BROOKINGS CEPS

REPORT
FEBRUARY 2026

IS AI SOVEREIGNTY POSSIBLE?

BALANCING AUTONOMY AND INTERDEPENDENCE

Brooke Tanner, Cameron F. Kerry, Andrew Wyckoff, Nicoleta Kyosovska, Andrea Renda, and Elham Tabassi

ACKNOWLEDGEMENTS

Joshua P. Meltzer contributed to this report during his tenure as a senior fellow at Brookings and a founder of the Forum for Cooperation on AI. The authors are grateful to him for his contributions during his time at Brookings, and also to Pablo Chavez, Samm Sacks, and David Shrier for their generous input to the report and events that informed it. They also thank Michelle Du, Carolina Oxenstierna, and Shreya Sampath for research assistance. We are also thankful for editing and production assistance from Antonio Saadipour, Josie Stewart, Massimiliano Colonna, and Adelle Patten of the Brookings Institution, Jennifer Kaczor, and Julia Huang.

Amazon, Google, Meta, Microsoft, and the Taiwan Semiconductor Manufacturing Company are donors to the Brookings Institution. Amazon Web Services, Google, Meta and Microsoft are donors to CEPS. Brookings and CEPS recognize that the value they provide is in their absolute commitment to quality, independence, and impact. The findings, interpretations, and conclusions in this report are not influenced by any donation.

ABOUT

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its authors, and do not reflect the views of the Institution, its management, or its other scholars. For more, visit www.brookings.edu.

The Centre for European Policy Studies (CEPS) is an independent policy research institute in Brussels. Its mission is to produce sound policy research leading to constructive solutions to the challenges facing Europe. Facebook, Google, and Microsoft are donor members of CEPS. The views expressed in this report are entirely those of the authors and should not be attributed to CEPS or any other institution with which they are associated or to the European Union.

The Forum for Cooperation on Artificial Intelligence (FCAI) is a collaboration between the Brookings Institution and the CEPS. FCAI hosts regular AI dialogues among high-level officials from seven governments (Australia, Canada, EU, Japan, Singapore, U.K., and the U.S.) as well as experts from industry, civil society, and academia, aimed at identifying opportunities for international cooperation on AI regulation, standards, and R&D.

CONTENT

EXECUTIVE SUMMARY

The concept of artificial intelligence (AI) sovereignty has entered policy discussions as governments confront the strategic importance of AI infrastructure, data, and models amid rising dependence on a small number of firms and jurisdictions. This report defines AI sovereignty as a spectrum of strategies to enhance a country's capacity to make independent decisions about critical AI infrastructure deployment, use, and adoption, rather than literal autarky. Motivations vary—from protecting national security and resilience and supporting economic competitiveness, to ensuring cultural and linguistic inclusion in model training and datasets and strengthening influence in global governance. These aims are often legitimate, but "sovereign AI" can also become a vehicle for protectionism, fragmented markets and standards, and duplicative or stranded public investment. The central finding is that full-stack AI sovereignty is structurally infeasible for almost any country because AI is a transnational stack with concentrated choke points across minerals, energy, compute hardware, networks, digital infrastructure, data assets, models, applications, and the crosscutting enablers of talent and governance. The practical alternative is "managed interdependence," an approach that relies on strategic alliances and partnerships to reduce risks throughout the AI stack. Countries can operationalize managed interdependence by mapping dependencies by layer, prioritizing feasible interventions, diversifying suppliers and partners, and embedding interoperability and portability through technical standards, procurement, and governance. Done well, managed interdependence can strengthen resiliency and agency while preserving the benefits of open markets and cross-border collaboration.

INTRODUCTION

As artificial intelligence (AI) occupies an increasingly central role in global public policy and discourse, "AI sovereignty" has become part of many policymakers' vocabularies. This term bundles several concepts of strategic, economic, and cultural autonomy by managing key infrastructure, data, and governance rules within jurisdictional boundaries. Its concerns stem from numerous objectives that reflect valid governmental interests as well as others that may prove counterproductive. AI rests on global foundations—transnational research collaborations, complex supply chains, information technology networks, and vast stores of data that reflect human knowledge and activity—from which no country can separate entirely. This report examines how valid aims of sovereign AI will require understanding and managing interdependencies.

The potential impact[1] and rapid pace[2] of AI development and diffusion have widened digital sovereignty concerns globally and given them added urgency. So too have the dominance of the United States and China in AI development and deployment and the geopolitical rivalry between these two global powers, as other countries seek to close gaps and avoid being caught in between. Ambitions around AI compute, data, and models take many forms as countries seek greater security, resilience, economic competitiveness, and cultural-linguistic inclusion through AI sovereignty strategies. With India, a leader in AI sovereignty initiatives, hosting the February 2026 AI Impact Summit,[3] the topic will be on the international stage.

The potential impact and rapid pace of AI development and diffusion have widened digital sovereignty concerns globally and given them added urgency.

There are sound reasons for countries to seek agency over AI systems. Clearly, support for multiple languages enhances the utility of AI, providing wider access to the knowledge and benefits that AI enables. Developing or operating AI systems domestically can provide societal benefits and is often deemed essential for national security and domestic and international competition. These benefits are not guaranteed; their complexity and cost may render them infeasible or inefficient, and their performance, resiliency, and security may not equal those of international alternatives. As a result, sovereign AI systems may lead to stranded or underused investment.

Sovereign AI systems could fragment markets, slow the global development and diffusion of AI, and reduce host countries' economic competitiveness. Such systems can become tools for digital authoritarianism

within countries, eroding individual rights. Some countries pursue sovereign AI to secure influence within emerging global AI governance networks. Without coordination across borders, fragmented AI systems could reduce interoperability among AI systems. Conversely, some countries with global influence have pursued "sovereign AI strategies" to cement or extend existing dominance.

Thus, AI sovereignty presents complex trade-offs and necessitates key questions for global AI players, including the United States and China, as they seek to diffuse their AI products and for many other countries that want their own AI systems.

- How can countries capture the economic benefits of domestic AI systems while avoiding inefficient investments, underperformance, and reduced competitiveness?
- How should countries reconcile AI sovereignty with international cooperation in areas like safety and security?
- How can governments ensure that sovereign AI systems protect human rights rather than serve as instruments of digital authoritarianism?
- How can countries manage such objectives in ways that avoid fragmentation or stranded investment?

This report examines these trade-offs and how governments can manage them. It describes the aims and motivations of AI sovereignty aspirations, the geopolitical landscape in which they operate, and how various governments are responding. Then, the report proposes a policy framework that focuses on a carefully tailored assessment of advantages and vulnerabilities tied to the essential building blocks of AI—the various layers of the AI value chain and ecosystems that comprise the AI stack—and the dependencies that they present. The trade-offs call for what we describe as "managed interdependence," reconciling state autonomy with necessary and beneficial international cooperation and coordination. The report considers how countries can navigate these trade-offs in the context of a turbulent global order.

PART I.
WHAT IS AI SOVEREIGNTY?

Drivers of AI sovereignty

Sovereignty in the digital arena emerged from the development of the global internet. Early internet exceptionalism[4] argued that the internet was immune to state control; even so, states and policymakers have come to see digital space as a critical domain of national policy and have asserted sovereignty in various ways. As Jack Goldsmith and Tim Wu wrote[5] in 2006, "Territorial government is a persistent fact of human history that accommodates humanity in its diversity and allows it to flourish," and "the United States, China, and Europe are using their coercive powers to establish different visions of what the Internet might be."

