DECEMBER 2025

The Sovereign Cloud-Sovereign AI Conundrum

Policy Actions to Achieve Prosperity and Security

AUTHOR

Bill Whyman

A Report of CSIS Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

DECEMBER 2025

The Sovereign Cloud-Sovereign AI Conundrum

Policy Actions to Achieve Prosperity and Security

AUTHOR
Bill Whyman

A Report of CSIS Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values–nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decision making of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

The author would like to thank CSIS, especially Matt Pearl and the Strategic Technologies Program, for supporting cutting edge research. CSIS's new Economic Security and Technology Department integrates the many dimensions of complex policy issues that often remain in silos. Thank you to the many who contributed to this report, including cloud users, industry operators, policy experts, and academic scholars. They helped bring out important ideas well beyond current debates.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

Contents

Executive Summary

Rising geopolitical competition and the power of artificial intelligence (AI) are driving governments around the world to establish greater control over cloud computing. The growth of cloud has made it the backbone of modern economies, integral to the provision of public services, and the foundation of advanced technologies such as AI. U.S. cloud providers–led by Amazon, Google, Microsoft, and Oracle–provide 75 percent of global cloud services.[1] Countries are reassessing their dependencies on the United States and hence on U.S. cloud providers, and pursuing independent "sovereign clouds" and "sovereign AI" supported by local providers. This is part of a broader push for digital sovereignty by other countries to more fully control their economies and security.

More and more, countries around the world are requiring restrictive sovereign cloud controls that go well beyond strong security, data sovereignty, and building local datacenter infrastructure that have been the focus of the past five-plus years. Some governments are now insisting on full operational control by their citizens and full governance control, with local source code repositories and, in some cases, majority local (non-U.S.) ownership. Governments want to ensure they can assume full control of cloud infrastructure in case disruption halts cloud operations in their country or denies them access to cloud infrastructure. Recent sanctions on Russia and China and the rise of the Trump administration's "America First" policy are also fueling international concerns about how potential U.S. sanctions could disrupt their access to U.S. cloud provider services.[2] This is leading countries to embrace sovereign cloud initiatives that establish not only data sovereignty but sovereignty over the whole IT stack, including datacenters, networks, storage, AI models, operations, and governance. Further, the potential transformative capability of AI is heightening government desires to capture its benefits and avoid being harmed or relegated to dependent players. This is driving governments' push for more restrictive sovereign cloud controls and sovereign AI initiatives. Calls for a “EuroStack”—a full IT cloud and AI infrastructure owned and fully controlled by European entities that is independent of the United States—is the most recent example.[3]

Governments have legitimate political, economic, and security interests in regulating cloud computing. Yet how do they achieve their goals? Do they pursue them with allies and partners who hold shared values and interests in ways that increase prosperity and security, or by building walls and excluding others with restrictive policies that reduce prosperity and security. If nationalistic sovereign clouds become isolated “splinter clouds,” it accelerates fragmentation, brings huge economic costs, and works against the open, rules-based global technology system. Fractures in the global cloud are already visible. China, Russia, Iran, and North Korea have formed an authoritarian axis; Europe has its own vision and is charting an independent course; Brazil and India champion the “Global South.” Further, the allure of sovereign AI is boosting interest in sovereign cloud. Yet, sovereign cloud is not required for sovereign AI. National AI models and datasets can be built, deployed, and secured using most modern IT infrastructure.

Sovereign clouds may offer greater control, but they do not provide greater technical security. Yet sovereign controls bring higher costs, slower growth, and less innovation—making the economies of countries that use them less competitive. Governments can achieve most of their security goals in traditional commercial cloud regions via technology, operational controls, and legal/compliance regimes. Sovereign cloud brings additional visibility, access, and political control—and thus, trust—even though the underlying technical security is the same. (See the definition of sovereign cloud in the next section.) But at what cost? A European think tank study showed discriminatory sovereign cloud rules in the draft European security certification scheme (EUCS) would lead to annual losses of €29 to €610 billion within two years, depending on how broadly they are applied.[4] Proponents of a Euro-IT stack have proposed an initial €300 billion investment. Given the huge costs, have governments explicitly defined their risks, the likelihood of such risks, and how they can be mitigated before jumping to restrictive sovereign clouds? What additional steps can cloud providers take to enhance trust by demonstrating security, transparency, and sovereign control? How can governments provide strong legal protections for access to user data, minimizing the need for sovereign restrictions? Further, how broadly will sovereign clouds reach: to sensitive government functions only, or broad public services? Or will they extend to even privately-owned public services in communications, healthcare, banking, and energy? Government expenditures are large (e.g., 40-60 percent of GDP in Europe), so sovereign clouds risk splintering the cloud market.[5] Decades of experience show that sovereign infrastructure has a poor track record of success and often becomes stranded investment, burdening economies. This has already happened with an early version of Cloud Deutschland and Europe’s Gaia-X cloud project.[6] Even if well-intentioned, restrictive sovereign clouds may simply not achieve their goals, are likely unsustainable, and will require continued investments.

These are not hypothetical risks. Cloud providers are listening to their government customers and providing a continuum of sovereign cloud solutions. Amazon, Google, IBM, Microsoft, and Oracle all have sovereign cloud solutions, ranging from local private clouds that can be installed in government datacenters to software-controlled sovereign clouds running on top of public cloud infrastructure to physically and logically isolated sovereign regions. These are not small initiatives; for example, Amazon’s European Sovereign Cloud is planned to cost €7.8 billion.[7] Nvidia is also urging countries to build their own sovereign AI infrastructure, which is on track to provide it $20 billion in revenue this fiscal year.[8] IDC estimates the sovereign cloud market will exceed $250 billion in 2027.[9]

Rising geopolitical competition, digital sovereignty, and the allure of AI suggest that sovereign cloud and sovereign AI will gain greater adoption. This paper proposes ten recommendations to focus sovereign cloud on achieving government priorities, minimizing costs, and building greater prosperity and security among democratic, rule-of-law nations. The following are brief summaries of the recommendations, and the conclusion of this report provides more specifics.

1. **Avoid burdening purely commercial activities** with the cost and innovation penalty of sovereign cloud.
2. **Use sovereign clouds for government services where they are appropriate** to the threat and where the political and economic benefits outweigh the costs. Governments should fully use security tools before jumping to sovereign clouds.
3. **Take a risk-based approach** that classifies government applications and data into risk-based tiers, quantifies the likelihood of risks, and identifies priority risks to mitigate.
4. **Build trust** by enhancing cloud transparency and joint industry-government confidence-building measures that test security controls and resiliency commitments. Convene a G7 and Organisation for Economic Co-operation and Development (OECD) group with industry to develop trustworthy cloud criteria. Create a sovereign cloud training academy and skill certification.
5. **Mitigate risk of disruption of the cloud by sanctions or "kill switch" risks by strengthening resiliency and workload portability** via architectural requirements, tools, and open-source software. Avoid restrictive national clouds except where absolutely necessary and as part of an overall risk management strategy.
6. **Partner with cloud providers** to achieve sovereign goals, so governments can avoid spending billions of dollars replicating largely undifferentiated IT infrastructure. Focus national economic development initiatives on higher-level services and workforce training that better drive growth and promote national priorities.
7. **Focus sovereign AI on building national AI models and datasets** that reflect a nation's distinct heritage rather than lower-level IT that does not. Sovereign cloud infrastructure is not required for sovereign AI.
8. **Avoid country-ownership-based cloud requirements** that erect trade, investment, and political barriers to partners and splinter the cloud. Use transparent, functional requirements instead.
9. **The U.S. government and U.S. cloud providers need to show other countries that their economic development goals are better achieved in partnership** with the United States, rather than by exclusion.
10. **Accelerate government-to-government negotiations** to address underlying political and policy concerns that give rise to sovereign clouds, especially data sovereignty and economic sanctions.

What Is Sovereign Cloud?

There is no common definition of sovereign cloud, and different countries and government departments define it differently. However, the core idea of sovereign cloud is to achieve greater transparency, control, and trust of cloud computing, so that governments are assured of security, availability of services, resiliency in cases of disruption, geographic residency and control of data at all times, and confidence that bad actors or the cloud operator does not have access to their data. There is a spectrum of approaches, as each country has different goals and requires different controls for different uses.

