay a massive "tech rent" abroad in perpetuity. In summary, building Europe's own digital infrastructure is about ensuring the next generation of tech growth and jobs happen in Europe, fueling the EU's economic competitiveness in a digital age.

Retaining Talent and Fostering Innovation

Another pillar of Europe's strategy is the recognition that technology is ultimately a human endeavor – and without top talent, even the best infrastructure will languish. For years, Europe has faced a brain drain in advanced tech fields: many of the continent's brightest AI researchers, software engineers, and entrepreneurs have departed for Silicon Valley, Boston, or other global tech centers. The reasons often come down to opportunity and resources. The EU has world-class universities and produces highly skilled graduates, but historically it has struggled to offer the same scale of R&D investment, startup funding, or cutting-edge facilities that attract talent in the United States or China[32][33]. As a Harvard analysis noted, Europe "struggles to retain AI and STEM talent, with many skilled professionals leaving for the United States, where large tech companies and substantial research facilities offer more attractive opportunities." [33] This talent exodus further hampers Europe's ability to build an innovative ecosystem – it's a vicious circle where lack of local opportunity drives talent away, which in turn makes it harder for local tech industries to thrive.

01

Breaking the cycle

European policymakers and industry leaders know that retaining talent requires creating an environment where innovators can do world-class work without leaving Europe. This involves multiple efforts: improving salaries and career prospects for researchers and engineers, directing more public and private funding into tech R&D, and building facilities that give talent the tools they need to succeed.

02

Infrastructure for academia and discovery

Europe's universities and research centers are not just talent pipelines – they are also end-users that urgently need sovereign infrastructure. Scientific research today relies on big data and big compute. If European researchers have to rely on foreign-owned cloud services or hardware to do advanced research (be it genomic sequencing, climate modeling or AI training), Europe risks both security issues and missed innovation.

03

High-performance computing leadership

Hand-in-hand with cloud, Europe is also investing in high-performance computing as a strategic asset for both science and industry. In 2023–2025, the EU's EuroHPC Joint Undertaking deployed some of the world's most powerful supercomputers in European facilities.

Leaders in the European cybersecurity sector, such as the CEO of Stormshield, have argued that Europe must "invest massively via support for universities and start-ups" and make training and retaining digital talent a top priority – via "appropriate programs and competitive salaries." In practice, this might mean EU-wide scholarships for AI specialists, new research institutes for emerging technologies, and stronger incentives for European tech startups (e.g. easing access to capital markets, or preferential procurement as mentioned earlier). The EU Chips Act and various national AI strategies all include talent components, from sponsoring semiconductor engineering programs to funding PhD positions in AI. Crucially, sovereign infrastructure projects themselves can help retain talent: when Europe builds its own cutting-edge supercomputers, cloud platforms or AI research centers, it not only serves strategic needs but also creates exciting opportunities at home for experts to work on leading technology.

Thus, a key part of the sovereignty agenda is providing world-class research infrastructure within Europe, so that scientists can push the boundaries of knowledge on European soil and within European legal protections. The EU's European Open Science Cloud (EOSC) initiative is one example: EOSC aims to give all European researchers a "trusted multi-disciplinary environment" where they can store, share and reuse data and tools for research within a federated European network[35]. Launched in 2018, EOSC is now establishing federated data nodes across member states – the first EOSC EU Node came online in late 2024 – to interconnect university data centers and national research clouds into a secure, open framework[36][37]. This aligns with the broader goal of sector-specific "data spaces" under the EU's data strategy (similar to how GAIA-X envisions data spaces for industry, EOSC is the data space for science).

Most notably, Europe's first exascale supercomputer, called **JUPITER**, was inaugurated in Germany in 2025 and achieves over one quintillion operations per second. Beyond the raw performance, JUPITER is significant for talent and innovation: it "strengthens Europe's digital sovereignty, accelerates discovery, and ensures that the most powerful and sustainable computing resources are available to our researchers, innovators, and industries," as EU Commissioner Ekaterina Zaharieva remarked at its launch[38]. In other words, European scientists and engineers now have cutting-edge computational tools at their disposal at home, reducing the temptation to relocate elsewhere for want of infrastructure. JUPITER is part of a network of planned "AI & supercomputing factories" – large-scale, energy-efficient computing hubs across Europe dedicated to AI model training and advanced simulations[39]. These facilities "bring together the key ingredients for AI success: computing power, data, and talent," providing startups, industries and academia access to the massive capacity needed for breakthroughs[40]. By investing in such infrastructure, Europe sends a strong message to its tech workforce: **you can do big things here**. Over time, a robust ecosystem of local cloud services, HPC centers, and data platforms could make Europe a net importer of talent – attracting researchers and entrepreneurs who see Europe as the place to be for privacy-conscious, cutting-edge tech development.