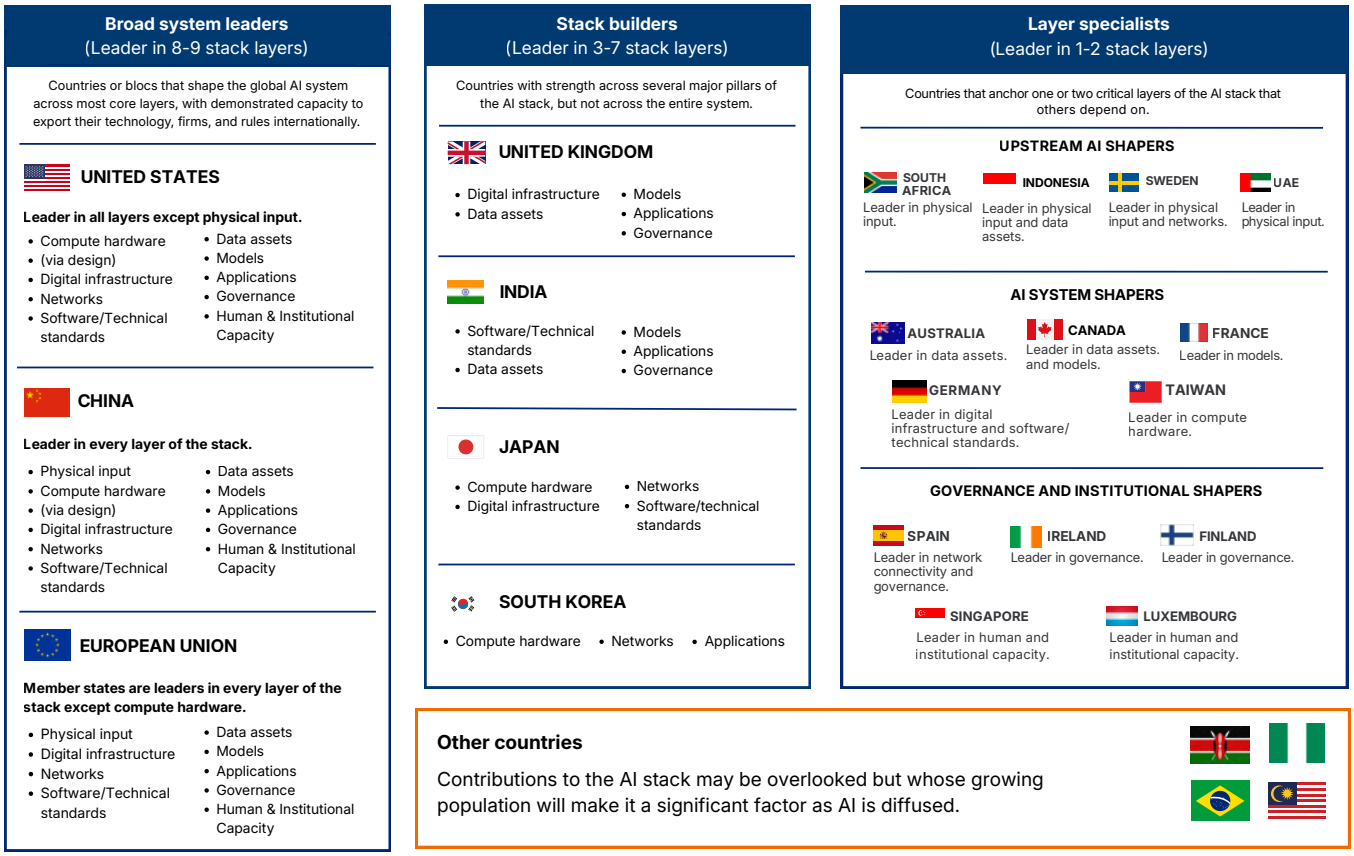
China has been the most assertive in exercising such powers,[6] beginning with its Great Firewall and restrictions on service providers that drove out Google and Yahoo. This greatly expanded state control over information flows and public opinion under a "cyber sovereignty" policy—articulated in a 2010 white paper[7]—and excluded foreign competitors,[8] including Facebook, Google, and Twitter. "Sovereignty" in this approach is a matter of state sovereignty. Europe has made "digital sovereignty"[9] a feature of an ambitious digital agenda aimed at setting global rules for the digital economy via the Brussels effect,[10] as the General Data Protection Regulation[11] (GDPR) did.[12] In this approach, sovereignty is a broader concept that encompasses choice and agency for society as a whole. Other countries have drawn digital regulations from these roadmaps, such as requirements for localized storage[13] of data gathered on their territory or restrictions on social media providers.[14]

AI sovereignty extends these previous sovereignty claims across the AI stack, from content and data to compute, models, and other dependencies. The quest for sovereignty comprises four groups whose positioning is detailed in Figure 1.

1. **Broad stack leaders**: the United States, China, and the European Union, which have invested the most and have the most integrated AI stacks (though not fully integrated).
2. **Coordinated stack builders**, such as India, Japan, and the United Kingdom, each of which has strengths across several major layers of the AI stack (through prominence in AI supply chains, strong domestic talent, high capital for investment, or national interest/attention to sovereign AI) but not across the entire system.
3. **Strategic layer specialists**, including Canada, Germany, Singapore, and South Korea, which are strong in particular layers of the AI stack but remain heavily dependent on other countries for essential elements like minerals, chips, data, talent, and compute.
4. **Other countries** beginning AI deployment, whose contribution to the AI value chain has been overlooked but whose growing population will make it a significant factor as AI is diffused. These categories describe positions within the global AI ecosystem, not stages of development or paths toward a single model of AI sovereignty.

FIGURE 1

Global AI leadership: AI stack strategic positioning[15]



BROOKINGS

SOURCE: Authors' determinations using data from the Global Critical Minerals Outlook (May 21, 2025), International Energy Agency, Electricity Mix, Market share for logic chip production, by manufacturing stage, and Cumulative number of large-scale AI systems by country since 2017 (2021–2024, Our World in Data), Stanford AI Index Report (2025, Stanford AI Human-Centered Artificial Intelligence), Data Centers Around the World (May 2021, United States International Trade Commission), Broadband statistics (2024, Organisation for Economic Co-operation), Safeguarding Subsea Cables (2024, Center for Strategic and International Studies), GitHub Repositories (January 2026, GitHub), Distribution of Authors per Country (August 2024, Internet Engineering Task Force), ICT service exports (BoP, current US$) (2024, World Bank), Individuals using the Internet (2025, International Telecommunication Union), and Wikimedia statistics (2025, Wikimedia). For more information on determinations, see Appendix A.

These groups and their respective contributions to the AI stack shape how the governments involved see AI sovereignty. For the United States, China, and the European Union, it is about expanding the global markets and protecting their flanks by shoring vulnerabilities in key inputs like semiconductors. For others, it is about finding pathways to cope with the superpowers' dominance.