Table 1: Defining a "Sovereign Cloud"

Sovereign Cloud Design Goals	Sovereign Cloud Controls
1. Data sovereignty— control over data and data access	▪ Granular control over geographic residency and access to data ▪ Data controls include metadata (e.g., roles and permissions, configurations, and resource tags) ▪ Secure chip enclave to limit access by cloud operators/bad actors ▪ Data encrypted at rest, in transit, and (in some cases) in memory ▪ Users can hold encryption keys outside of the cloud or via partners

2. Physical sovereignty— separation of datacenters and servers	▪ Datacenters are physically separated from commercial datacenter regions and geographically located in-country ▪ Data, storage, and servers are in a separate sovereign jurisdiction ▪ Networks are isolated with granular controls and monitoring
3. Software sovereignty— logical separation of software and systems	▪ Systems and software are logically isolated and separated from commercial systems (separate partition and separate control plane) ▪ Potential use of open source to reduce dependency on providers
4. Operational sovereignty— independent operational controls	▪ Separate identity and access management (IAM) credential system ▪ Operational support by vetted local residents/citizens ▪ Customer service and 24/7 technical support provided by local residents/citizens, who are employees and located in-country ▪ Separate billing and metering system specific to sovereign cloud ▪ Local source code repository and continuity plan with local providers
5. Enforceability, verification, compliance, and resiliency	▪ Application programming interface (API) calls monitored and logged for transparency, verification, and compliance, including administrative access by cloud providers ▪ Detection and prevention of change from approved configuration templates ▪ Compliance with multiple security and compliance regimes ▪ Resiliency via multiple geographically distant datacenters and data backups, with separate power and telecommunications
6. Independent governance and ownership	▪ Separate local corporate entity in country, bound by local laws ▪ Separate governing board with local citizens and local fiduciary ▪ Legal commitments enforced by binding contracts ▪ Potential restrictions on foreign financial ownership of the cloud

Source: Author’s analysis

The controls in Table 1 (right column) represent the array of sovereign goals (left column) countries seek when they build sovereign clouds. Nearly all of the controls are offered by U.S. hyperscale sovereign cloud solutions and are custom designed to meet sovereign requirements while preserving the innovation of commercial clouds. However, requiring majority local (non-U.S.) ownership and separate national or regional clouds provided by national champions that are immune from the laws of others are what the author calls “restrictive” or “autarkic” clouds that break the backbone of the global public cloud and its many benefits.

Sovereign clouds have essentially the same technical security as commercial cloud regions. Other work has shown that cloud computing gives governments the tools they need to achieve technical security.[10] However, for sensitive workloads, some governments want enhanced transparency, access, and controls that provide additional confidence and trust (e.g., more granular controls to enforce data and metadata residency, operations and customer support by local citizens, separate identity and access controls, and extra monitoring to prove compliance). France goes even further, requiring majority local ownership of clouds handling sensitive data as a precondition of service. Cloud regions for classified data and defense and intelligence purposes are also a type of sovereign cloud for the most sensitive uses, but this paper does not explicitly address them since they are often “air-gapped” and present separate issues. These “classified clouds” are best pursued with allies that have close relations or security treaties that establish a broader political alignment and baseline level of trust.

Government concerns are growing about disruption of the cloud—and even being cut-off from it—leading to expanding sovereign cloud requirements. Initial focus on data sovereignty led cloud providers to build hundreds of local datacenter regions around the world. This expanded to networking, software, security, and the logical end-to-end systems to provide greater transparency and control. In turn, countries focused on operational sovereignty and the people and processes that run the cloud. In 2025, rising geopolitical competition is leading to new rules for full operational and governance control, in case access to U.S.-controlled cloud infrastructure is potentially cut off or disrupted. In Europe, many are calling for an independent sovereign EU cloud—such as the EuroStack proposal put forth in January and March 2025—to reduce dependencies on the United States.[11]

- Shortly after the EuroStack proposal, on April 30, 2025, Microsoft President Brad Smith launched new “European digital commitments,” including an EU corporate entity for Microsoft’s EU datacenter operations, with an all-European board of directors, under EU law, on top of its many decade-long EU cloud commitments. Microsoft will implement “digital resilience” plans that include saving the source code in Switzerland, setting up continuity agreements with local EU cloud providers, and implementing binding contracts. Microsoft explicitly commits: “In the unlikely event we are ever ordered by any government anywhere in the world to suspend or cease cloud operations in Europe, we are committing that Microsoft will promptly and vigorously contest such a measure using all legal avenues available . . . (and) by including a new European Digital Resilience Commitment in all of our contracts.”[12]
- On May 21, 2025, Google updated its sovereign cloud solutions, including an air-gapped distributed cloud solution (without connectivity to an external network) with open-source software that can be operated by local partners in the event that there is no access to the global public cloud.[13]

- On June 3, 2025, Amazon announced a new EU governance structure and controls for its €7.8 billion AWS European Sovereign Cloud. It "will have no critical dependencies on non-EU infrastructure" and there will be "zero operational control outside of EU" borders.[14] Amazon is creating a new corporation in Germany, led by EU citizens, that is bound by EU rules. The new corporation has an independent governance structure, a dedicated EU security operations center, and a local EU replica of the source code.

These latest actions on governance and control—even after years of expanding commitments and tens of billions of dollars in investment—suggest that U.S. cloud providers see a risk that governments could create their own restrictive sovereign clouds that exclude the United States and U.S. companies.

The Forces Driving Sovereign Cloud

The issues of sovereignty and political control are governments' core concerns. At first, governments around the world were pushing back on U.S. Big Tech companies' business practices. Many believe that these companies set most of the tech policy rules in the Internet 1.0 period.[15] Though many of these issues (e.g., social media) concern individual consumers and are substantively different than the issues surrounding enterprise cloud computing, they fed government desires for greater political control to align IT with their goals, avoid dependency, and independently set the rules that govern technology in their countries. These high-level goals are appropriate in a world of sovereign states. Yet, the devil is in the details, and digital sovereignty can be a double-edged sword. It can be used to unfairly block foreign market access, surveil and suppress political opponents, and censor information.

The U.S. shift to an America First policy has added to growing sovereign cloud momentum by increasing the perceived risk of countries being cut off from U.S. cloud providers' infrastructure around the world. Recent national security sanctions against Russia and China have illustrated how countries can be cut off from the global economy and infrastructure. This is leading governments to go beyond jurisdictional control to achieve full operational control of the cloud to ensure that they are not denied access to cloud services, either by hostile actors or by sanctions. In 2018, insurer Lloyd's of London found that a hypothetical cyber incident in which a top cloud provider was taken offline in the United States for three to six days would create losses of $6.9-$14.7 billion.[16] The potential loss has since grown much larger, showing the unacceptable costs of losing access to the cloud.

Countries are reassessing their dependencies on the United States, though they are still reliant on U.S. clouds. Northern European countries (Denmark, Germany, and the Netherlands) that are more free-market oriented have traditionally supported the United States and have limited restrictive EU cloud rules, yet even they have now become more favorable to restrictive EU sovereign approaches.[17] The suspension of a Microsoft email account in Brussels in response to a U.S. executive order sanctioning the prosecutor of the International Criminal Court in May 2025 was a political shock in Europe. Though the issues are not new, this incident illustrated fears that the United States could shut off the cloud in Europe.[18] Bitkom, Germany's "digital economy" association of 2,200 companies, has issued a formal call for a German cloud, showing "62 percent of companies in Germany would stagnate without cloud services . . . 78 percent believe Germany is too dependent on US cloud providers, and 82 percent want . . . hyperscalers from Germany or Europe . . . . Furthermore, [the] 50 percent that use cloud computing feel compelled to rethink [their] own cloud strategy due to the policies of the new US administration."[19] The Dutch parliament has passed motions to build the Netherlands its own national cloud and is pushing the European Union to move from U.S. clouds to European providers.[20]

Many governments are responding to the risk of losing access to cloud services by building more controls around sovereign clouds inside their borders. Yet the best example of a response to a loss of cloud services is Ukraine ending its data localization rules and moving the bulk of its government IT outside its borders in the wake of Russia's invasion. In 2022, ten petabytes (PB) of data from 42 Ukraine government authorities, 24 universities, and dozens of private companies were migrated to the cloud outside of Ukraine.[21] Ukraine's PrivatBank, which serves 40 percent of the country's population, moved all of its operations to the cloud, including 270 applications and 4 PB of client data.[22] Similarly, Estonia and Monaco have built a "data embassy" backup in Luxembourg. Luxembourg and Bahrain have created legal and physical infrastructure to host data embassies. These cases represent the opposite of data localization, as countries move data outside their borders but retain full legal control.

