PALADIN

GLOBAL INSTITUTE

NAVIGATING DIGITAL SOVEREIGNTY IN EUROPE



Preamble

American businesses and their investors are increasingly wary of the risks associated with Europe's demand for sovereignty of its digital infrastructure. In fact, in its pre-initial public offering (IPO) filing with the Securities and Exchange Commission (SEC), Anthropic warned that this is a risk factor for investors to consider.

> ***We are expanding our data center capacity internationally as part of our efforts to diversify our infrastructure footprint and reduce concentration risks associated with operating a significant portion of our compute infrastructure in the United States and to support our international growth strategy, including by entering into letters of intent and negotiating lease and related agreements for data center facilities in multiple non-U.S. jurisdictions, which exposes us to additional risks related to foreign regulatory requirements and approvals, data sovereignty, and localization laws, governmental access or assistance requirements, cross-border data transfer restrictions, foreign tax regimes, and increased operational complexity.***[1]

Anthropic also identifies the United States government's ability to impose export controls on Anthropic's advanced models as another risk to investment. These warnings to potential investors come just days after the Wall Street Journal reported that Elon Musk throttled Ukraine's use of its low earth orbit satellite communications constellation during an ongoing conflict with Russia.[2] Anthropic's warnings and Starlink's actions are the latest examples validating Europe's concerns with a so-called "kill switch." This paper answers questions by American technology companies and their investors on responding to European sentiments in connection with sovereignty.

---

1 Anthropic, PBC, Form S-1 Registration Statement, October 26, 2026, https://www.sec.gov/Archives/edgar/data/2130357/000162828026068676/anthropicpbc-sx1ax1.htm.

2 "Musk Ordered Starlink Slowdown That Blindsided Ukraine," The Wall Street Journal, October 21, 2026, https://www.wsj.com/world/ukraine-starlink-elon-musk-trump-dbc49193.

Executive Summary

Digital sovereignty is now one of the most frequently invoked terms in European policy and technology circles — and one of the least consistently defined. At its core, it describes a growing determination among European governments and institutions to reduce dependence on American technology providers across cloud infrastructure, software, artificial intelligence (AI), and hardware. That determination is driven less by a rejection of American technology than by a specific fear: that access to it could be withdrawn.

This paper examines why that fear took hold, what digital sovereignty means in practice across the technology stack, and how the resulting demand is shaping the way technology is built. Full decoupling from American technology is neither feasible nor imminent; the two technology bases are too structurally intertwined for separation to be a near-term option. Nor is decoupling automatically safer. Sovereignty pursued through domicile alone — local vendors, local data centers, local flags — can weaken foundational security principles and create new vulnerabilities unless security is engineered in from the start. Sovereignty alone does not guarantee security. Europe can strengthen both sovereignty and security by applying existing security and trustworthiness criteria to the systems it is building and buying.

Europe is renegotiating the terms of technological dependence, reshaping procurement, regulation, and industrial policy across the continent. This paper recommends a series of coordinated policy responses that give Europe greater agency while preserving transatlantic security and technological cooperation. The United States and Europe should build a trusted transatlantic technology ecosystem, with guaranteed allied access, giving European governments greater confidence that critical technologies will remain available. Both sides should develop common, evidence-based security standards and interoperable systems that preserve the cross-border visibility defenders need. Europe should continue to invest in its own companies, infrastructure, talent, and technical skills, building greater capacity without cutting itself off from the technologies on which it still depends. Together, these measures can give Europe greater control and capability without fragmenting the technology ecosystem on which collective security depends. Digital sovereignty is not a location; it is the ability to exercise meaningful control over technology while preserving the security, interoperability, and trusted relationships required to make that control durable.

How We Got Here: Defining Digital Sovereignty

Defining the Term

The meaning of "digital sovereignty" remains unsettled. Digital sovereignty means different things to different governments, institutions, and experts, and its definitions are still being written. Rather than adopt a single definition, this paper draws on three complementary accounts. The World Economic Forum (WEF) defines digital sovereignty as the ability to *control* one's own digital destiny — the data, hardware, and software a nation relies on and creates — and frames it as a structural dilemma between preserving openness and interoperability on one side and safeguarding national autonomy and resilience on the other.[3] The European Commission's Technological Sovereignty Package offers a more institutional definition: Europe's ability to develop, control, and scale the critical technologies, infrastructure, services, and data that underpin its economy, security, and society.[4] The cyber diplomat Jovan Kurbalija is more direct: in most cases, he argues that digital sovereignty describes a country's desire to reclaim some measure of digital authority from technology companies and platforms.[5]

Taken together, these definitions present digital sovereignty as a combination of control, capacity, and authority: control over the technology and data on which a country depends, the capacity to develop and operate critical systems, and the authority to set the conditions under which those systems are used.