Although all countries pursue AI sovereignty in different ways for different reasons, they share a common desire[16] for control over technology and to reduce dependence on foreign providers, mitigate exposure to extraterritorial policy shifts, and enable wider deployment of AI systems that are culturally and linguistically aligned with their national or regional context across government services and critical sectors. On

the adoption side, governments view sovereign AI as a means of ensuring reliable access to advanced AI capabilities that are aligned with domestic legal frameworks, linguistic contexts, and public-sector needs. On the competition side, countries may pursue sovereign AI to strengthen national competitiveness, capture economic value, and secure influence within emerging global AI ecosystems. This motivation is closely tied to concerns about industrial policy, talent retention, and control over data, compute, and foundational models.

The shift from digital sovereignty to AI sovereignty reflects a move from governing online content and data flows to governing dependencies in the AI stack. Across jurisdictions, the policy case for sovereignty primarily rests on four propositions: protecting security and continuity of critical systems; capturing economic value and limiting strategic dependence; ensuring models and deployments reflect local language, law, and norms; and strengthening a country's position in emerging international rules and standards.

NATIONAL SECURITY AND RESILIENCE

Countries increasingly[17] view control over critical digital infrastructure as a core component of national security.[18] Governments seek to safeguard[19] their systems against foreign disruption, surveillance, or malign influence. The use of export controls to restrict the export of specific goods has underscored the dangers of being cut off from essential technologies, motivating[20] nations to develop domestic capabilities to secure greater strategic autonomy. For some jurisdictions, national security framing also includes concerns about extraterritorial legal access to data[21] and compelled cooperation[22] by foreign providers.

Using a foreign company's AI cloud for military data analysis, for example, may raise concerns about intelligence leakage or remote interference. States seek sovereign capability to develop and deploy AI in defense and critical infrastructure without backdoors controlled by adversaries. AI could be used to manage[23] power[24] grids[25] or emergency response;[26] few countries are comfortable relying on an adversary's technology for such functions. Fears that terrorists[27] or rogue states[28] could weaponize AI motivate the buildup of state capacity to counter malicious uses of AI, leading to sovereign projects focused on both defensive and offensive capabilities.

ECONOMIC COMPETITIVENESS AND INDUSTRIAL POLICY

Second, AI is widely regarded as a general-purpose technology that will drive some amount of economic growth. The United States, home to many of the world's leading companies across the AI stack, already occupies a dominant position. In response, many sovereign AI strategies include components of industrial policy aimed at increasing domestic production capabilities in specific layers of the AI stack to reduce these dependencies. The dislocation of manufacturing associated with globalization, combined with supply-chain disruptions during the COVID-19 pandemic, has heightened sensitivities to dependencies on imports. More recently, U.S. export controls, the weaponization of tariffs, and threats to allies and trading partners have increased uncertainty about the dependability of the U.S. AI stack in particular. For U.S. allies, such concerns have been magnified by rhetoric and conduct toward close partners, such as threats of tariffs[29] and even military force[30] over claims for Greenland that cast doubt on the stability of their alliances.

Nations also fear being relegated to the status of "consumers" of foreign AI products, ceding high-value industries and jobs to other countries. Sovereign AI policies are therefore often designed to capture[31] a greater share of the economic value[32] created by AI. These policies aim to foster local talent,[33] build domestic innovation ecosystems,[34] and ensure that a nation's industries remain competitive.

CULTURAL, LINGUISTIC, AND NORMATIVE VALUES

Third, there is a growing concern that AI systems trained on ostensibly global datasets—but often predominantly Western and English-language sources—may perpetuate an "AI monoculture"[35] that fails to account for local languages, cultures, and legal

principles. Sovereign AI initiatives seek to counter this risk by developing models aligned with national or regional values. For example, Singapore's SEA-LION[36] project aims, in part, to avoid[37] a "West Coast American bias" perceived in existing models. Similarly, Taiwan's development of the Trustworthy AI Dialogue Engine (TAIDE model)[38] was partly motivated by the desire for an AI system that reflects Taiwanese culture as a counterweight[39] to Chinese models designed to adhere[40] to "core socialist" values. Other motivations[41] include preserving data protection, maintaining public trust, and entrenching digital rights.

STAKES IN INTERNATIONAL GOVERNANCE DISCUSSIONS

Lastly, some countries are building sovereign AI strategies and domestic capacity in specific areas of the AI stack to gain leverage in international governance discussions. As global governance bodies debate AI principles[42] and rules of the road,[43] many governments want a seat at the table[44] and may perceive that having an AI strategy or a developed AI-related industry could strengthen[45] their voice or representation in the international dialogue. This rationale is especially salient for mid-sized powers and Global Majority countries that seek influence over standards, evaluation norms, and terms of access for compute and models. These countries may want more global recognition, not only as consumers of AI but also as producers. From this perspective, sovereign AI is not only about access or resilience but also about positioning in an increasingly stratified global AI landscape, where early movers and system owners may shape standards, markets, and norms.

LEGITIMATE CONCERNS OR PROBLEMATIC DRIVERS?

While analytically distinct, the propositions discussed above frequently reinforce one another. Efforts to enable broad domestic adoption can build the technical capacity and institutional confidence needed for competitive positioning, while competitive ambitions can justify the investments required to support large-scale adoption. Understanding the balance between adoption-driven and competition-driven rationales is therefore critical for assessing how sovereign AI strategies are likely to evolve.

Still, there are genuine concerns about managing concentrated power,[46] both at a firm and geographic[47] level, to ensure representation and trust. At a firm level, dependence[48] on a small number of frontier-model providers, hyperscalers, and semiconductor manufacturers, can lead to market concentration with undesirable outcomes, including risks of lock-in, asymmetric bargaining power, self-preferencing and discrimination, and unbalanced economic and political power. Sovereignty strategies can operate to restore democratic control,[49] local agency, and oversight to ensure key decisions are not made "elsewhere" by unelected, distant, or unaccountable actors.

Similarly, relying on a few countries[50] for compute, talent,[51] capital, and governance choices can risk other countries' representation in global discussions and may challenge a government's public trust and legitimacy. This concentration also risks national security goals if a country is overly reliant on an unstable geographic region or partner for access to AI infrastructure. Sovereignty strategies may aim to ensure that the benefits of AI are not captured exclusively by dominant actors.

These concerns take a problematic turn when steeped in digital authoritarianism,[52] where "AI sovereignty" may increase state control over information and digital infrastructure. Sovereignty rhetoric can legitimize policies that concentrate control points[53] in the hands of state security agencies through state surveillance systems, censorship or filtering algorithms, or political control over digital infrastructure, while using the language of security and sovereignty to legitimize these restrictions. If a country lacks democratic and transparent norms, pushes toward greater AI sovereignty could accelerate the erosion of rights and freedom.

While most AI sovereignty strategies aim to expand domestic capacity and competitiveness, some strategies include more protectionist or mercantilist framings. Protectionist versions of sovereignty strategies often treat foreign competition as the central threat[54] and thus restrict competition or influence markets

through coercive or asymmetric tools, including localization requirements, data hoarding, or weaponized licensing. A useful distinction between industrial strategy and protectionism is whether interventions primarily build domestic capacity while preserving interoperability and contestability or discriminate against foreign providers and promote national champions. Furthermore, as AI sovereignty efforts often involve close partnerships between states and private platforms, they may distort public priorities if governments invest heavily without clear public returns.[55]

If each country were to achieve complete control over the domestic production of the entire AI stack, markets could fragment[56] and lead to isolated "AI islands" with potentially incompatible standards and governance systems that thwart interoperability, complicate compliance requirements, reduce diffusion of innovations, and allow for regulatory arbitrage.[57] These risks are more likely, and consequences are more severe, if sovereignty strategies are not paired with initiatives for interoperability and cooperation.