The earlier push for data sovereignty is expanding to sovereign control over the entire IT stack–in the form of the sovereign cloud. Data sovereignty, data privacy, and the free flow of data are long-standing issues that have been addressed in multilateral government fora such as the OECD, the World Trade Organization, the G7, the Asia-Pacific Economic Cooperation (APEC), and others. In particular, the United States and Europe have been challenged to achieve predictable rules for data flows in the wake of the EU General Data Protection Regulation (GDPR) and the Schrems lawsuits. The European Union (and other countries) are concerned about potential U.S. government access to EU data held outside the United States via the cloud. The US Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018 was in part intended to provide more clarity, protect data, and resolve conflicts of law related to requests for electronic data for public safety. Further, the U.S. Department of Justice formally stated that its policy is to first make data requests directly to the affected parties or customer, not to the cloud provider. The cloud providers disclose government data requests; for example, Amazon says there are no "requests [that] resulted in the disclosure to the U.S. government of enterprise or government content data located outside the United States."[23] However, this has proven insufficient, and U.S.-EU efforts to negotiate a separate bilateral agreement have not yet materialized. Other experts have delved into these complex data sovereignty issues, and this paper will not replicate that work.[24] Yet it should be emphasized that sovereign cloud expands the focus from just data sovereignty to sovereignty over the full IT stack, including the AI stack.

Economic development and economic nationalism are also driving sovereign cloud. . . .Cloud is integral to a country's growth and economic competitiveness.

Economic development and economic nationalism are also driving sovereign cloud. States set the rules to distribute wealth to their companies and treasuries and to generate local jobs and income. A strong economy and technical leadership are sources of national power. Cloud computing is rightly seen as a foundational technology. Cloud is integral to a country's growth and economic competitiveness. Yet given the huge economies of scale and the billions of dollars needed to build and maintain a full cloud region, it is not economically viable to have national cloud computing champions. Nonetheless, countries are seeking to build their own cloud industries. The U.S. Trade Representative (USTR) identifies discriminatory trade concerns against U.S. cloud providers in 15 countries, plus the European Union—amounting to roughly 45 percent of global GDP (nearly 60 percent with the European Union included)—in its 2025 National Trade Estimate (NTE) of trade barriers.[25] China has blocked foreign cloud providers and requires them to license their technology to Chinese-owned joint ventures. Europe has several cloud providers (e.g., Deutsche Telecom, Hetzner, Orange, Outscale, OVHcloud, and Scaleway) that are much smaller, with more limited services. The European Union created its Gaia-X project to build a European cloud industry and is spending over €1.2 billion on its next generation cloud, boosted by additional member-state spending.[26]

French policies that prevent foreign cloud providers from managing sensitive data as a precondition for providing service are likely a discriminatory violation of French trade agreements. The 2025 NTE and the prior Biden administration NTE called this out, stating that French "government agencies and commercial entities considered 'critical' must select only cloud services vendors with a SecNumCloud certification to handle their highly sensitive data."[27] This certification "requires that any cloud provider . . . must be at least 61 percent EU-owned and 'immune' from non-EU laws."[28] Google (S3ns with Thales) and Microsoft (Bleu with Cap Gemini and Orange) have been forced to license their technologies to French-owned joint ventures to meet these rules. Efforts to make the rules apply across Europe via the EUCS cybersecurity certification scheme have been stopped, but these provisions may resurface in areas such as government procurement.[29] In the new era of tariffs, these practices are unlikely to be challenged, but they show how even advanced market economies and democratic allies are pursuing restrictive policies that block foreign providers.

The EuroStack project seeks to go well beyond these efforts and create a sovereign EU IT stack that is fully independent from the United States and that encompasses semiconductors, software, cloud computing, quantum, networking, and even applications. The German Bertelsmann Foundation describes the EuroStack project goals: "Beyond reducing technological dependence, the initiative seeks to boost industry competitiveness, drive innovation, [and] build resilient sovereign infrastructures."[30] Over 250 companies in Europe have signed a letter to the president of the European Union calling for deployment of the EuroStack by 2030. While likely not a realistic alternative to U.S. clouds, the initiative shows how many leading actors in Europe are aggressively pursuing sovereign IT.

Sovereign cloud has political appeal; yet it may not end up achieving its goals. It imposes costs on growth and innovation to achieve goals that may be better achieved in other ways. The goal of immunity from the laws of others directly contradicts and is incompatible with the basic economics of trade. Sovereign cloud may help insulate countries from risk, but there is no way for states to be fully independent.

AI Is Leading to More Regulation of the Cloud

The power and potential transformative capability of AI—especially generative AI—is heightening governments' push for more control over the cloud. AI has increased governments' concerns about being left out of its benefits, exposed to its potential harms, or relegated to dependent players. Most generative AI systems physically reside in the cloud, so AI regulation often means more cloud regulation. AI's large potential impact is raising the stakes and increasing interest in sovereign cloud.

Governments want to benefit from AI-driven economic growth and productivity. Much has been written about the potential transformative benefits of AI in content creation, workforce productivity, new drug discovery, software development, and many other areas. Governments rightly see AI as central to their economic vitality and future. AI is a general-purpose technology, and governments are seeking broad public access and diffusion across the economy to drive productivity. How much economic benefit AI will create is an active debate. A recent McKinsey study found that "Generative AI could add the equivalent of $2.6 trillion to $4.4 trillion annually" in value and "enable labor productivity growth of 0.1 to 0.6 percent annually through 2040."[31] However, others including Massachusetts Institute of Technology economist and Nobel laureate Daron Acemoglu are more cautious.[32]

Governments are rightly concerned about national security and the risks of harm from AI. Nearly all countries are debating the benefits and risks of AI in economics (e.g., employment disruption, innovation, growth, antitrust, and copyright), social and culture issues (e.g., biases and inaccuracy of AI models; privacy; and discrimination in housing, finance, and insurance), energy (e.g., availability, sustainability and cost), politics (e.g., elections, disinformation, and surveillance), and security issues (e.g., cybersecurity and autonomous weapons). These risks, potentially including existential risk to humanity, give governments a strong interest in regulating AI.

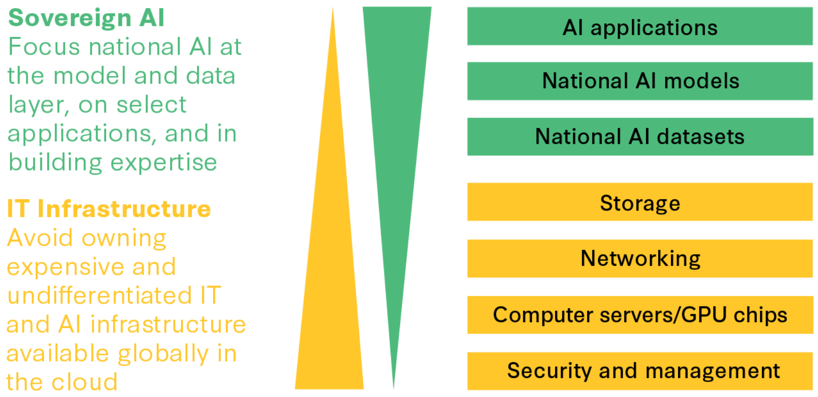
Governments want their sovereign voice in AI development and governance. Technology drives national power, and AI will likely change the balance of power among countries. Governments do not want to be relegated to being dependent players. AI has big potential impacts across economics, politics, culture, and security, and countries want a say in how it is developed. AI expertise is concentrated in the United States and China. Countries that lack AI expertise and infrastructure do not want to be forced to accept what others decide, or left out of AI governance discussions. AI is especially dependent on big volumes of data, so countries do not want to only provide data to models that are controlled by others. Saudi Arabia and Abu Dhabi, for instance, are using their wealth to acquire AI capabilities and get a seat at the table. Abu Dhabi's state-backed G42 AI company struck a deal with Microsoft, and then came under pressure from the United States to limit flows of AI to China if it wanted access to cutting-edge U.S. AI.[33]

Regulation of AI often leads to regulation of the cloud in which AI is trained and deployed. For example, the U.S. 2023 AI executive order (now repealed) "require[s] United States IaaS [cloud] Providers to submit a report to the Secretary of Commerce when a foreign person transacts with that United States IaaS Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity."[34] AI models make big demands on IT infrastructure, and especially on AI accelerator chips, or graphics processing units (GPUs). AI is driving a "re-architecture" of over $1 trillion of cloud datacenters, including storage, networking, and power and cooling. In 2024, the big five U.S. cloud providers invested $265 billion to achieve this with another $435 billion underway in 2025.[35] Few beyond the cloud providers have the expertise and resources to build AI infrastructure at scale. And the scale and shared capacity of the cloud mean that it has higher (more profitable) economic utilization. Further, many organizations' data and IT are already in the cloud, and AI applications will need to integrate with these core systems. As a result, the majority of modern AI systems will likely live in the cloud. The large potential impact of AI is driving regulation that will also apply to the cloud, and it is boosting interest in a sovereign cloud with strict controls.