Beneath the definitional variation sit two different policy objectives. Europe treats sovereignty as a path to autonomy. The United States treats it as a path to technological primacy.

In practice, European governments and institutions are concerned with autonomy: the capacity to operate without dependence on decisions made elsewhere. For some, that means control, independence, or choice. For others, it means the ability to engineer and operate homegrown infrastructure on their own terms. The instruments reach across all three domains as articulated by the WEF: data (including cloud infrastructure), software (including applications and models), and hardware. The sovereign cloud requirements and national certification schemes govern where data sits and who can reach it. Procurement rules set conditions that favor European vendors. Public investment seeks to expand European semiconductor production, while export controls seek to protect strategic European capabilities. The instruments differ in intent and reach, and yet they draw lines at national borders in the same way.

3 "What is digital sovereignty and how are countries approaching it?" *World Economic Forum, Geo-Economics and Politics*, January 10, 2025, https://www.weforum.org/stories/geo-economics-and-politics/europe-digital-sovereignty.

4 European Commission, "Questions and answers on the Technological Sovereignty Package," QANDA/26/1188, June 3, 2026, https://ec.europa.eu/commission/presscorner/detail/en/qanda_26_1188.

5 Jovan Kurbalija, "Digital sovereignty stack: Infrastructure, services, data, and AI knowledge," DiploFoundation, 2026, https://www.diplomacy.edu/blog/digital-sovereignty-stack-infrastructure-services-data-and-ai-knowledge/.

For the U.S., primacy means the capacity to lead in developing and deploying critical technologies – and to set the terms on which others adopt them. The 2026 U.S. National Cyber Strategy commits the country to securing "American technology dominance," and the instruments follow from it.[6] Export controls restrict access to advanced chips, chipmaking equipment, compute, and model weights on national security grounds, with the collateral effect of shaping markets toward American technology. Trusted-vendor designations steer procurement toward the American technology stack. A domestic build-out expands compute capacity onshore.

Europe's pursuit of autonomy and America's pursuit of primacy are therefore not parallel projects. The former is, in significant part, a response to the latter: Europe's dependence on American technology, combined with U.S. policies that demonstrate how that dependence can be leveraged, has made technological reliance a question of sovereignty. Europe's response has been to seek greater control over where its technology comes from, where it operates, and who ultimately has authority over it. Yet the infrastructure over which Europe is seeking greater control crosses borders by design.

The Kill Switch Fear

For many European officials, dependence on American technology companies is a concrete fear. It is the fear that a U.S. provider, under U.S. government pressure, could sever access to critical systems without warning. That "kill switch" fear has pushed European sovereignty efforts toward relocating control back onto European soil.

The concern began taking shape more than a decade ago, in the litigation between Maximilian Schrems, an Austrian citizen, and Facebook, a U.S. company, about the company's handling of European data under the European Union's (E.U.) General Data Protection Regulation (GDPR).[7] To comply with GDPR, the E.U., in partnership with the U.S., developed a framework, known as Privacy Shield, to facilitate cross-border transfers of data with the requisite level of protection of European data.[8] And the European Commission published a set of Standard Contractual Clauses (SCC) for industry to use in their contracts to transfer data, which require non-E.U. companies to comply with the GDPR.[9] However, in practice, the Court of Justice of the European Union (CJEU) found that American intelligence authorities – the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 – eroded the intended level of protection of European

6 The White House, (March 2026), President Trump's Cyber Strategy for America. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf.

7 Regulation (EU) 2016/679 (General Data Protection Regulation), *Official Journal of the European Union* L 119 (May 4, 2016), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

8 Commission Implementing Decision (EU) 2016/1250 on the adequacy of the protection provided by the EU–U.S. Privacy Shield, July 12, 2016, https://eur-lex.europa.eu/eli/dec_impl/2016/1250/oj.

9 Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, June 4, 2021, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

data contemplated by the GDPR.[10] In a series of cases dubbed *Schrems I* and *Schrems II,* the CJEU invalidated the E.U.–U.S. Privacy Shield because U.S. surveillance law reaches European data held by U.S. providers. The E.U. now requires companies relying on SCCs to implement supplementary technical measures to safeguard European data.[11]

Two successive transatlantic transfer frameworks were struck down on these grounds. Both times, European courts asserted jurisdiction over an American technology company and, in effect, relocated control of European data onto European soil. Schrems established the predicate rather than the fear itself — that U.S. law reaches European data wherever it sits. What came next established that access could be withdrawn.

In February 2025, following Executive Order 14203 sanctioning Karim Khan, the chief prosecutor of the International Criminal Court (ICC), Khan reportedly lost access to his Microsoft email account and moved to a Swiss provider.[12] Microsoft denied cutting the account. The sanction was a retaliatory measure for the Court's prosecution of Israeli Prime Minister Benjamin Netanyahu and former Defense Minister Yoav Gallant, issued on the U.S. position that the ICC holds no legal jurisdiction over the United States or Israel. In October 2025, the ICC announced it would migrate off Microsoft entirely and onto open software built under a German digital sovereignty initiative.[13] The facts remain contested; the migration proceeded anyway.