How countries are approaching AI sovereignty

BROAD STACK LEADERS

United States

The United States has leveraged its private sector dominance across key layers of the AI stack to promote an "American AI stack" as the de facto global standard. The United States' dominance is part of what is driving other governments[58] to diversify and gain more control over AI technologies.

The U.S. AI Action Plan,[59] released in July 2025, explicitly endorses the idea of an American sovereign AI stack as the "gold standard" for AI worldwide and seeks to ensure allies build on U.S. technology. The plan's strategy is built on three pillars: accelerate innovation, build AI infrastructure, and lead in international diplomacy and security.

In line with the AI Action Plan, the White House issued an executive order[60] (EO) establishing the American AI Exports Program.[61] This program aims to preserve and extend U.S. leadership while reducing international dependence on adversarial technology by deploying full-stack AI export packages, including AI-optimized hardware, data pipelines, AI models, and cybersecurity measures. The EO also directs U.S. development finance organizations to prioritize AI initiatives.

The federal government has made several investments in AI development, including taking[62] a 10% stake in Intel,[63] a private company, and expressing interest[64] in "many more [investments] like it." Similarly, the government recently announced[65] a $12 billion U.S. stockpile of rare earth minerals. Additionally, it has incentivized private investment in AI infrastructure, including fundraising[66] for large-scale AI projects in American states such as Pennsylvania[67] and support for private infrastructure initiatives like the Stargate Project.[68]

At the same time, the U.S. government maintains one of the world's most mature public-sector AI ecosystems. According to recent estimates, U.S. firms developed[69] over 70% of foundation models. Supercomputers operated by the Department of Energy,[70] the Department of Defense,[71] and NASA[72] support classified and publicly available AI research at scale. The federal government has decades of institutional experience in large-scale data processing, scientific computing,[73] and mission-oriented research and development (R&D). These assets provide a strong foundation for national AI capability, even if not branded as sovereign infrastructure. The U.S. has worked with allies and partners to shape international governance frameworks,[74] including support for global AI safety initiatives[75] and policy frameworks[76] around digital infrastructure.

The recent National Security Strategy[77] outlines AI as a core foreign policy interest "to ensure that U.S. technology and U.S. standards—particularly in AI, biotech, and quantum computing—drive the world forward."

The United States also uses development finance to promote U.S.-aligned AI infrastructure abroad. The Development Finance Corporation (DFC), established in response[78] to China's trillion-dollar Belt and Road Initiative (BRI), remains limited in scale compared with that program's global footprint. In its first four years, the agency made investments[79] in more than 100 countries and reached[80] a portfolio of $48.9 billion in 2024. After a brief lapse in funding, Congress reauthorized[81] the DFC until 2031.

The United States has implemented stringent export controls[82] on advanced semiconductors and manufacturing equipment and strengthened[83] these controls in 2024 to slow China's military and technological progress. These controls included monitoring potential misuse of U.S. data centers by adversaries. For example, China's AI engineers were able to access[84] banned AI chips through cloud computing after gaps in 2024 export-control rules. The Biden administration aimed to close[85] this loophole through its January 2025 Framework for Artificial Intelligence Diffusion,[86] which was revoked[87] in May 2025.

The U.S. has assumed the G20 presidency for 2026. One of the three themes[88] will be "pioneering new technologies and innovations" and many member governments are pursuing AI sovereignty to reduce dependence on foreign models and infrastructure. While the U.S. was active in shaping the Organisation for Economic Co-operation and Development (OECD) AI Principles during the first Trump administration, this year the United States has taken a more antagonistic posture toward multilateral engagement. In 2025, U.S. agencies were directed[89] to halt all engagement with the G20 summit in Johannesburg, and in early 2026, President Trump signed[90] a presidential memorandum directing the U.S. government to cease participation in and funding for 66 international organizations, including 31 U.N. entities and 35 non-U.N. bodies, and the National Security Strategy denounces "a network of international institutions...that explicitly seeks to dissolve individual state sovereignty." These actions risk weakening U.S. influence over the international rulemaking that shapes global AI development and adoption and could reinforce other countries' incentives to build sovereign alternatives.

China

Over the past decade, China has invested[91] heavily[92] across the AI stack[93] through state-backed funds (including an $8.2 billion AI fund for startups), local government AI labs, pilot zones, and private AI investment. The Chinese government combined the regulatory control[94] of its "Great Firewall" with industrial policies[95] that first supported national champions like Huawei, Baidu, Tencent, and Alibaba domestically, and then later extended this strategy internationally.[96] While these companies operate as nominally private entities, they are increasingly embedded in state industrial policy and subject to government steering.

China's 2017 New Generation Artificial Intelligence Development Plan[97] and successive five-year plans[98] have treated AI as a pillar of national development and a means of strategic competition. In response to semiconductor manufacturing equipment export controls, the Chinese government pursued greater self-reliance, investing in national supercomputing capacity, large language databases,[99] and efforts to train foundation models[100] with lower[101] compute budgets. President Xi Jinping has emphasized "self-reliance" and the construction of an independent AI ecosystem. Initiatives like the national computing power network[102] aim to pool computing resources, while the government has supported domestic efforts, such as Huawei's Ascend[103] chips to replace Nvidia graphics processing units (GPUs).

China's AI+ initiative[104] aims to increase[105] AI adoption[106] across China by identifying and funding specific AI application use cases across society. Some Chinese models, especially open large language models (LLMs), may have exceeded leading models in adoption.[107]

Foreign firms often have a difficult time releasing AI models to the Chinese market, because the state has

introduced binding requirements[108] for generative AI systems, including registration mandates, content filtering obligations, and auditing protocols that reflect broader ideological and national security objectives. Foreign firms seeking to operate in China must localize infrastructure,[109] partner with domestic entities, and comply with these rules, acceding to Chinese digital sovereignty.

Internationally, China's Global AI Governance Action Plan[110] promotes the idea to "jointly explore cutting-edge innovations in AI technology" and "promote technological cooperation." China is explicitly supportive of a U.N. role in AI governance driven by member states, including the establishment of an international institution[111] to govern AI. Even as China seeks to decouple from certain foreign dependencies, it continues to exert global influence through trade and technical standard setting. Chinese firms are active[112] in international bodies such as the International Telecommunication Union (ITU) and International Organization for Standardization (ISO), and Chinese-made hardware and software are widely used in emerging markets across Asia, Africa, and Latin America.

China's AI governance plan continues Chinese international development efforts through its Digital Silk Road (DSR) Initiative, part of the BRI, to provide other countries with Chinese-built or funded technology infrastructure. The DSR has funded projects[113] throughout the AI stack, including fiber-optic cables, satellites, 5G network infrastructure, data and cloud centers, and surveillance technologies. China has signed[114] DSR-related agreements with around 40 countries.