The Allure of Sovereign AI Is Accelerating the Rise of Sovereign Cloud

The surge of excitement about AI has given rise to the idea that countries should have their own sovereign AI. There is no common definition of this term, but in general, sovereign AI is the broad notion that countries should have their own AI capabilities that they control. Sovereign AI initiatives often aim to reduce dependency on foreign cloud providers, promote domestic champions, expand domestic AI infrastructure, and ensure the availability of AI models that reflect local values. Sovereign AI is also motivated by national pride. These are similar to the reasons governments are pushing for sovereign clouds. Sovereign AI is also being promoted by leading AI semiconductor company Nvidia. Nvidia defines sovereign AI broadly as "a nation's capabilities to produce artificial intelligence using its own infrastructure, data, workforce and business networks."[36] Yet AI systems dedicated to sovereign AI are expensive and difficult to sustain. Nvidia is helping countries build their own AI datacenters. The company expects more than $20 billion in sovereign AI revenue this fiscal year, and has announced deals with Denmark, Japan, Singapore, India, and Switzerland, among others.[37]

Figure 1: Choose Sovereign AI at the Right Layers of the Stack


Sovereign AI
Focus national AI at the model and data layer, on select applications, and in building expertise
IT Infrastructure
Avoid owning expensive and undifferentiated IT and AI infrastructure available globally in the cloud
AI applications
National AI models
National AI datasets
Storage
Networking
Computer servers/GPU chips
Security and management

Source: Author's analysis.

Sovereign AI is a top priority, but it does not need to be tied to or require a sovereign cloud. Some governments that want sovereign AI also want to build their own sovereign clouds to train and deploy AI. However, governments can build their own national AI models, data sets, and AI expertise without spending billions of dollars to build their own sovereign cloud infrastructure. Model training and model data are the heart of sovereign AI, and they represent separate parts, or layers, of the cloud (see Figure 1). In slightly more technical terms, countries have a choice as to what layer of the tech stack they want to implement sovereign AI, as well as what layers are affordable and feasible. Countries can create their own national AI models and datasets in a commercial cloud and still control them. From a technical view, they can use strong cloud security and governance to protect their AI assets. National AI models can be trained and deployed in any location, in the cloud or on premises, without creating a sovereign cloud. For countries with the economic and technical resources to sustain AI investments, dedicated sovereign AI infrastructure may be helpful. Similarly, for those countries that lack access to AI infrastructure, sovereign AI may be appropriate. Yet, for most countries, so long as modern IT infrastructure is available, governments can focus on building their unique AI, rather than spending on costly infrastructure which is similar around the world. Simply put, sovereign AI may be built in the cloud, but it does not require a sovereign cloud.

Perhaps the strongest argument for sovereign AI is that AI models, and especially large language models, reflect the cultural and social views of their builders. Today, leading models are mostly built in the United States, China, and a few other countries including Canada, France, Germany, and the United Kingdom. AI models are heavily dependent on the data used to train them and the architectural choices made by their builders. U.S. and Western cultural and social views are often embedded in large models, especially via data from the public internet on which models are trained. Those values do not always fit easily with the culture and social values of other countries. Countries may want their own national AI, but this does not require them to build and own their own sovereign cloud infrastructure. There are widely available tools to steer model outputs, fine-tune them using a nation's own data, and provide instructions that align models to local concerns about safety, gender, racism, politics, and other goals. This is not perfect, but it is a much less expensive way to build sovereign AI than spending billions of dollars on rapidly depreciating IT infrastructure.

Countries are building national models that reflect their culture, language, and identity. Sovereign models can (and have) been trained and deployed in the cloud and do not require a sovereign cloud. Many of these are open source and are alternatives to models developed in the United States and China. A few examples are as follows:

- Singapore's SEA-LION model states that its "open-source Large Language Models . . . better understand Southeast Asia's diverse contexts, languages, and cultures."[38] This model was launched with just a $52 million budget.[39]
- The Falcon models are created by the United Arab Emirates' government-supervised Technology Innovation Institute in Abu Dhabi.[40] The Jais model focuses on Arabic languages.
- Saudi Arabia's Data and AI Authority Arabic large language model (ALLaM) claims that most "frontier-class models are primarily trained on English and often lack a connection to localized regional cultures and norms."[41]
- Taiwan's Trusted AI Dialogue Engine (TAIDE) model is backed by the country's National Science and Technology Council. TAIDE "aims to ground itself in Taiwanese culture, incorporating unique linguistic elements, values, and customs."[42]

Some governments want their own national AI to surveil their population, control political dissent, enable disinformation campaigns, and enforce their approved version of the truth. For example, Chinese government policy says generative AI models must "uphold the core socialist values" and be approved by the government in advance.[43] Companies must answer 20,000-70,000 set questions to test whether the models produce answers the Chinese government deems safe.[44] AI models, including Chinese company DeepSeek AI's model or Baidu's Ernie, will not answer questions that threaten Chinese Communist Party interests, acknowledge the Tiananmen Square uprising, or address the independence of Taiwan.[45] Some authoritarian states have interests in using generative AI to influence elections and create disinformation campaigns with their approved truths. If societies increasingly get their information through AI assistants, these then become powerful levers for censorship and control. Reportedly, one reason Taiwan created its TAIDE model was to build an alternative to bots controlled by the People's Republic of China (PRC) and prevent dependence on PRC AI-generated information.

The Challenges of Sovereign Cloud:

Higher Costs, Fewer Services, and Less Innovation

Sovereign cloud requires governments to make policy choices. Governments are moving ahead with sovereign cloud deployments, and cloud companies are already providing sovereign cloud solutions. According to IDC, half of global organizations are either using or planning to use sovereign cloud solutions.[46] All the major U.S. cloud providers and Nvidia have announced large sovereign cloud deals. Yet sovereign clouds may not be the preferred choice for many cloud providers. They are often smaller, semi-custom infrastructure that is more costly to build and operate. This breaks cloud providers' scale and operational rhythm across hundreds of datacenters around the globe. Nonetheless, providers are hearing their government customers and are providing a range of sovereign options. Each of these variants have different architectural choices (and policy implications) with their own pros and cons.

Sovereign cloud requires policy choices prioritizing control, cost, complexity, number of services, and ease of innovation. This author's previous work has shown that cloud computing is central to a nation's economic competitiveness.[47] Sovereign clouds come with difficult trade-offs, often favoring greater control at the expense of other national goals.

- **Sovereign clouds have higher cost**. Sovereign cloud infrastructure is usually smaller than major commercial cloud infrastructure and has smaller economies of scale. Sovereign clouds are also more costly and complicated to operate. The Singapore government has a smaller sovereign cloud (dedicated local zone) that it says is two-and-a-half times more expensive than its commercial cloud.[48] Even Amazon Web Service's large U.S. "Gov Cloud" (two regions, roughly six availability zones, many datacenters), which has operated since 2011, is typically at least 20 percent more expensive than commercial cloud regions.