Building Europe's Own Infrastructure: Key Initiatives and Examples

To translate these strategic goals into reality, Europe has launched a number of initiatives spanning policy, industry collaboration, and direct investment. Below we highlight a few flagship efforts that illustrate how the EU and member states are trying to co-create sovereign infrastructure for both the public and private sectors.

Gaia-X – Federated European Cloud Ecosystem

One of the most prominent projects is Gaia-X, unveiled in 2020 by France and Germany. Gaia-X is often described as Europe's bid for a sovereign cloud, though it isn't a cloud provider itself. Rather, it's an alliance and technical framework aimed at knitting together a federation of European cloud and data service providers under common standards for interoperability, transparency and trust[\[41\]](#)[\[42\]](#). The idea is to prevent any single platform (especially a non-European one) from monopolizing Europe's data infrastructure. Gaia-X envisions an "ecosystem of interconnected nodes based on open standards, designed to prevent concentration of power in the hands of a single player."[\[43\]](#) In practical terms, it is developing specifications, open-source code, and governance labels that cloud providers or data platforms can adopt[\[44\]](#)[\[45\]](#). Once compliant, these providers can more easily federate their services – meaning a company in Europe could use multiple cloud vendors seamlessly, or share data with partners across a common interface, all while retaining control and sovereignty over data usage policies[\[42\]](#)[\[46\]](#). A core concept of Gaia-X is the creation of sector-specific "data spaces." For example, in healthcare, automotive, or energy, stakeholders are encouraged to build shared data pools and services on Gaia-X principles, so that sensitive data (like health records or car telemetry) is handled in accordance with EU rules and not siloed by any one foreign corporation[\[47\]](#). As of 2025, Gaia-X is moving into implementation with over 180 federated data spaces in development across various domains[\[48\]](#). This shows both the ambition – spanning everything from smart city data to industrial manufacturing data – and the complexity of the task.

- ❏ However, Gaia-X's journey has not been smooth. It has faced skepticism and growing pains, highlighting how challenging building sovereign alternatives can be. Early on, some open-source advocates warned Gaia-X might become a "Trojan horse" for Big Tech, noting that numerous U.S. tech firms (Microsoft, Amazon, etc.) joined the initiative as members[\[49\]](#). There were fears that these dominant players could water down Gaia-X's requirements or use it to their own advantage, much like a previous French cloud consortium (project "Andromeda" around 2011) ended up channeling public funds to large non-European companies without achieving its original goals[\[49\]](#). Internal governance issues also emerged.

- ❏ By late 2021, reports of infighting and slow progress came to light; one founding member, French cloud provider Scaleway, very publicly quit Gaia-X, citing frustration that it was not delivering a truly sovereign European cloud and was "captured" by big corporate interests[50]. These controversies underscore a fundamental tension: Europe wants an open, industry-driven approach to tech sovereignty (to encourage broad adoption), but if too open, it risks being co-opted by the very foreign giants it seeks to offset. Gaia-X leaders have since tried to tighten the governance and refocus on European SME and cloud-provider involvement. The project's success is not guaranteed – it remains a bold experiment in collaborative infrastructure. Yet even its struggles have been instructive, revealing the need for political will and trust among European players to prefer homegrown solutions. Gaia-X has at least succeeded in galvanizing debate and spawning "lighthouse" projects in data-intensive industries, planting the seeds for a more sovereign cloud ecosystem in the years ahead.