European Union

As an economic union, the European Union is a global power, collectively accounting for the largest share[115] of global GDP after the U.S. and China, but it lags well behind these leaders in the tech sector. The EU sought to lead in AI with its EU AI strategy[116] in 2018, which introduced the objectives of making Europe competitive in AI and ensuring that AI is based on European values. This is consistent with the EU's framing of digital innovation through the lens of fundamental rights and market failures reflected in major regulations such as the GDPR, Digital Services Act (DSA), and Digital Markets Act (DMA). This regulatory approach has enabled the EU to project influence extraterritorially through market access—the Brussels effect[117]—rather than technological market power.

The EU became the first major jurisdiction to introduce a comprehensive AI regulation with its AI Act,[118] which aims to promote the development and uptake of AI while addressing the ethical and societal risks through a risk-based[119] framework that conditions[120] market access on compliance with safety requirements and obligations based on fundamental rights. The AI Act relies heavily on standards development to frame compliance and, while the EU looks first to international standards bodies, the commission is promoting development of uniquely European standards to address fundamental rights obligations.

Notwithstanding its two-fold[121] approach to fostering an AI ecosystem of excellence and trust, the EU's regulatory ambition has not been matched with commensurate growth in its AI industry. Over 80%[122] of Europe's technology stack is imported, and while the commission's AI Innovation Package[123] aims to scale public-private partnerships and expand access to shared compute and datasets, implementation remains slow. A singular exception is ASML, due to its dominance[124] in the extreme ultraviolet (EUV) lithography machines global market needed for semiconductor manufacturing. ASML represents the kind of strategically essential and competitive supplier the EU aspires to foster, but it remains an outlier.

The EU's sovereign AI ambitions have been described as a "third way"[125] between U.S. and Chinese models. The strategy to accomplish this faces serious structural limitations, which include market fragmentation, lack of capital, and high energy costs, all contributing to the difficulty in scaling tech companies. Europe consumes[126] about 20% of the world's microchips but manufactures only 9%, mostly in mature technologies.[127] While the U.S. and China together account[128] for over 85% of global corporate R&D spending in software and internet technologies, EU firms account for just 7%. The EU remains constrained by a "middle tech

trap,"[129] maintaining strength in mature industries but lacking presence in cutting-edge cloud infrastructure, AI platforms, and foundational software ecosystems.

Recent initiatives pivot from rulemaking toward capacity-building and simplification of regulation. Launched as a multiparty initiative[130] in the EU Parliament in late 2024, the EuroStack[131] builds on previous efforts for European digital resilience such as the Critical Raw Materials Act,[132] the European Interoperability Framework,[133] and the European Digital Identity Wallet.[134] EuroStack proponents have called for[135] approximately 300 billion euros in investment over 10 years for pooled infrastructure and shared capacity rather than building a complete AI stack.

The commission's 2025 AI Continent Action Plan[136] sets out a scattershot capacity-building agenda for AI infrastructure, talent, and data. It includes a network of publicly funded AI factories to build large-scale AI data and compute capacity; planned AI gigafactories equipped with approximately 100,000 advanced AI chips for frontier-model training (estimated at 20 billion euros in public-private investment); and the InvestAI[137] initiative, which seeks to mobilize up to 200 billion euros in total funding for AI development (including to set-up the gigafactories). A forthcoming Cloud and AI Development Act aims to triple[138] EU data-center capacity within five to seven years, alongside various parallel efforts to expand data access for model training and sectoral applications. In addition, the Apply AI Strategy focuses on boosting AI adoption[139] across 10 priority industry sectors and the public sector.

A key feature of the foregoing initiatives is a growing reliance on open-source solutions. An upcoming open-source software strategy is expected to address[140] the economic and political "importance of open source as a crucial contribution to EU technological sovereignty, security and competitiveness." Some analysts suggest[141] open-source models lag proprietary model benchmarks by 15 months[142] on average, although that gap may lessen over time. In parallel to the commission's agenda, larger member states including France and Germany have driven an even more ambitious effort, which culminated in a summit in mid-November 2025 where the two governments proposed[143] an agenda blending regulatory simplification and fairer digital markets with open-source solutions for public administrations, the launch of a joint task force on European digital sovereignty, and a public-private initiative for the development of frontier AI[144] in Europe. These intergovernmental efforts, expected to produce first results during 2026, have been accompanied by announced business partnerships among Mistral AI, Europe's leading AI models developer, and key European players at other layers of the stack, such as ASML[145] and SAP.[146]

The prodigious body[147] of digital regulation, all rapidly enacted and recently implemented, has created a complex compliance environment, raising costs[148] and legal uncertainty in ways that some firms and policymakers argue[149] constrain innovation. Further, some point to[150] the inability of the AI Act to address technological innovation without frequent revisions. In response to many of these concerns, the commission's recent Digital Omnibus[151] proposal introduced targeted amendments to digital legislation, including the DSA, DMA, GDPR, and AI Act, to reduce compliance burdens to businesses and public administrations. This represents a shift in the EU's approach to technology policy based on regulation and market access.

STACK BUILDERS

Other jurisdictions are pursuing paths toward AI sovereignty by operationalizing control over specific functions of the AI stack, such as digital public infrastructure (DPI), sovereign data and compute, and selective participation in international standard-setting, rather than aligning fully with the U.S. or Chinese offerings or attempting to develop a fully independent AI stack. Stack builders are countries attempting to coordinate selected layers where they have leverage, while accepting continued dependence elsewhere.

India has elevated[152] DPI as a coordinating layer for AI sovereignty. India's 2023 G20 presidency[153] gave DPI global visibility subsequently reflected in the 2024 Global Digital Compact,[154] which recognized DPI as a driver of inclusive digital transformation while affirming that local needs would drive implementation.

The first Global DPI Summit[155] in October 2024 and the Quadrilateral Security Dialogue (the Quad)'s[156] (a grouping of the United States, India, Japan, and Australia) nonbinding principles[157] on DPI further embedded DPI as a cooperative, sovereignty-preserving approach, including for AI systems.

India's flagship DPI framework,[158] the India Stack,[159] exemplifies this model in practice. Framed as a set of open APIs and modular public digital goods, it encompasses the Aadhaar digital identity system, the Unified Payments Interface (UPI), DigiLocker for secure document storage, and the Account Aggregator framework for managing digital consent. Together, these tools enable what India describes as a presence-less, paperless, and cashless layer of digital society.

Although often described as "open," India Stack components are publicly governed systems for domestic use rather than globally open infrastructure. The government has made clear that DPI is not value-neutral but rather a tool[160] of public-interest infrastructure and of strategic autonomy and global influence. The IndiaAI Mission,[161] launched in 2024, aims to organize and curate national training data, develop[162] public-private partnerships to build foundational models, and make publicly funded AI infrastructure available for domestic use and regional export. Although government officials have downplayed[163] direct competition with private firms, the plan signals intention to anchor[164] AI development in publicly governed data and infrastructure. In parallel, India has taken steps to shore up other layers, including India's National Critical Mineral Mission,[165] which aims to facilitate mining of 30 critical minerals by 2030.

After hosting the 2023 AI Safety Summit,[166] the **United Kingdom** launched the AI Security Institute[167] as a public-sector capability for safety testing and research, now operating within the Department of Science, Innovation, and Technology (DSIT). In parallel, DSIT established a Sovereign AI Unit[168] with a mandate to strengthen U.K. AI capabilities for economic growth and national security, backed by up to 500 million pounds. The U.K. has also expanded public compute access through the AI Research Resource[169] for researchers, academia, and small- and medium-size enterprises (SMEs). These initiatives build on the U.K.'s strong domestic AI capacity: The U.K. hosts more than 85,000 AI professionals[170] and ranks third[171] globally in AI research output. Together, the level of talent and research productivity strengthen the U.K.'s credibility in AI safety, standards, and evaluation, even while remaining structurally dependent on foreign semiconductors, hyperscalers, and frontier models.