- **Sovereign clouds provide fewer services, less choice, delayed access to new services.** Most cloud providers deploy new services to their largest markets first. Leading clouds have 200-plus service groupings. The core services are deployed everywhere, but specialized or newer services may initially (or only) be deployed in regions that have the scale to economically justify them. The much smaller Singapore sovereign cloud initially launched with only about 20 major services, though more are being added. Even in commercial clouds it can take years for smaller regions to receive new services. Missing the latest services limits what developers can build and undercuts innovation. One cloud provider advises that "while most . . . services are available in [a sovereign region], there are often limitations, missing features, and restrictions."[49] Politics may lead to faster deployment for sovereign clouds, but smaller sovereign regions are fighting economics.
- **Hard operational boundaries between commercial and sovereign regions make sovereign clouds more complex.** Workloads that span sovereign clouds and commercial regions are more complicated to operate. Sovereign clouds can have over 250 additional separate controls to manage. As one cloud provider advises: "We recommend deploying workloads that require multiple Regions to be kept within a single partition [commercial or sovereign] to reduce compliance, operational, and technical challenges."[50] This is a burden on government users. Sovereign clouds may also be less resilient because they are geographically concentrated and more vulnerable to disruption.
- **Sovereign clouds mean less innovation and less growth.** Most importantly, many sovereign clouds lack the deep, liquid pools of computational resources that support innovation and scalability. This is especially true for advanced services. The GPU chip shortage for AI workloads, for instance, is a bigger problem for smaller cloud regions.

  Additionally, sovereign clouds undercut the democratizing access of cutting-edge capabilities from startups to enterprise. Anyone can spin up a lawful cloud compute cluster. It makes the messy trial-and-error of innovation quicker and less expensive. OpenAI had only about 500 employees when ChatGPT 3.5 surprised the world, but it had access to Microsoft's Azure AI cloud. Boom, another startup, used the cloud to design a supersonic commercial airliner from scratch.[51] Aerospace is a challenge for startups due to barriers of scale and regulation, yet Boom tested hundreds of designs with thousands of flight simulations, using 53 million core hours in the cloud.

  Finally, sovereign clouds fragment the robust ecosystems that drive innovation. There are 100,000 partners in the cloud that can easily share data and apps from cloud marketplaces that have 2.5 million subscribers. Cloud users need their many partner companies to be in their cloud to provide full solutions. A separate, sovereign cloud optimized for control and compliance is more expensive for partners, especially smaller ones, and is unlikely to be a nexus of innovation.

Some European commercial organizations have openly opposed restrictive EU sovereign cloud requirements because of these limitations of higher cost, fewer services, and less innovation. In just one example, the German automotive industry association VDA has publicly stated that the "stringent sovereignty requirements imposed on cloud operators [via EUCS] could potentially restrict the use of leading solutions from major US hyperscalers. Since European alternatives currently do not meet the requirements of the German automotive industry, this would lead to a massive limitation in both the range and the availability of cloud services. . . . Differences in implementation by member states would result in significant efficiency losses in typically cross-border business processes."[52] VDA added: "Today's highly competitive market would be artificially restricted, which would be hugely detrimental to the range of services offered and represent a retrograde step in digitization."[53] Requiring private companies to use a sovereign cloud typically puts them at a competitive disadvantage relative to their global peers.

The government of Singapore's approach to sovereign cloud offers a promising example. They explicitly evaluated the trade-offs of different cloud infrastructure solutions in terms of cost, scalability, agility, resiliency, security, innovation, and transparency.[54] They also defined the risk and sensitivity of their workloads and data. This enabled the government to assign workloads to different levels of sovereign control to achieve security goals while limiting the costs to economic growth and innovation. Public-facing, lower-risk government workloads run in the commercial cloud, and their share of total government workloads is growing. A minority share of sensitive applications run in a hyperscale cloud provider's "local zone" that geographically resides in Singapore and is dedicated solely to the government of Singapore's use.

Policy Recommendations to Achieve Both Prosperity and Security

Digital sovereignty centers on maximizing national control and standalone independence. It seeks to reduce potential vulnerabilities through limiting interdependence with others, often by creating barriers to outside forces. In contrast, the public cloud offers an open, rules-based technology ecosystem for democratic nations and like-minded partners. The global public cloud can increase security and prosperity well beyond self-sufficient sovereign approaches. It is also more resilient and flexible than building stand-alone national barriers. U.S. allies and partners are deciding how closely they want to participate in U.S. clouds and, more broadly, align with U.S. economic and technical systems. They are weighing access to leading-edge U.S. technology, innovation, and growth against the greater independence and control that comes with strict sovereign approaches. White House Office of Science and Technology Policy (OSTP) Director Michael Kratsios stated at the August 2025 APEC ministerial that the United States wants its allies and partners to "have the AI sovereignty, data privacy, and technical customization that you so rightly demand on behalf of your peoples. We are committed to finding a way to enable America's private companies to meet your national technological needs."[55]

The global public cloud can increase security and prosperity well beyond self-sufficient sovereign approaches.

The more global-partner-focused Biden administration warned in its May 2024 International Cyberspace and Digital Policy Strategy that “there is an increasing willingness by some countries to embrace narratives of digital sovereignty and protectionism by blocking access to their markets, unduly preventing cross-border data flows, and preferencing domestic manufacturers and service providers.” The report continued that this has the “potential to undermine key digital economy and cybersecurity objectives,” recognizing that “cloud services and datacenters are also a source of tension with close trade partners.”[56]

Sovereign cloud can be implemented in ways that either increase shared prosperity and security or cut against it. These are policy choices. For example, policies like SecNumCloud that block foreign cloud providers from allied countries for ill-defined sensitive workloads, including at commercial entities, risk being more counterproductive than helpful. This creates barriers, rather than pooling resources and promoting stronger common solutions. Alternatively, the U.S. Federal Risk and Authorization Management Program (FedRAMP) for sensitive unclassified government workloads enables non-U.S. companies—such as Germany’s SAP and Siemens, France’s Ipsos, and many others—to provide cloud services to the U.S. government through their wholly owned U.S. subsidiaries. FedRAMP is based on open technical rules, not on country of ownership, and is for federal government use instead of commercial uses.

This paper proposes 10 recommendations to help governments achieve their security and economic goals and buttress an open, democratic, rules-based technology system.

1. **Avoid burdening purely commercial activities with the costs and innovation penalty of sovereign cloud.** Limit the spread of sovereign requirements to quasi-public commercial activities (for example, airlines, postal services, and banks). Sovereign cloud burdens a country’s economy with costs and complexity, and limits innovation and job growth. Though often intended to strengthen a domestic cloud industry, broad sovereign controls undercut a nation’s economic competitiveness. Broad public use of services does not by itself require a government sovereign cloud. Sovereign cloud is already impacting commercial markets. For example, an Accenture study found that “50% of European CXOs see data sovereignty as a top issue when selecting cloud vendors.”[57] Private sector entities should be free to assess the benefits and trade-offs of sovereign cloud and permitted to take a risk-based approach to adoption.
2. **Use sovereign clouds for government services, where they appropriately match the severity and likelihood of risk, and where the political and economic benefits outweigh the costs.** Sovereign requirements should be clearly defined and transparent. Many government workloads providing basic citizen services and public information can be run securely in commercial regions. For example, the government of Singapore initially ran 30 percent of government workloads in commercial regions and plans to increase workloads in commercial cloud regions.[58] There are multiple technical and operations tools in commercial clouds that provide essentially the same security that exists in sovereign clouds, and in some cases, more resiliency. Governments should fully explore and use these security tools first, potentially obviating the need for restrictive sovereign solutions.
3. **Classify government workloads and data into risk-based tiers to identify priority risks to mitigate.** Establishing a rigorous, data-driven process to transparently define

risks, their likelihood of occurrence, and how they can be mitigated is crucial to helping governments decide whether a workload needs to run in a sovereign cloud. It is also helpful for governments to determine which risks require priority action and how much they are willing to pay for sovereign controls. For example, the UK government moved "from approximately seven data classification levels to only three. The result of this simplification was that 96% of the government's [data] load was classified as being [the least restrictive] 'Official' level."[59] This also improves security by allowing governments to focus resources on the most critical data and systems.