Trust in a provider or partner may take years to establish, but a single disruption — or even the credible possibility of one — can quickly undo it. Recent U.S. provider actions have amplified the kill switch fear further. According to reporting, in October 2026, the Starlink founder, Elon Musk throttled Ukraine's access to satellite communications technology during its conflict with Russia.[14] In June 2026, consistent with its U.S. Export Control legal authorities, the U.S. Department of Commerce directed the U.S. frontier lab, Anthropic, to suspend all access to its newly released Claude Fable 5 and Mythos 5 models for any foreign national anywhere in the world — including

10 Court of Justice of the European Union, Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Maximilian Schrems*, ECLI:EU:C:2020:559, July 16, 2020, https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=en.

11 European Data Protection Board, *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, Version 2.0, June 18, 2021, https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

12 Executive Order 14203, "Imposing Sanctions on the International Criminal Court," February 6, 2025, 90 FR 9369 (February 12, 2025), https://www.federalregister.gov/documents/2025/02/12/2025-02612/imposing-sanctions-on-the-international-criminal-court;

13 "International Criminal Court Dumps Microsoft Office," *The Register*, October 31, 2025, https://www.theregister.com/2025/10/31/international_criminal_court_ditches_office/.

14 "Musk Ordered Starlink Slowdown That Blindsided Ukraine"*, The Wall Street Journal*, October 21, 2026, https://www.wsj.com/world/ukraine-starlink-elon-musk-trump-dbc49193?st=wCgPVz.

the company's own non-U.S. employees — citing national security concerns.[15] Because Anthropic had no practical way to filter users by nationality across its global platforms in real time, it disabled both models for every customer worldwide within hours. Commerce lifted the order eighteen days later, but its control over U.S. technology companies was unambiguous.[16] Anthropic's October 2026 pre-IPO filing with the SEC now lists, among the risks to investors, that an American agency can cut off access to critical American technology as an ongoing possible disruption.[17] Both actions are evidence that European officials point to when they describe the kill switch.

15 "Anthropic Disables Access to Fable 5 and Mythos 5 to Comply with Government Directive," *CNBC*, June 12, 2026, https://www.cnbc.com/2026/06/12/anthropic-disables-access-to-fable-5-and-mythos-5-to-comply-with-government-directive.html.

16 "Anthropic Says Trump Admin Has Lifted Export Controls on Claude Fable 5 and Mythos 5," *CNBC*, June 30, 2026, https://www.cnbc.com/2026/06/30/anthropic-says-trump-admin-has-lifted-export-controls-on-claude-fable-5-and-mythos-5.html.

17 Anthropic, PBS Form S-1 filing to the SEC, October 26, 2026, https://www.sec.gov/Archives/edgar/data/2130357/000162828026067168/anthropicpbc-sx1.htm.

European Digital Sovereignty in Practice

The Three Domains

Across Europe, governments and institutions are reconfiguring their technology dependencies — how they procure cloud infrastructure, govern data flows, evaluate AI systems, and judge the trustworthiness of foreign providers. In practice, digital sovereignty means pursuing autonomy from American companies across three domains: data (including cloud infrastructure), software (including applications and models), and hardware. Additionally, the concentration of effort in these domains reflects the geopolitical energy behind the development, deployment, and adoption of AI. Advances in data quality, algorithmic efficiency, and training methods are creating opportunities for smaller, more efficient models — a shift that has fueled European interest in homegrown alternatives. Still, no European model has yet reached frontier scale.

Full decoupling, though, is not available in the near term. Gaia-X, the international nonprofit association that offers a digital sovereignty governance framework, has acknowledged that American hyperscalers can serve roughly 90 percent of European cloud requirements.[18] What is emerging instead is a hybrid architecture: European actors taking control of specific elements within each domain while remaining structurally dependent on American providers for frontier capability.

The scope of sovereignty will likely continue to expand as new dependencies emerge. Space infrastructure may be the next frontier, as communications, positioning, and other digital services increasingly depend on commercial satellite systems operating across national boundaries.

Domain	European Autonomy Goal	Current Reality
Cloud Infrastructure and Data Sovereignty	Sovereign data storage and hosting	American hyperscalers hold nearly 70 percent of the European cloud market; local providers hold about 15 percent[19]
Software, including Applications and Models	Procurement rules favoring European Union (E.U.) vendors; Homegrown, efficient models	American platforms remain dominant across enterprise and public-sector software; No European model has reached frontier scale
Hardware	Domestic semiconductor and chip capacity	Limited leading-edge fabrication; the longest path to autonomy

18 Ulrich Ahle, CEO, Gaia-X, quoted in Christine Horton, "Gaia-X Warns US Hyperscalers About Selling Cloud Sovereignty," *Channel Dive*, December 19, 2025, https://www.channeldive.com/news/gaia-x-warns-us-hyperscalers-about-selling-sovereignty/807362/.