Japan has used international process leadership to shape governance norms, most notably through the G7 Hiroshima AI Process[172] under its 2023 presidency, and its long-running push for Data Free Flow with Trust.[173] In parallel, Japan has pursued a more material form of AI sovereignty centered on domestic compute and infrastructure. The government has made large-scale public investments in national research compute through the AI Bridging Cloud Infrastructure[174] (ABCI), now expanded as ABCI 3.0,[175] explicitly framed[176] as sovereign, in-country compute capacity for AI R&D. On the model side, Japan has demonstrated an ability to translate this infrastructure into domestic capability, including the training of Fugaku-LLM[177] on largely Japanese public infrastructure. Under the Economic Security Promotion Act,[178] Japan's Ministry of Economy, Trade and Industry (METI) has designated "cloud programs" as specified critical products and subsidized domestic GPU cloud capacity to secure in-country compute resources and strengthen the resilience of AI and cloud services for Japanese users. METI and the Ministry of Internal Affairs in Communications also compiled AI Guidelines for Business,[179] recommending risk mitigation measures for generative AI.

South Korea has used its hardware advantage in memory chips paired with a state-backed push for Korean-language foundation models and domestic compute buildout. In 2025, the Ministry of Science and ICT selected five teams for a Sovereign AI Foundation Model[180] project to build sovereign AI foundation models. At the same time, SK Group and Amazon Web Services (AWS) announced[181] $5.1 billion to build an AI-focused data center in Ulsan, and SK Hynix plans to invest[182] about $12.9 billion in an advanced chip packaging plant.

South Korea's AI Basic Act[183] will be the one of the world's first comprehensive AI legal frameworks to go into effect. This law follows the EU AI Act in establishing a risk-based regulatory regime covering high-impact AI systems and generative AI. The Personal Information Protection Commission (PIPC) released its Guidelines for Personal Data Processing for the Development and Use of Generative AI in August 2025, clarifying legal standards[184] for data use in generative AI training and deployment.

LAYER SPECIALISTS

Layer specialists concentrate public investment and policy attention based on existing strengths on one or two leverage layers, rather than attempting vertical integration. These approaches prioritize based on existing strengths, such as investment capital, access to talent, government agility, existing industries, or access to raw materials. These countries typically specialize in either upstream components, AI system development, or governance and research functions.

Upstream shapers

The **United Arab Emirates** is using open-source diffusion as a diplomatic and soft-power tool. Central to this strategy is G42, the UAE's primary state-aligned AI conglomerate.

The 2024 Microsoft-G42 partnership[185] illustrates this hybrid sovereignty model.[186] Under the deal, the UAE retains ownership of physical infrastructure through G42, while Microsoft has operational control, cloud services, and compliance obligations under an Intergovernmental Assurance Agreement (IGAA). This arrangement allows the UAE to scale advanced compute domestically but cedes control to a U.S. company on many governance, compliance, and security decisions. Similar dynamics are visible in Stargate UAE,[187] a planned multi-gigawatt AI campus backed by Emirati capital and energy but reliant on U.S. firms for chips, models, and system operations, reinforcing the UAE's role as an infrastructure hub rather than a full-stack AI producer.

State-backed capital vehicles further reinforce this strategy. MGX,[188] an Abu Dhabi-based AI investment platform with state-owned investment firm Mubadala and G42 as founding partners, targets AI infrastructure, semiconductors, and enabling technologies globally, positioning capital allocation itself as a lever of sovereignty and geopolitical influence.

At the model layer, the UAE has pursued both symbolic and practical initiatives. Falcon,[189] developed by the Technology Innovation Institute, and the Arabic-focused Jais[190] model from Mohamed bin Zayed University of Artificial Intelligence (MBZUAI) and G42's Inception, serve different purposes: Falcon's open-weight releases function as soft-power and ecosystem-building tools, while Jais is more directly "sovereign" in practice, addressing Arabic-language capability gaps and public-sector use cases.

Other countries with leading positions in upstream components such as raw materials and energy include Indonesia, South Africa, and Sweden (see Appendix A).

System and institution shapers

In **Canada**, sovereignty is a driving factor for state-supported AI development. The federal government is lowering barriers to compute access, particularly for start-ups and researchers, and has positioned open-source AI as a national priority. These efforts are anchored in the Toronto-Waterloo corridor's dense research and commercialization ecosystem, reinforced by Pan-Canadian AI Strategy phase two funding,[191] which continues to support the country's three national AI institutes (Vector, Mila, and Amii) while prioritizing commercialization and adoption. Complementing this research base, the Scale AI supercluster[192] translates AI research to applied industrial capabilities. In parallel, Canada's critical minerals strategy[193] highlights the country's access to rarer minerals such as cobalt, graphite, lithium, and nickel, working to strengthen their position in upstream layers.

Similarly, **Australia's** critical minerals strategy[194] aims to "build sovereign capability in critical minerals processing" while also creating supply chains through international partnerships.[195] Upstream layers like mineral processing and semiconductor tools can help

shape bargaining power and long-term resilience but may not have the same direct impact on model autonomy in the near future.

Germany has a strong industrial base. Its national AI action plan[196] emphasizes competitiveness through research, development, and diffusion of AI into industry, and its manufacturing base (Industrie 4.0)[197] creates a natural pathway for sovereignty-by-adoption in production systems even absent a dominant domestic frontier-model lab. As a central EU member, Germany also shapes how Europe operationalizes AI governance through implementation capacity and industrial-policy alignment.

Singapore has focused on building sovereign AI models with data and training to better represent domestic culture and languages. Singapore's SEA-LION project,[198] launched[199] with a government investment of roughly $52 million, aims to develop multilingual models in Southeast Asian languages. SEA-LION is not intended to rival frontier foundation models, but it is intended to ensure that high-impact public-sector applications are trained on linguistically and culturally representative[200] data.

Beyond model development, Singapore is positioning itself as a governance and testing hub: AI Verify[201] provides a practical testing framework for responsible AI, and Singapore's AI Safety Institute[202] is pursuing joint testing and technical collaboration with counterpart institutes. This coordination role is intertwined with regional infrastructure realities; data-center expansion serving Singaporean demand is increasingly sited across the border[203] in Johor, Malaysia.

These countries are case studies of how layer specialists are approaching AI sovereignty strategies, but this is not an exhaustive list of countries specializing in a few AI stack layers. Other examples include **France's** high number[204] of notable[205] machine learning models, **Taiwan's** dominance in semiconductor manufacturing, and several European states, including **Spain**, **Luxembourg**, **Ireland**, and **Finland**, who demonstrate high levels[206] of AI discussion at the national government level, as well as through public AI investments and patents.

OTHER COUNTRIES

For other countries, sovereign AI is often linked to regional integration and economic transformation. Rather than replicating large-scale model development, many African countries are focusing on sovereign data centers, interoperable DPI, and cross-border digital trade protocols. Countries such as **Nigeria** and **Kenya** have each emphasized[207] localized AI infrastructure and training datasets, while others, like the **Democratic Republic of Congo**, are investing[208] in mineral-based value chains to support upstream AI infrastructure.