4. **Build trust rather than walls—enhance cloud transparency, run cloud confidence building measures, and convene a joint G7/OECD-industry group to develop trustworthy cloud criteria.** At their root, sovereign clouds are about greater trust. Governments and cloud providers should jointly set up production environments to test and verify security, operational controls, governance, and resiliency. Cloud providers understand that transparency builds trust; they should provide enhanced transparency (e.g., logs, API requests, and information on how key services handle data) to governments in ways that do not diminish security or reveal proprietary information. Governments already have dozens of national standards (e.g., FedRAMP in the United States, G5 in Germany, and G-Cloud in the United Kingdom) as well as international standards (e.g., ISO 27001, 27017, and 27018, and System and Organizational Controls (SOC reports) to audit and enforce cloud compliance, including third party validation. The G7/OECD should convene a government-industry group to jointly develop trustworthy cloud criteria, similar to the Prague Principles for telecom.[60] Further, governments can increase trust in cloud by improving expertise through a sovereign cloud academy and sovereign cloud skill certification. Technical controls are only part of security. People and organizational processes are also critical and feature in many sovereign cloud controls. Cloud providers should tailor their training programs to meet sovereign objectives, similar to how "partner competencies" have been tailored for sovereign cloud.[61] Training also helps government operators learn best practices and improve security.

5. **Mitigate risk of disruption of the cloud by sanctions or "kill switch" risks by improving workload portability and resiliency across countries and cloud providers.** Governments may decide that autarkic sovereign clouds may be necessary in limited, well-defined cases, but they are a complement to public cloud solutions rather than a viable replacement and should be part of a broader risk management approach. Furthermore, it is not clear if autarkic national clouds are even achievable. How is software updated? When do replacement parts for IT hardware run out, and is the supply chain (including semiconductors) sovereign too? How long will autarkic clouds be competitively viable with global hyperscalers? Governments can achieve nearly all their goals through hyperscaler sovereign cloud solutions. Going the last mile to protect against kill switch risk via ownership restrictions and autarkic full immunity from the laws of others imposes huge costs. Governments must decide the likelihood of potential kill switch sanctions and how much they are willing to pay for redress with slower growth, less innovation, and less competitiveness.

   Governments should start by improving portability of key workloads through architectural requirements as alternatives or complements to restrictive sovereign controls. Architectural practices, standard technologies such as Kubernetes, and open-source software enable workloads to move to other clouds or to move on-premises. Operational techniques including standard configuration templates (infrastructure as code) also enable portability. Low-cost services that back up data stores in other geographies are widely available too. Cloud providers are also offering disconnected cloud operations, which have limits but could be part of a broader approach. Further, cloud workloads can operate across multiple regions (active-active), not just moved between regions. Yet portability, resiliency, and multi-region workloads require careful planning, service selection, and architectural consistency. This requires substantial skills to execute. Cloud providers should provide tools, architectural blueprints, and other support to help government users achieve this. The EU Data Act requires cloud providers to facilitate switching among clouds; a multi-stakeholder group facilitated by the European Commission has developed data portability codes of conduct.[62] This does not eliminate all risk of foreign dependency (which is impossible), but it is better than separate autarkic clouds for most uses.

6. **Partner with cloud providers on sovereign goals** so that governments do not spend tens of billions of dollars replicating largely undifferentiated IT infrastructure. Focus national economic development initiatives on higher-value services and workforce training that does a better job of driving growth, encouraging innovation, and promoting distinct cultural heritages. The five largest U.S. clouds will invest roughly $860 billion from 2023-2025, a budget that governments cannot afford.[63] Lower-level IT does not add unique national value or promote culture. Governments can focus on higher-value efforts and national priorities (e.g., healthcare); cloud providers can build IT infrastructure. Only 25 percent of cloud spending is used on infrastructure; another 25 percent is used for platform services like databases.[64] Half of user spending is on applications that customers actually use, rather than on the IT "plumbing." Governments will achieve greater economic development by encouraging a robust software, AI, and digital economy that exploits a low-cost cloud with few barriers and encourages innovation and entrepreneurship. Harnessing U.S. cloud provider technology, capital, and sovereign solutions to enhance economic growth is more effective than building restrictive national or regional clouds.

7. **Focus sovereign AI on building national datasets and AI models that are unique to individual countries rather than basic IT that does not reflect a nation's heritage.** Sovereign AI requires modern IT infrastructure, but it does not require a sovereign cloud. AI infrastructure for sovereign AI is typically available via access to commercial clouds. As with other sensitive workloads, there are many layers of security tools available in the cloud (encryption, identity and access controls) to protect AI datasets and model weights. There is little about IT infrastructure that is specific to national heritage, culture, or language. While there has been a shortage of AI chips in AI's early days (a situation which is improving), spending billions of dollars on largely undifferentiated IT infrastructure is often not sustainable. Purchasing AI infrastructure locks a country into hardware and software that rapidly becomes obsolete, which can hinder a country's AI competitiveness. Scarce public funds are better focused on nationally important data, AI models, and applications, so long as IT infrastructure is available. Achieving the benefits of AI also requires diffusing it broadly and building skills in application domains–not just buying cutting-edge IT systems.

8. **Avoid country-ownership-based requirements that erect trade, investment, and political barriers to partners and splinter the cloud.** France's SecNumCloud discriminates against treaty allies and forces technology transfer to local joint ventures as a condition of market entry. Governments should focus on the ability to meet transparent technical and operational requirements. National-ownership-based rules likely violate trade agreements (such as government procurement and trade in services) and feed distrust. They erect barriers to foreign partners and allies rather than enable joint efforts. They are also counterproductive to achieving their own goals, and they reduce security in practice by limiting access to global cybersecurity resources (e.g., threat data), hindering incident response (e.g., testing and patching), and creating obstacles to information sharing. Further, these measures often leave government users saddled with second-class services or stranded "white elephant" investments that hinder their economic goals and economic competitiveness.
9. **The U.S. government and U.S. cloud providers need to show other countries that their economic development goals are better achieved in partnership with the United States rather than by exclusion.** U.S. industry has a strong record of creating research and development, investment, and jobs around the world, localizing technology to national markets, and building local tech economies. This stands in contrast to China's record.[65] One recent example of the United States supporting other's economies is France's leading AI company, Mistral, which is led by French ex-employees of Google and Facebook. AWS, for its part, says, "We've driven economic development through our investment in infrastructure, jobs, and skills . . . across Europe."[66] Since 2010, Amazon has invested more than €320 billion in the European Union and currently employs more than 150,000 people in permanent roles there.[67] Google, IBM, Microsoft, Oracle, and others have similar sustained commitments. These efforts stand in contrast to Europe's more bureaucratic Gaia-X cloud promotion effort. More extreme proposals, such as EuroStack, that seek to create a fully independent tech stack and supply chain are widely seen as unworkable. The European Union (and many countries) has set ambitious technology goals in its "digital decade." The EU Draghi report calls out many of the challenges of regulatory-driven approaches.[68] EU countries are more likely to achieve their goals by partnering with U.S. cloud providers and tapping into their capital, technology, and skills. The U.S. government would be well served by continuing its technical cooperation programs (e.g., the National Science Foundation and Department of Energy), as well as U.S. university research exchanges and U.S. economic development programs (e.g., the Development Finance Corporation and the Export-Import Bank) with partners and allies. For example, these can be inputs into the "AI export packages" the Trump administration is developing, including what OSTP Director Kratsios identifies as "direct loans, loan guarantees, equity investments, co-financing, political risk insurance, credit guarantees, technical assistance, and feasibility studies."[69]
10. **Accelerate government-to-government negotiations to address underlying policy concerns that give rise to sovereign clouds, especially concerns about data sovereignty and economic sanctions.** Ultimately, political negotiations are needed to address political concerns. A new U.S.-EU Technology Initiative should prioritize and accelerate agreements. In Asia, APEC can provide similar mechanisms. For example, discriminatory actions against U.S. cloud providers could be dropped in exchange for U.S.

agreement to safeguard ally and partner access to U.S. technology from sanctions. This could be coupled with recent hyperscaler commitments to sovereign controls, local source code repositories, pre-positioned continuity agreements with local cloud providers, binding contracts, and local governance.