19 Synergy Research Group, "European Cloud Providers' Local Market Share Now Holds Steady at 15%," July 2025, https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15.

Cloud Infrastructure and Data Sovereignty

Cloud infrastructure — the servers, storage systems, and networking that underpin digital services — is where European sovereignty efforts are most visible in practice, driving data residency requirements, sovereign cloud procurement mandates, and initiatives like Gaia-X. The scale of Europe's dependence limits how far that control can extend. Three U.S. hyperscalers hold the substantial majority of the European cloud market, and the "sovereign cloud" products they now offer do not resolve the underlying legal exposure (e.g., the Clarifying Lawful Overseas Use of Data (CLOUD) Act reaches data wherever it physically sits).[20] European governments are responding with national certification schemes and procurement rules that set baselines for where data can be stored and who can reach it. France's SecNumCloud qualification, for example, effectively bars American hyperscalers from bidding on the most sensitive government contracts.

Data residency has driven substantial investment in data center capacity across Europe. Under the E.U. Data Act, the Network and Information Systems Directive v. 2 (NIS2), and national frameworks like France's SecNumCloud and Germany's Federal Office for Information Security (BSI) Cloud Computing Compliance Criteria Catalogue (C5), European governments and enterprises are investing heavily in in-region data center capacity. The European Data Centre Association projects €176 billion in data center investment between 2026 and 2031, double the figure forecast a year prior.[21] American hyperscalers are responding to residency pressures. In January 2026, Amazon Web Services (AWS) launched its European Sovereign Cloud in Brandenburg, a €7.8 billion investment structured as a standalone German entity, physically and logically isolated from AWS's global infrastructure.[22] Despite the uptick in national investment, the largest share of European data center investment still comes from American players, and physical presence in Europe satisfies residency requirements without reducing reliance on American hyperscalers.

Software, including Applications and Models

In software, European sovereignty concerns are reshaping procurement behavior. American platforms remain dominant across enterprise and public-sector software, and European governments are increasingly using procurement rules to create the conditions for alternatives. In Ireland, the government cancelled a €1 billion Microsoft tender amid sovereignty questions, with calls to weigh European and open-source options.[23] The government signaled it would publish a new tender "as early as is feasible" – an indication that the issue was process and scrutiny rather

20 Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V (2018), codified at 18 U.S.C. § 2713, https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2713&num=0&edition=prelim.

21 European Data Centre Association, *State of European Data Centres 2026* (Brussels: EUDCA, February 2026), https://www.eudca.org/new-2026-state-of-european-data-centres.

22 Amazon Web Services, "AWS Launches AWS European Sovereign Cloud and Announces Expansion Across Europe," press release, January 15, 2026, https://press.aboutamazon.com/aws/2026/1/aws-launches-aws-european-sovereign-cloud-and-announces-expansion-across-europe.

23 Lindsay Clark, "Ireland stalls €1B Microsoft tender amid digital sovereignty questions," The Register, July 22, 2026, https://www.theregister.com/public-sector/2026/07/22/ireland-stalls-1b-microsoft-tender-amid-digital-sovereignty-questions/5276149.

than a shift away from Microsoft entirely. Ireland's pause illustrates the pattern: not a blanket rejection of an American provider, but a refusal to award a contract of that size without alternatives on the table. European governments want optionality, and procurement is the lever they can control.

European ambitions in AI are significant, and the capability gap at the frontier remains wide. Governments and institutions have prioritized two dimensions of the AI technology stack: the infrastructure layer, where dependence on American-designed chips and hyperscale infrastructure is near-total, and the model layer, where the goal is a viable European alternative to American frontier models.

Mistral, founded in Paris in 2023, represents Europe's leading frontier effort. It develops its own models and sells them through a pay-per-token developer API, a consumer assistant, and enterprise and on-premise deployments, releasing model weights openly to drive adoption. Its strategy rests on efficiency rather than scale, and its models are well regarded for their cost-efficiency, trailing the leading American models on complex reasoning while closing much of the gap on routine tasks and on European languages. The capital has followed — in September 2026, Mistral raised €3 billion at a valuation above €21 billion, the largest equity round ever completed by a European technology company.[24] The investment signals the demand for a viable European alternative; however, the gap between Mistral and the American frontier labs in both capital and compute capacity remains substantial.