Brazil is one example of increased AI deployment. The government has taken a "brownfield"[209] approach to AI deployment, modernizing legacy public-sector systems to be interoperable rather than building a new stack. Its central innovation is Pix, a real-time payments system developed by the Central Bank that now has roughly[210] 172 million users and has processed[211] over $166.2 billion Brazilian reais in one day of transactions. In June 2024, Brazil codified its DPI vision in Presidential Decree No. 12.069, defining DPIs as "cross-application structuring solutions"[212] built for the public interest and capable of integrating services across both public and private sectors. Reflecting Brazil's federal structure, implementation often occurs through cooperation between national-level coordination and state-level experimentation. Brazil's 2025 PBIA (Plano Brasileiro de Inteligência Artificial)[213] frames sovereign AI as a national capacity-building program through 2028, with a stated investment of roughly 23 billion Brazilian reais and a dedicated infrastructure-and-compute axis that includes ambitious upgrades to national supercomputing capacity.

International cooperation also helps facilitate better coordination on critical mineral supply chains. The Quad also launched the Quad Critical Minerals Initiative[214] in 2025 to diversify supply chains. The U.S. has also signed several bilateral[215] partnerships[216] centered[217] on critical[218] minerals.[219] The African Union's Digital Transformation Strategy envisions[220] digital infrastructure as key to Agenda 2063 development goals, while the African Continental Free Trade Area (AfCFTA) positions cross-border data flows as foundational to a regional innovation economy.

PART II.
STRATEGIES FOR AI SOVEREIGNTY

Why absolute AI sovereignty is impossible

Assessing approaches to AI sovereignty requires looking at AI not as a single product but as a "stack" of interconnected layers that enable a complete system. These layers—physical input including minerals, energy, and water; compute hardware such as semiconductors; networks; digital infrastructure including cloud and data centers; data assets; models, applications, and crosscutting enablers including talent and governance—jointly determine capability and risk.

Table A treats AI sovereignty as a set of layered constraints, leverage or choke points, and opportunities. The columns show how dependencies compound across layers of the stack, while the rows show how absolute control is structurally infeasible. Governments should assess their competitive advantages and take a clear-eyed view into vulnerabilities from varying levels of concentration across the AI stack.

These layers are also transnational.[221] Because the lower layers of the AI stack, such as advanced chips and frontier foundation models, are dominated[222] by a small number of highly capitalized actors, opportunities for broad-based innovation and national sovereignty are structurally limited at those levels. A disruption or choke point in one layer, such as a shortage[223] of specialized chips, causes risk[224] through the entire system and gives certain countries leverage over others. In contrast, the upper layers of the stack, particularly applications and domain-specific systems, offer far greater scope for differentiation, competition, and local value creation. These layers allow governments, firms, and institutions to tailor AI to national priorities, regulatory frameworks, languages, and sectoral needs, making applications the primary locus where most countries can realistically exercise AI sovereignty and capture economic and societal benefits.

As one of the authors (Kerry) has previously argued,[225] the key inputs to AI development are intrinsically subject to economies of scale, and many inputs (especially R&D) are products of collaboration across national boundaries. Accordingly, coordinated sovereignty strategies may risk duplicative investments and fragmented supply chains rather than resilience.

Not all layers of the AI stack are equally relevant for managing sovereignty. Their significance depends in part on a country's position in the global economy and its level of digital development. In wealthy, advanced digital economies, access to advanced hardware and compute capacity has emerged as essential to AI sovereignty, but for countries on the other side of the digital divide, network infrastructure and connectivity can be critical, not only for access to AI systems, but also the availability of domestically relevant data.

TABLE A

The AI Stack: layered dependencies, concentration points, and mitigation levers

Layer	Key jurisdictions, in order of strategic leverage or concentration	Concentration risks	Mitigation strategies
Physical inputs			
Critical minerals	Australia and Chile (lithium); China (processing, refining, and rare earths mining); Democratic Republic of the Congo (cobalt)	Extraction is concentrated for several critical minerals, while downstream processing and refining are heavily concentrated in China, creating exposure to export controls, price volatility, and geopolitical leverage.	Diversify supply toward allied jurisdictions; strategic stockpiling; recycling and substitution; investment in alternative materials.
Energy	Canada, EU, Nordic states, United States; Middle East (emerging hubs)	AI infrastructure requires reliable, low-cost power at scale. Permitting delays, grid congestion, and local opposition constrain expansion in established markets, while emerging hubs may introduce new geopolitical dependencies.	Grid modernization and expansion; diversified energy mix; colocation with generation capacity; long-term power purchase agreements.
Water	Regionally variable; Middle East and parts of Asia (desalination capacity)	Water-intensive cooling constrains data-center siting and can generate environmental and political opposition in water-stressed regions. Desalination capacity is geographically concentrated, creating secondary dependencies.	Deploy advanced cooling technologies; water-efficient infrastructure; siting strategies aligned with water availability; desalination investment where required.
Digital infrastructure			
Compute hardware	United States (design and IP); Taiwan (advanced fabrication); South Korea (memory, packaging); Netherlands and Japan (equipment); China (legacy nodes)	Single-firm and single-country choke points in advanced lithography, leading-edge fabrication, and high-bandwidth memory, combined with long lead times and export-control exposure, create systemic supply risk.	Diversify fabrication and packaging capacity across allied jurisdictions; support alternative architectures; strategic inventory buffers; domestic equipment capability where feasible.
Digital infrastructure (cloud and platforms)	United States (hyperscalers); China (domestic platforms); EU, U.K., Japan	Vendor lock-in to dominant cloud providers creates pricing and jurisdictional exposure. Integrated tooling ecosystems raise switching costs and operational dependency.	Adopt multi-cloud strategies; interoperability requirements; open tooling; contractual safeguards (recognizing limits under geopolitical stress).
Networks and connectivity	United States, EU, China, South Korea, Japan, Sweden	Risks include subsea cable fragility and exposure to disruption or interception; vendor concentration in network equipment markets; and geopolitical contestation over telecommunications infrastructure.	Physical and routing redundancy; vendor diversification; hardened protocols; monitoring and incident response capacity.
AI models and capabilities			
Software frameworks and technical standards	United States (major machine learning frameworks); China (domestic frameworks)	Framework and ecosystem dominance create path dependency. Tight hardware–software coupling increases switching costs. Standards processes may be shaped by dominant ecosystem actors.	Support interoperable frameworks; invest in open standards; participate in international standards bodies; develop abstraction layers to reduce lock-in.
Data assets	United States, China, India (scale); EU, U.K, Canada, Australia (governance and quality)	Proprietary dataset control by large platforms and legal uncertainty around training data reuse create risks; localization requirements fragment access. Scale advantages favor large, digitally active populations.	Public-sector data release with clear licensing; trusted data-sharing infrastructure; curated domestic datasets; legal clarity on training data use.
Models and training capacity	United States and China (frontier scale); U.K., France, South Korea, India, UAE (emerging)	Frontier-scale training and evaluation capacity is concentrated in a small number of firms and jurisdictions. Independent access to evaluation and safety-testing infrastructure is limited.	Invest in frontier-model development where resources allow; otherwise focus on open-weight models, fine-tuning, and domain adaptation; build independent evaluation capacity.
Application and deployment			
Applications and deployment	Broadly distributed; United States and China lead in scale; U.K., South Korea, India, EU active by sector.	Downstream actors inherit upstream concentration risks. Dependence on external models and platforms limits operational autonomy. Skills and procurement gaps constrain effective deployment.	Integration capacity-building; procurement frameworks emphasizing substitutability; sector-specific adaptation; vendor diversification.