National "Cloud of Trust" efforts

At the member-state level, countries are also taking action for critical infrastructure. France, for instance, introduced the concept of Cloud de Confiance (Trusted Cloud) in 2021. Under this scheme, cloud services for sensitive data (like health, defense, or government data) must be operated by companies under EU jurisdiction, even if they use technology from U.S. firms. This led to partnerships where U.S. cloud tech is licensed to European providers who run the data centers and guarantee data stays under French/EU legal control[51]. The French Health Data Hub mentioned earlier is now migrating to such a setup. Germany and others have similar guidelines for certain sectors, essentially mandating sovereign options for areas where data sensitivity or strategic importance is highest. Over time, these could bolster European cloud firms (such as OVHcloud, Deutsche Telekom's T-Systems, or smaller niche providers) by giving them a home-field advantage in public sector contracts.

European Open Science Cloud & Supercomputing

We already touched on EOSC and EuroHPC in the context of supporting researchers and retaining talent, but it's worth noting how these fit into the broader sovereignty puzzle. The European Open Science Cloud can be seen as the academic sibling of Gaia-X – both seek to create federated, interoperable clouds, one for science and one for industry. EOSC's emphasis is on open data and scientific collaboration, but by ensuring this happens on European infrastructure, it also secures an independent capability for discovery (for example, European climate researchers sharing data via EOSC won't be locked out if a foreign provider changes terms or if transatlantic data flows get restricted). Meanwhile, the EuroHPC initiative, by funding ultra-powerful supercomputers like JUPITER, Leonardo (in Italy), and LUMI (in Finland), ensures that Europe remains at the forefront of computing power. These machines are not just prestige projects; they have practical implications for sovereignty. Supercomputers are used in designing advanced materials, nuclear simulations, cryptography, AI model training and more – some of these are sensitive or strategic domains. Owning that hardware on European soil, with European teams, avoids scenarios where Europe might have to depend on another country's supercomputing facility (which might not be available for EU-specific projects or could come with strings attached). Commissioner Zaharieva's statement at JUPITER's launch explicitly framed it in sovereignty terms, celebrating that Europe's most powerful computing resources are now locally controlled and available to European users across research and industry[38].

Summing up the strategy

Europe's approach to building sovereign infrastructure is thus multi-layered. At the top, there is a clear policy direction backing "strategic autonomy" in digital tech (frequently emphasized in EU official documents and speeches). Then there are regulatory levers – from privacy to cybersecurity to competition laws – shaping the market context in favor of sovereignty (e.g., data localization requirements for certain data, or interoperability mandates that reduce lock-in). Concurrently, there are collaborative industry initiatives like Gaia-X that try to rally the private sector around common European-centric standards. And finally, direct investment projects (EuroHPC, EOSC, national clouds, etc.) build out the physical and software infrastructure. Importantly, these efforts are increasingly linked together. For example, the European Data Act and Data Governance Act create rules for data sharing which Gaia-X's data spaces will implement; the Chips Act funding for semiconductor plants complements the goal of cloud sovereignty by ensuring local supply of critical hardware. We see a concerted attempt to cover all bases – legal, technological, and economic – to gradually weave a fabric of digital sovereignty.

Conclusion: Toward a Sovereign and Thriving European Digital Ecosystem

Europe's quest for digital sovereignty is a long-term project born of both aspiration and anxiety. It aspires to a future where European companies, governments, and citizens can leverage cutting-edge digital technologies on their own terms – with full confidence in the security of their data and in alignment with Europe's democratic values. At the same time, it is driven by the sobering realization that without intervention, Europe could slip into permanent second-tier status in the digital realm, wholly dependent on decisions made in boardrooms an ocean away. The stakes are not just technical or economic, but civilizational: in an era when data and AI will underpin everything from healthcare and finance to national defense, whoever controls these infrastructures will wield enormous influence.

The journey will not be easy. There are valid concerns about protectionism, and Europe must strike a careful balance to avoid excessive isolation or fragmentation of the global internet^[5]. Sovereignty cannot mean stagnation – Europe also needs to remain open to international collaboration and trade, and European tech firms will still want to serve global markets. The key is finding a balance between openness and control. Early missteps and controversies (like Gaia-X's struggles) show that unity and clarity of purpose will be essential. Europe's internal diversity – 27 member states, each with their own priorities and industrial strengths – can be a hurdle, but also a source of strength if harnessed (for instance, France's expertise in AI, Germany's in industrial engineering, and Nordic countries' in telecom can all complement each other in a pan-European ecosystem).