A U.S.-EU electronic evidence agreement (begun in the first Trump administration) would also help address EU data sovereignty concerns. The devil is in the details, but mutual defense treaty allies and rule of law democracies should be able to address each other's data requirements. The 2022 OECD Declaration on Government Access to Personal Data held by Private Sector Entities is a good starting point for building common data approaches that address necessity, proportionality, transparency, oversight, and redress.[70] A shared agreement on "what is a trusted cloud" criteria (in recommendation four above) would also help guide policy. The United States and other governments should pursue enhanced cybersecurity exchanges that can build trust in the cloud and in government data access. These mechanisms would generate confidence in foreign-owned clouds and minimize the need for costly and divisive sovereign controls. More broadly, government pursuit of sovereign clouds occurs within a given country's political, economic, and security relationships. Governments need to prioritize building shared security and prosperity with their allies and partners. Letting differences divide and weaken democracies only serves to strengthen their adversaries.

Sovereign clouds can be implemented in ways that increase prosperity and security, not reduce it. They can support mutually beneficial relationships in trade, investment, and security. The actions above can help nations enjoy the benefits of cloud computing and the AI revolution.

This is a choice and countries must act.

About the Author

Bill Whyman is a leading expert on the technology sector and is the Founder of Tech Dynamics LLC. He is known for market-tested expertise on the changing technology industry, competition, technology policy, and business model change. He brings a distinctive perspective combining industry experience (Amazon Web Services, McKinsey), financial markets (Evercore ISI, Legg Mason), and government policy (White House). Whyman was director for international economics at the White House National Security Council and National Economic Council. He also served at the State Department, including assignments at the White House Office of Science and Technology Policy and the Office of the U.S. Trade Representative. Most recently, Whyman was a senior manager at Amazon Web Services, where he built a 150-person global organization that enabled governments, education, and nonprofits to adopt cloud computing and accelerate their mission. For two decades he was the investment community's leading technology strategist, advising the top global investors on technology industry dynamics and company investments. He was chosen as the top-ranked Institutional Investor independent software analyst. He also cofounded his startup, Precursor. Whyman graduated from Cornell University Phi Beta Kappa, summa cum laude, and was a Truman Scholar. He studied at Oxford University and received an MPA from Princeton University.

Endnotes

[1] "Q2 Cloud Market Nears $100 Billion Milestone - and it's Still Growing by 25% Year over Year," Synergy Research Group, July 31, 2025, https://www.srgresearch.com/articles/q2-cloud-market-nears-100-billion-milestone-and-its-still-growing-by-25-year-over-year.

[2] President Donald J. Trump (@realDonaldTrump), Truth Social, August 25, 2025, https://truthsocial.com/@realDonaldTrump/posts/115092243259973570.

[3] "EuroStack," EuroStack, https://eurostack.eu/.

[4] Matthias Bauer and Philipp Lamprecht, *The Economic Impacts of the Proposed EUCS Exclusionary Requirements: Estimates for EU Member States* (Brussels: European Centre for International Political Economy, October 2023), https://ecipe.org/wp-content/uploads/2023/10/ECI_23_OccasionalPaper_04-2023_LY06.pdf.

[5] International Monetary Fund, "Government Expenditure, Percent of GDP," https://www.imf.org/external/datamapper/exp@FPP/USA/FRA/JPN/GBR/SWE/ESP/ITA/ZAF/IND.

[6] Microsoft, "Microsoft to deliver cloud services from new datacentres in Germany in 2019 to meet evolving customer needs," August 31, 2018, https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/#:~:text=In%20March%202018%2C%20we%20announced,(C5)%20certification%20in%20Germany. The Microsoft Cloud service documentation shows Cloud Deutschland is closed at: https://learn.microsoft.com/en-us/power-platform/admin/about-microsoft-cloud-germany.

[7] Max Peterson, "AWS plans to invest €7.8B into the AWS European Sovereign Cloud, set to launch by the end of 2025," AWS, *AWS Security Blog*, May 14, 2024, https://aws.amazon.com/blogs/security/aws-plans-to-invest-e7-8b-into-the-aws-european-sovereign-cloud-set-to-launch-by-the-end-of-2025/.

8 “What Is Sovereign AI?” Nvidia, *Blogs*, February 28, 2024, https://blogs.nvidia.com/blog/what-is-sovereign-ai/; and Nvidia, “NVIDIA Announces Financial Results for Second Quarter Fiscal 2026,” press release, August 27,2025, https://nvidianews.nvidia.com/news/nvidia-announces-financial-results-for-second-quarter-fiscal-2026.

9 IDC, “IDC Forecasts Worldwide Sovereign Cloud Spending to Reach More Than $250 Billion in 2027,” press release, December 14, 2023, https://hostingjournalist.com/news/idc-global-sovereign-cloud-spending-to-exceed-250b-by-2027#:~:text=News%20Summary,over%20data%20access%20and%20usage.

10 Bill Whyman, *Secrets from Cloud Computing’s First Stage: An Action Agenda for Government and Industry* (Washington, DC: Information Technology & Innovation Foundation, June 2021), https://itif.org/publications/2021/06/01/secrets-cloud-computings-first-stage-action-agenda-government-and-industry/.

11 *#Eurostack: European Strategic Sovereign Digital Infrastructures* (Brussels: EuroStack, January 10, 2025), https://eurostack.eu/wp-content/uploads/2025/06/eurostack_pitch_10-january-2025.pdf; EuroStack, “Open Letter: European Industry Calls for Strong Commitment to Sovereign Digital Infrastructure,” March 14, 2025, https://euro-stackletter.eu/wp-content/uploads/2025/03/EuroStack_Initiative_Letter_14-March-.pdf.

12 Brad Smith, “Microsoft Announces New European Digital Commitments,” Microsoft, *Microsoft on the Issues* (blog), April 30, 2025, https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/.

13 Hayete Gallot, “Advancing Sovereignty, Choice, and Security in the Cloud for our Customers,” Google, *Blog*, May 21, 2025, https://cloud.google.com/blog/products/identity-security/google-advances-sovereignty-choice-and-security-in-the-cloud?e=48754805.

14 About Amazon Team, “Built, Operated, Controlled, and Secured in Europe: AWS Unveils New Sovereign Controls and Governance Structure for the AWS European Sovereign Cloud,” Amazon, *Amazon News* (blog), June 3, 2025, https://www.aboutamazon.eu/news/aws/built-operated-controlled-and-secured-in-europe-aws-unveils-new-sovereign-controls-and-governance-structure-for-the-aws-european-sovereign-cloud.

15 U.S. House of Representatives Subcommittee on Antitrust, *Investigation of Competition in Digital Markets*, 116th Cong., 1st sess. (2020), https://democrats-judiciary.house.gov/sites/evo-subsites/democrats-judiciary.house.gov/files/migrated/UploadedFiles/Competition_In_Digital_Markets.pdf.

16 Lloyd’s of London and AIR Worldwide, *Cloud Down: Impacts on the US Economy* (London: Lloyd’s, 2018), https://assets.lloyds.com/assets/pdf-air-cyber-lloyds-public-2018-final/1/pdf-air-cyber-lloyds-public-2018-final.pdf.

17 Tim Ross and Nette Nöstlinger, “Germany’s Merz Vows ‘Independence’ from Trump’s America, Warning NATO May Soon Be Dead,” *Politico*, February 23, 2025, https://www.politico.eu/article/friedrich-merz-germany-election-united-states-donald-trump-nato/.

18 Adam Satariano and Jeanna Smialek, “Europe’s Growing Fear: How Trump Might Use U.S. Tech Dominance Against It,” *New York Times*, June 20, 2025, https://www.nytimes.com/2025/06/20/technology/us-tech-europe-microsoft-trump-icc.html.

19 Bitkom, “Business Calls for a German Cloud,” press release, June 11, 2025, https://www.bitkom.org/Presse/Presseinformation/Wirtschaft-ruft-nach-deutscher-Cloud.

20 “Motions Submitted During the Debate on Migrations of Government ICT Abroad,” Dutch Parliament, March 18, 2025, https://www.tweedekamer.nl/kamerstukken/stemmingsuitslagen/detail?id=2025P04110&did=2025P04110.

21 Amazon Staff, “Safeguarding Ukraine’s Data to Preserve its Present and Build Its Future,” Amazon, *News*, June 9, 2022, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future.

22 Ibid.

23 *Amazon Information Request Report* (Seattle: Amazon, July 2025), https://d1.awsstatic.com/Security/pdfs/Amazon_AWS_Information_Request_Report_H1_2025.pdf.