The frontier race is being run between the United States and China, and other technology powers are deciding where to compete within it. Nandan Nilekani, co-founder and chairman of Infosys, has argued that India should leave frontier model development to Silicon Valley and concentrate on applications, synthetic data, and small language models, on the view that models will commoditize and value will accrue to what is built on top of them.[25]

Similarly, the nearer opportunity for European developers may sit at the application layer: building tools, fine-tuned models, and sector-specific systems built on top of American foundation models rather than competing at the frontier directly. European data, domain expertise, and familiarity with the European regulatory environment are advantages at that layer in a way they are not at frontier scale. Investment in frontier parity is a decade-long industrial project. The application layer therefore offers Europe a nearer-term opportunity.

Hardware

Hardware is where European dependence runs deepest and the path to autonomy is longest. Europe has almost no leading-edge logic fabrication, and the E.U. Chips Act target of 20 percent of global semiconductor production by 2030 remains far from current output. Dependence on American-designed processors underpins every other domain examined in this paper — the compute supporting European AI efforts and the servers inside European sovereign cloud are built on American designs.

24 Mistral AI., September 2026, "Making sovereign, open-weight AI the technology frontier," Retrieved from https://mistral.ai/news/mistral-makes-sovereign-open-weight-ai-to-frontier/

25 Nilekani, Nandan, July 2025, "Indian tech pioneer Nandan Nilekani on AI's future, LLMs, U.S.–China rivalry," Rest of World, Retrieved from https://restofworld.org/2025/nandan-nilekani-interview-india-ai/.

Europe's position varies sharply by segment. ASML holds a monopoly on extreme ultraviolet lithography (EUV) tool shipments and roughly 90 percent of deep ultraviolet (DUV) immersion shipments, with no substitute available from any American or Asian supplier; Carl Zeiss SMT supplies the optics those systems depend on. American export control policy toward China operates through that node; restricting Chinese access to advanced lithography requires Dutch licensing decisions, which the Netherlands has issued in step with U.S. restrictions since 2019. European firms also lead in automotive and power semiconductors, where Infineon held the largest share of the global automotive semiconductor market in 2024, followed by NXP and STMicroelectronics. European strength lies in the equipment that enables fabrication and in semiconductor segments less dependent on the leading edge.

The Price of Domicile

The costs of pursuing autonomy, even at the margins, are high. Industry analysts put the sovereign cloud premium at 15 to 30 percent, and Europe is paying it anyway.[26] Gartner projects European sovereign cloud Infrastructure-as-a-Service (IaaS) spending will more than triple from $6.9 billion in 2025 to $23.1 billion in 2027.[27]

The premium is an expense and diverts capital from capability. Europe has no frontier model and almost no leading-edge fabrication, and it is paying 15 to 30 percent above market for infrastructure whose distinguishing feature is where it is domiciled rather than what it can do. The capability cost is compounded by the cost of procurement itself. Ireland's cancelled tender created both delay and re-tendering costs – the requirement did not disappear when the contract did, and the interval is spent running the systems the tender was meant to replace.

Some European enterprises are hosting models themselves to keep sensitive data and critical operations off a foreign provider's infrastructure. This comes at a cost on two fronts. In compute, a self-hosted deployment carries a largely fixed bill whether or not it is fully used. And, in security, protecting the models becomes a standing internal cost: securing and patching the inference stack, red-teaming for bypasses, building moderation and abuse monitoring, and re-testing as new techniques surface – work that an API provider can perform across its entire customer base and price into the service.

The E.U. Chips Act target of 20 percent of global semiconductor production by 2030 is the most expensive commitment in the sovereignty program and the furthest from delivery, and it is the one domain where the spending buys no near-term autonomy at all.[28] The pattern is consistent: Europe is paying most where it can change least.

26 Boston Consulting Group, August 2025, Cloud Cover: Price Swings, Sovereignty Demands, and Wasted Resources, Retrieved from https://www.bcg.com/publications/2025/cloud-cover-price-sovereignty-demands-waste.

27 Gartner, Inc., February 9, 2026, Gartner Says Worldwide Sovereign Cloud IaaS Spending Will Total $80 Billion in 2026, Retrieved from https://www.gartner.com/en/newsroom/press-releases/2026-02-09-gartner-says-worldwide-sovereign-cloud-iaas-spending-will-total-us-dollars-80-billion-in-2026.

28 European Union, (September 2023), Regulation (EU) 2023/1781 (Chips Act), Official Journal, Retrieved from https://eur-lex.europa.eu/eli/reg/2023/1781/oj.

A Widening Geopolitical Divide

The costs of sovereignty are not only economic. As Europe has moved toward greater technological autonomy, the policy divergence with Washington has widened. A State Department cable dated February 18, 2026 directed American diplomats to counter foreign data localization mandates, to track proposals promoting data sovereignty laws, and to promote an alternative multinational framework for cross-border data flows. The cable's stated concern was that such laws would disrupt global data flows, raise costs and cybersecurity risks, limit AI and cloud services, and expand government control in ways that can undermine civil liberties. Whatever the merits of that position, it puts American policy and European sovereignty ambitions on a potential collision course.