"We choose to go to the Moon not because it is easy, but because it is hard"^[31] – meaning the difficulty is precisely why it's worthwhile.

One encouraging sign is that Europe increasingly frames digital sovereignty as a positive opportunity rather than a cost. It's about investing in Europe's own capacity – a form of self-reliance that, in the long run, should pay dividends economically and socially. Yes, it requires significant upfront investment and some tough choices (e.g. favoring local providers, funding "moonshot" projects). But as a rebuttal to skeptics aptly put it, "We choose to go to the Moon not because it is easy, but because it is hard"^[31] – meaning the difficulty is precisely why it's worthwhile. By undertaking the "hard things" now, such as building a distributed European cloud or a new generation of European AI startups, the EU seeks to future-proof its economy and sovereignty for decades to come. The cost of doing nothing – of remaining a digital colony – is deemed far higher when one considers the dependency tax, lost growth, security risks, and brain drain that would otherwise persist^[30].



In conclusion, Europe's push for its own digital infrastructure is about more than technology. It is a strategic, economic, and human-capital endeavor to shape Europe's destiny in a digitized world. If successful, European businesses will operate AI and cloud systems without shipping sensitive data overseas, European researchers will make breakthroughs on European supercomputers, and European youths will see thriving tech careers at home. The road is long and there will be challenges and adjustments along the way. But the direction is set: toward a Europe that is digitally sovereign – mastering its own tools, guarding its values, and sharing in the prosperity of the digital age on its own terms. As EU officials often remind us, digital sovereignty is not an end in itself, but a means to ensure that the digital revolution advances European society's goals of security, prosperity and freedom[52][53]. In that sense, investing in sovereign infrastructure is investing in the very future of Europe's democracy and competitiveness – a future that Europeans intend to build and own together.

About Onyx Consulting

This white paper was co-authored by Jean-Christophe Cuvelier and advanced AI research tools, reflecting the innovative approach at Onyx Consulting.

At Onyx Consulting, we specialize in empowering European organizations to develop robust, sovereign AI infrastructures. Our expertise spans strategic guidance, software engineering, and infrastructure design, ensuring clients achieve unparalleled data control, GDPR compliance, and crucial independence from global hyperscalers. This enables businesses, universities, and public institutions to innovate securely and confidently within the stringent European legal frameworks.

We established Onyx Consulting after two decades dedicated to software development and architecture, fueled by a steadfast conviction: for Europe to thrive—to remain free, competitive, and innovative—it must unequivocally master its own digital foundations.

If you resonate with this vision, we welcome the opportunity to connect and discuss how we can collectively strengthen Europe's technological sovereignty.

👉 Connect with me on LinkedIn:
<https://www.linkedin.com/in/totophe/>

Learn more at <https://getonyx.eu>



Sources

1. Fleming, S. What is digital sovereignty and how are countries approaching it? – World Economic Forum, Jan 2025[\[54\]](#)[\[4\]](#).
2. Hentzen, P.-Y. European Union puts its Digital Sovereignty to the Test – Stormshield (press article), 2023[\[6\]](#)[\[7\]](#).
3. van Oirsouw, T. AI, Digital Sovereignty, and the EU's Path Forward – Ash Center, Harvard Univ., 2024[\[55\]](#).
4. Rebuttal: Digital Sovereignty is an Investment in Europe's Future, Not a Cost to Its Present – EuroStack blog, May 2025[\[23\]](#)[\[29\]](#).
5. Asterès & Cigref Report – Technological dependence on American cloud and software services: Economic consequences for Europe, Apr 2025[\[22\]](#)[\[24\]](#).
6. Musiani, F. Gaia-X: the bid for a sovereign European cloud – Polytechnique Insights, Jun 2025[\[41\]](#)[\[47\]](#).
7. Wikipedia: Gaia-X[\[42\]](#)[\[50\]](#) (initiative details and controversies).
8. European Commission – European Open Science Cloud (EOSC) overview, 2025[\[35\]](#)[\[36\]](#).
9. Techzine – JUPITER is Europe's fastest supercomputer, Sep 2025[\[38\]](#)[\[40\]](#).
10. Morrison Foerster (NYU blog) – Health Data Made in France – Sovereign Cloud for Health Data?, Nov 2020[\[8\]](#)[\[51\]](#).