24 A leading example is the Cross-Border Data Forum: https://www.crossborderdataforum.org/.

25 U.S. Trade Representative, *2025 National Trade Estimate Report on Foreign Trade Barriers* (Washington, DC: U.S. Trade Representative, 2025), https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf; and IMF, “World Economic Outlook,” https://data.imf.org/en/datasets/IMF.RES:WEO.

26 European Commission, “IPCEI on Next-Generation Cloud Infrastructure and Services to Boost Europe’s Digital Decade,” European Commission, *News & Views*, December 5, 2023, https://digital-strategy.ec.europa.eu/en/news/ipcei-next-generation-cloud-infrastructure-and-services-boost-europes-digital-decade.

27 U.S. Trade Representative, *2024 National Trade Estimate Report on Foreign Trade Barriers* (Washington, DC: U.S. Trade Representative, 2024), 145, https://ustr.gov/sites/default/files/2024%20NTE%20Report.pdf.

28 Ibid.

29 Meredith Broadbent, “The European Cybersecurity Certification Scheme for Cloud Services,” CSIS, *Commentary*, September 1, 2023, https://www.csis.org/analysis/european-cybersecurity-certification-scheme-cloud-services.

30 Martin Hullin, “EuroStack - A European Alternative for Digital Sovereignty,” Bertelsmann Siftung, February 13, 2025, https://www.bertelsmann-stiftung.de/en/our-projects/reframetech-algorithmen-fuers-gemeinwohl/project-news/eurostack-a-european-alternative-for-digital-sovereignty.

31 McKinsey & Company, *The Economic Potential of Generative AI: The Next Productivity Frontier* (New York: McKinsey & Company, June 2023), https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20economic%20potential%20of%20generative%20ai%20the%20next%20productivity%20frontier/the-economic-potential-of-generative-ai-the-next-productivity-frontier.pdf.

32 Peter Dizikes, “Daron Acemoglu: What Do We Know about the Economics of AI?” MIT Economics, *MIT News*, December 6, 2024, https://economics.mit.edu/news/daron-acemoglu-what-do-we-know-about-economics-ai#:~:text=One%20of%20his%20crucial%20concerns,workers%20share%20in%20the%20gains?.

33 Gregory C. Allen, Georgia Adamson, Lennart Heim, and Sam Winter-Levy, “The United Arab Emirates’ AI Ambitions Key Implications for Maintaining U.S. AI Leadership, CSIS, January 24, 2025, https://www.csis.org/analysis/united-arab-emirates-ai-ambitions.

34 “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,” White House, October 30, 2023, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

35 Author’s calculation based on company quarterly earnings releases.

36 Angie Lee, “What Is Sovereign AI?” Nvidia, *Blogs*, February 28, 2024, https://blogs.nvidia.com/blog/what-is-sovereign-ai/.

37 Nvidia, “Investor Presentation Q2 FY26 September 2025,” https://s201.q4cdn.com/141608511/files/doc_financials/2026/q2/NVDA-F2Q26-Quarterly-Presentation-FINAL.pdf.

38 “About SEA-LION,” SEA-LION AI, https://sea-lion.ai/our-story/.

39 Goh Yan Han, “$70m S’pore AI initiative to develop first large language model with South-east Asian context,” *Straights Time*s, December 4, 2023, https://www.straitstimes.com/singapore/70m-s-pore-ai-initiative-to-develop-first-large-language-model-with-south-east-asian-context.

40 “Introducing TII’s Falcon-H1 and Falcon Arabic,” Technology Innovation Institute, https://falconllm.tii.ae/.

41 M Saiful Bari et al., “ALLaM: Large Language Models for Arabic and English,” ArXiv, July 22, 2024, https://arxiv.org/html/2407.15390v1.

42 “TAIDE Model,” TAIDE, https://en.taide.tw/download.html.

43 “Interim Measures for the Administration of Generative Artificial Intelligence Services,” Cyberspace Administration of China, July 13, 2023, https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm#:~:text=(1)%20Adhere%20to,and%20harmful%20information%3B.

44 Liza Lin, “China Puts Power of State Behind AI—and Risks Strangling It,” *Wall Street Journal*, July 16,2024, https://www.wsj.com/tech/china-puts-power-of-state-behind-aiand-risks-strangling-it-f045e11d.

45 Jinahan Li, “What questions will China’s DeepSeek not answer?,” Deustche Welle, January 31, 2025, https://www.dw.com/en/what-questions-will-chinas-deepseek-not-answer/a-71470843.

46 “Digital Sovereignty”, International Data Corporation, https://my.idc.com/getdoc.jsp?containerId=IDC_P45150#:~:text=Enhancing%20cybersecurity%2C%20expanding%20cloud%20use,recommendations%20for%20vendors%20and%20users.

47 Whyman, *Secrets from Cloud Computing’s First Stage*.

48 AWS Events, “Meet digital sovereignty needs with AWS Dedicated Local Zones (WPS214),” recorded at AWS re:Invent 2023, YouTube video, December 11, 2023, https://www.youtube.com/watch?v=nU4HkNmpG8w.

49 As stated in cloud service product documentation and guidance.

50 Ibid.

51 “Boom Is Supersonic,” Boom, https://boomsupersonic.com/.

52 The German Association of the Automotive Industry, *European Cybersecurity Certification Scheme for Cloud Services (EUCS)* (Berlin: VDA, April 2024), https://www.vda.de/en/news/publications/publication/european-cybersecurity-certification-scheme-for-cloud-service--eucs-.

53 Ibid.

54 Amazon Web Services, “AWS re:Invent 2023 - Meet digital sovereignty needs with AWS Dedicated Local Zones (WPS214)” December 11, 2023, YouTube video, 28:35 and 37:11, https://www.youtube.com/watch?v=nU4HkNmpG8w.

55 “Remarks by Director Kratsios at the APEC Digital and AI Ministerial Meeting,” The White House, August 5, 2025, https://www.whitehouse.gov/articles/2025/08/remarks-by-director-kratsios-at-the-apec-digital-and-ai-ministerial-meeting/.

56 U.S. State Department, *United States International Cyberspace & Digital Policy Strategy* (Washington, DC: U.S. State Department, May 6, 2024), https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf.

57 Accenture, *Sovereign Cloud Comes of Age in Europe* (Dublin: Accenture, 2023), https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-Sovereign-Cloud-PoV-Short-2023.pdf.

58 AWS Events, "Meet digital sovereignty needs with AWS Dedicated Local Zones (WPS214)."

59 Antonio García Zaballos et al., *Public Procurement of Cloud Computing Services: Best Practices for Implementation in Latin America and the Caribbean* (Washington, DC: Inter-American Development Bank, BEST Network, and Microsoft, 2020), 15, https://publications.iadb.org/es/contratacion-publica-de-servicios-de-computacion-en-la-nube-mejores-practicas-para-su.

60 CSIS Working Group on Trust and Security in 5G Networks, *Criteria for Security and Trust in Telecommunications Networks and Services* (Washington, DC: CSIS, May 2020), https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services.

61 "AWS Digital Sovereignty Competency," Amazon Web Services, https://aws.amazon.com/compliance/digital-sovereignty/partners/.

62 "SWIPO Data Portability Code of Conduct," https://cloud.google.com/security/compliance/swipo-codes.

63 Author's calculation from company quarterly financial reports.

64 Gartner, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Surpass $675 Billion in 2024," press release, May 20, 2024, https://www.gartner.com/en/newsroom/press-releases/2024-05-20-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-surpass-675-billion-in-2024.

65 Bill Whyman, *Competing for the Future of Cloud Computing in Latin America* (Washington, DC: CSIS, June 2023), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-06/230607_Whyman_Cloud_Computing_1.pdf.

66 Max Peterson, "AWS plans to invest €7.8B into the AWS European Sovereign Cloud."

67 About Amazon Team, "Hope Returns to Europe's Industrial Heartlands: Amazon's €320 Billion Investment Story, " Amazon, *Amazon News* (blog), June 4, 2025, https://www.aboutamazon.eu/news/job-creation-and-investment/hope-returns-to-europes-industrial-heartlands-amazons-320-billion-investment-story.

68 The European Commission, *The Future of European Competitiveness: Part A* (Luxembourg: Publications Office of the European Union, 2025), https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.

69 "Remarks by Director Kratsios," The White House.

70 "Declaration on Government Access to Personal Data Held by Private Sector Entities," OCED, December 14, 2022, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

COVER PHOTO AR_TH VIA ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**