That collision reflects a deeper tension inside American strategy itself. Washington wants allies that are more self-sufficient: at the 2025 Hague Summit, NATO allies agreed to a defense spending target of 5 percent of GDP by 2035, with 1.5 percent dedicated to resilience, critical infrastructure, and defense.[29] At the same time, the current National Cyber Strategy commits the United States to securing American technology dominance. Both objectives can be true, and they can conflict — expanding Europe's autonomy in cyber defense serves the NATO objective and can, in some circumstances, work against sustained American technology dominance. This is sovereignty-as-primacy and sovereignty-as-autonomy colliding in practice.

The tension is unlikely to resolve on its own. Sanctions, export controls, and lawful process are permanent features of American authority, available to any administration and exercised as designed, and European officials therefore treat the exposure as structural rather than political. That is what makes the kill switch difficult for Europeans to dismiss. Relocation does not answer the risk for Europeans, and both sides lose in the attempt: Europe pays a premium for control it does not fully obtain, Washington forfeits allied adoption while asking those same allies to become more resilient, and both give up the shared threat visibility that makes defense work at scale. The more durable response is not to eliminate technological interdependence, but to make it more predictable, reciprocal, and trustworthy.

Fragmentation also creates a strategic opening for providers outside the existing transatlantic ecosystem. If the United States and Europe cannot offer a trusted, interoperable technology stack together, governments and companies may turn to suppliers that can offer a more complete alternative — even when doing so introduces different and potentially greater dependencies.

29 North Atlantic Treaty Organization, (n.d.), Defence Investment and NATO's 5% Commitment, Retrieved September 2026, from https://www.nato.int/en/what-we-do/introduction-to-nato/defence-expenditures-and-natos-5-commitment.

From Trusted to Trustworthy

Closing the divide requires moving from assumed trust to demonstrated trustworthiness. Washington can reduce the fear that drives decoupling by providing greater assurance of allied access, while Europe can strengthen its domestic capacity without treating domicile as a proxy for security. Companies on both sides of the Atlantic can compete on the capabilities that make sovereignty durable: control, transparency, portability, interoperability, and resilience. A trusted transatlantic technology ecosystem must ultimately rest on whether its infrastructure can demonstrate the properties that make it trustworthy — not simply on where that infrastructure or its provider is located.

Guarantee Allied Access

There is a way through the tension for Washington, and it runs through assurance rather than pressure. Europe wants greater control over the technology on which it depends, while American companies want continued access to the European market. A trusted transatlantic technology ecosystem can serve both interests — but only if European governments have confidence that access to critical American technology will remain predictable. If the United States wants allies that are both more resilient and connected to the American technology ecosystem, it must address the fear driving European efforts to pull away from it.

Guaranteed allied access should form the foundation of that ecosystem. This requires commitments within export-control and sanctions policy ensuring that allies in good standing will not lose access to critical American technology without notice, consultation, and recourse. The Department of Defense's Security of Supply Arrangements (SOSAs) offer a precedent: reciprocal commitments with allied governments designed to provide priority support for defense goods and services during periods of disruption. Those arrangements are nonbinding, and a credible framework for cloud, AI, and critical software would need to go further. But the underlying principle is transferable. Predictable access would slow European decoupling more effectively than pressure against sovereignty measures because it would address the underlying fear rather than its policy consequences.

A trusted technology ecosystem must also be reciprocal. Europe is not merely a market for American technology; it is a source of technologies on which American security and competitiveness also depend. ASML occupies an indispensable position in advanced semiconductor manufacturing. Nokia and Ericsson provided the trusted alternatives that made the U.S. campaign to remove Huawei and ZTE from allied 5G networks possible. Mistral and SAP represent important European capabilities in AI and enterprise software. These dependencies vary across the technology stack, but together they demonstrate that technological reliance runs in both directions. The United States and Europe each possess capabilities the other cannot easily replace.

The 5G experience offers a practical model. Washington's campaign to exclude Huawei and ZTE from allied 5G networks depended on European vendors as the trusted alternative: Secretary of State Pompeo named Ericsson and Nokia in urging European governments away from Chinese equipment, and American agencies extended loans to help developing

countries buy from them.[30] The United States relied on European suppliers to achieve a security objective it could not achieve through domestic industry alone. A similar approach to cloud, AI, software, and other strategic technologies would combine guaranteed allied access with reciprocal reliance, common security expectations, and support for trusted suppliers on both sides of the Atlantic. This would give Europe greater agency while preserving the scale and interoperability on which collective security depends. Trust takes time to build and can be lost quickly; it therefore must be reinforced through durable policy rather than political goodwill alone.

The Market for Sovereignty

European digital sovereignty is not only a defensive effort to reduce dependence; it is also a market-building project. European governments are trying to expand both the supply of homegrown technology and the demand required to sustain it. On the supply side, they are investing in companies, research laboratories, compute infrastructure, talent, and technical skills. On the demand side, they are using procurement, regulation, and public investment to encourage adoption across government and industry. Together, these efforts are intended to build capacity, strengthen strategic autonomy, and make European technology more competitive.

France's AI strategy illustrates this approach. In May 2024, the French government allocated €360 million to nine "artificial intelligence clusters," university-based centers of excellence in AI research and training, as part of a €560 million public package for AI research and training under France 2030, the national investment plan.[31] The clusters are tasked with significantly increasing the number of AI graduates at every level of qualification, attracting international talent, and building applied research capacity in fields including cybersecurity and health. One of them, SequoIA in Rennes, is dedicated to trustworthy AI for cybersecurity and defense, and demonstrates how investments in people and research can support sectors in which Europe already has relevant expertise. Companies and infrastructure can be financed relatively quickly; the talent and institutional capacity needed to sustain them takes longer to develop. Europe's ability to retain that talent and give researchers and engineers opportunities to build and scale companies at home will matter as much as its ability to train them. Building supply therefore requires consistent investment in skills as well as technology.

On the demand side, public procurement can provide European companies with anchor customers, while regulation and incentives encourage adoption across the private sector. Requirements rooted in regulation, security, and resilience, including the Digital Operational Resilience Act in financial services, health-data protections, and defense procurement, are likely to persist regardless of how the broader sovereignty debate evolves. Preferences based primarily on vendor domicile are more exposed to political change, trade negotiations, and shifts in procurement

30 Pompeo, Michael R, (December 2019), "Europe must put security first with 5G." Politico, Retrieved from https://www.politico.eu/article/europe-must-put-security-first-with-5g/.

31 Agence nationale de la recherche, (May 28, 2024), *Intelligence artificielle : 9 nouveaux « IA Clusters » et 2 nouveaux lauréats « Compétences et métiers d'avenir » soutenus par l'Etat au titre de France 2030,* Retrieved from https://anr.fr/fr/actus/details/news/intelligence-artificielle-9-nouveaux-ia-clusters-et-2-nouveaux-laureats-competences-et-metie/.

policy. The 15 to 30 percent premium Europe is already willing to pay for sovereign cloud services is evidence that the demand for greater control is real. The opportunity is to convert that willingness to pay into a durable market for capable and secure European technology, rather than a protected market sustained by nationality alone.

Closing markets to outside providers will not, on its own, create European champions. It can instead reduce competition, restrict access to leading capabilities, and produce a more isolated and fragile technology base. Europe's more durable opportunity is to build a market in which domestic firms can grow, customers can choose among providers, and common standards preserve security and interoperability across them. That requires capital, talent, sustained demand, and a regulatory environment that allows strong technology to reach the market. The objective is not self-sufficiency across every layer of the stack, but greater European capacity and control within a trusted transatlantic technology ecosystem.

Design Security In

The opportunity rests on something that should be true of any resilient technology base, wherever it is built: security and capability have to be designed in from the start, not added afterward. A homegrown alternative that is fragile or under-resourced does not deliver resilience because it is local. The better measure of progress is whether the technology base becomes more capable, secure, and resilient.

Sovereignty measures can involve a tradeoff between jurisdictional control and defensive visibility. The hyperscalers' security advantage lies in the scale of investment and breadth of visibility. A global provider sees attack patterns across millions of tenants and pushes defenses across its infrastructure within hours. A national sovereign cloud sees only its own traffic, defended by the personnel and systems available to it. Localization can therefore reduce jurisdictional exposure while increasing technical exposure. Sovereignty pursued through separation can also weaken the shared visibility on which collective cyber defense depends.

Digital networks do not end at national borders, and attackers do not organize their operations around them. Defenders need access to data across systems, providers, and jurisdictions to hunt threats, detect lateral movement, and understand how an adversary is moving through an environment. Penetration testing likewise depends on visibility across the systems and connections being tested; an assessment bounded by organizational or geographic divisions can miss the pathways an attacker would use. For global companies, restricting telemetry to individual jurisdictions can leave each defensive team with only part of the network while an attacker operates across the whole. Preserving that visibility does not require unrestricted transfers of customer data. It requires clear rules that distinguish the security telemetry defenders' need from the personal, proprietary, or sensitive data that sovereignty measures are intended to protect.

European measures carry costs of their own. Under the Technological Sovereignty Package, the Cloud and AI Development Act (CADA) proposes a tiered framework for public-sector cloud procurement in which the highest assurance levels would restrict international transfers of customer data, including telemetry and metadata, to keep it

within the European Union.[32] Security tooling depends on precisely the opposite: threat telemetry pooled across customers and jurisdictions, so that an attack pattern seen in one country becomes a defense deployed in another within hours. Confining European telemetry to Europe would leave European defenders working from a narrower picture of the threat than the adversaries they face – and it would do so as a matter of law.

The transition itself becomes an attack surface. Data migrations, identity re-architecture, and parallel-running systems create concentrated points of vulnerability, and Europe is preparing to run thousands of these transitions at once — most in the public sector, many under political deadlines. As a result, the years of greatest sovereignty enthusiasm may also be the years of greatest exposure.

The distinction to keep in mind is the difference between trusted infrastructure and trustworthy infrastructure. Trust is behavioral: a policy decision or judgment extended to a provider. Trustworthiness is an engineering property that can be specified, tested, and procured. Governments have already written versions of the criteria — France's SecNumCloud qualification and the United Kingdom's cloud security principles establish overlapping requirements that could form the basis of a broader transatlantic standards agenda. A sovereign offering earns the label of trustworthiness when it meets criteria like these:

Criterion	What Trustworthiness Requires
Key custody	Customer-held or externally held encryption keys the provider cannot access or surrender
Data in use	Confidential computing that protects workloads during processing, not only at rest and in transit
Supply chain transparency	Software bills of materials and provenance for the components beneath the service
Independent assurance	Audit rights exercised by parties the customer chooses, not attestations the provider selects
Security interoperability	Common formats and interfaces that allow authorized telemetry, threat intelligence, and defensive tools to operate across providers
Incident disclosure	A contractual duty to disclose breaches and government demands to the extent law allows
Exit and portability	Tested, guaranteed paths to move data and workloads out without penalty
Personnel jurisdiction	Clarity about which government can compel the people who operate the system

32 European Commission, (June 3, 2026), Proposal for a Regulation on harmonised rules for Cloud and Artificial Intelligence Development (Cloud and AI Development Act). Retrieved from https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada.

Europe has already legislated the principle. The Cyber Resilience Act (CRA) and NIS2 mandate secure-by-design engineering. Procurement has yet to catch up, often screening vendors on domicile without applying the same rigor to technical security. Applying common trustworthiness standards across providers would give Europe greater choice and control while preserving the interoperability and cross-border visibility required for effective defense.

Conclusion

Digital sovereignty is neither a passing trend nor a settled policy consensus. It reflects a measurable shift in how governments assess dependence, control, and risk. The evidence in this paper points to several findings. Full decoupling between the U.S. and European technology ecosystems is structurally constrained — the two remain too intertwined for separation to be feasible in the near term. Restriction-based approaches to sovereignty have not, on the evidence, produced more capable or more secure technology; they have, in some cases, increased technical exposure while reducing jurisdictional exposure. And the "sovereign" label, as currently applied across procurement and policy, frequently reflects domicile rather than trustworthiness — buying a flag rather than resilience.

The more durable frame is trustworthiness. Criteria for trustworthy infrastructure already exist — in France's SecNumCloud qualification, in the U.K.'s cloud security principles, in the requirements of the Cyber Resilience Act and NIS2. Sovereignty procurement that screens on nationality without applying those same standards risks substituting location for security. Common, evidence-based standards can preserve provider choice while ensuring that systems remain interoperable and defenders retain the cross-border visibility required for threat hunting, detecting lateral movement, and testing interconnected environments. The question should not be whether infrastructure is European or American, but whether the people who depend on it can verify how it behaves, who controls it, and what happens when something goes wrong.

A trusted transatlantic technology ecosystem offers a more durable path. Guaranteed allied access would address the fear driving European decoupling, while reciprocal reliance would recognize that both sides possess technologies the other needs. This requires Washington to respond through assurance rather than pressure and Europe to pursue greater capacity without closing itself off from trusted providers. Combined with common security standards, this approach would give Europe greater agency without sacrificing the scale, interoperability, and shared visibility on which both sides depend. Trust takes time to build and can be lost quickly; predictable access must therefore be reinforced through durable policy rather than political goodwill alone.

The distinction between domicile and security also creates a market. European demand is durable where it is rooted in regulation, resilience, and genuine requirements for control. But building domiciled alternatives is costly, particularly when it requires reproducing capabilities already delivered at scale by global providers.

Customer-held key custody, confidential computing, portability, independent assurance, supply-chain transparency, and cross-border security tooling offer another path. The opportunity is not simply to build European substitutes for American technology, but to give European customers meaningful control without sacrificing the scale, interoperability, and security on which they also depend.

The renegotiation of technological dependence is underway, and its terms are still being set. Washington can shape those terms through guaranteed allied access. European institutions can anchor them in trustworthiness rather than nationality. Companies on both sides of the Atlantic can build the capabilities that make greater European control compatible with collective security. The objective is not technological independence, but a more balanced and resilient form of interdependence — one capable of sustaining a trusted transatlantic technology ecosystem over the decade ahead.