TABLE A (CONTINUED)

The AI Stack: layered dependencies, concentration points, and mitigation levers

Layer	Key jurisdictions, in order of strategic leverage or concentration	Concentration risks	Mitigation strategies
Talent and research (crosscutting)			
Talent and research (crosscutting)	United States (primary hub); China, U.K., Canada, EU, Israel	Advanced AI research and engineering talent is concentrated in a small number of institutions and firms. Compensation and compute access differentials drive talent concentration.	Competitive research environments; targeted immigration pathways; domestic research investment; industry–academia partnerships.
Governance and regulatory frameworks (crosscutting)			
Regulatory frameworks	EU (risk-based framework); U.S. (sectoral and voluntary approaches); China (algorithm and content regulation)	Regulatory divergence increases compliance complexity and fragmentation. Compliance burdens may advantage large incumbents. Early regulatory models may become de facto benchmarks.	Active engagement in standards development; compliance infrastructure investment; regulatory sandboxes; international coordination where feasible.

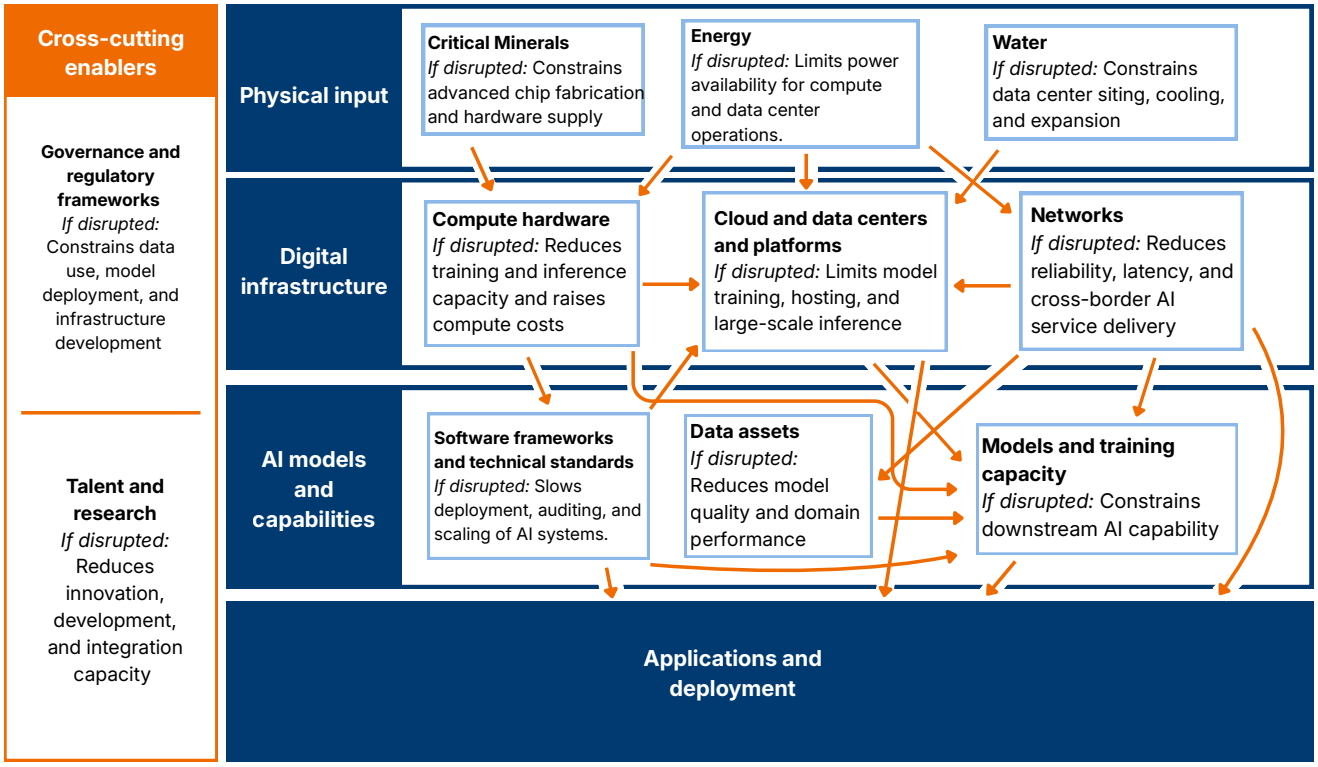
BROOKINGS

SOURCE: Authors' determinations using data from the Global Critical Minerals Outlook (May 21, 2025), International Energy Agency, Electricity Mix, Market share for logic chip production, by manufacturing stage, and Cumulative number of large-scale AI systems by country since 2017 (2021-2024, Our World in Data), Stanford AI Index Report (2025, Stanford AI Human-Centered Artificial Intelligence), Data Centers Around the World (May 2021, United States International Trade Commission), Broadband statistics (2024, OECD), Safeguarding Subsea Cables (2024, Center for Strategic and International Studies), GitHub Repositories (January 2026, GitHub), Distribution of Authors per Country (August 2024, Internet Engineering Task Force), ICT service exports (BoP, current US$) (2024, World Bank), Individuals using the Internet (2025, International Telecommunication Union), and Wikimedia statistics (2025, Wikimedia).

NOTE: The table presents layers separately, but strategic planning should account for cross-layer dependencies. Governance frameworks and talent are treated as cross-cutting layers affecting all stack levels.

FIGURE 2

Interdependencies across the AI stack[226]



BROOKINGS

SOURCE: Authors' qualitative determinations. For more information on determinations, see Appendix B.

NOTE: Figure 2 maps primary dependency paths related to sovereignty risks. Cross-border concentration increases as you move down the stack. Text in each layer shows consequences of disruptions at that layer. Disruptions at upstream layers—such as physical inputs or digital infrastructure—propagate downward, constraining model development and, ultimately, application deployment. Governance and talent function as crosscutting enablers rather than linear dependencies.

Figure 2 shows dependencies and consequences of disruption in each layer of the stack.

For each layer of the stack, governments should assess four questions:

1. **System criticality**: If this layer were disrupted or constrained, would it create a binding bottleneck for the rest of the AI stack?
2. **Near-term policy tractability**: Can a government meaningfully improve its strategic position in this layer within a realistic policy timeframe (e.g., 3–5 years)?
3. **Market structure and substitutability**: Does this layer offer genuine supplier or architectural alternatives, or is it characterized by single-firm or single-jurisdiction dominance?
4. **Risk management under dependency**: Where foreign reliance is unavoidable, can exposure be reduced through governance mechanisms, diversification strategies, or technical and architectural design choices?

Why managed interdependence

Taken together, these patterns point to a structural conclusion. Because advantages and vulnerabilities are distributed unevenly across the stack, and because most of the critical layers are intrinsically transnational, assembling a complete AI stack is a near impossibility. Policymakers need to be strategic in how they pursue AI sovereignty as a means to shape interdependence across the stack. As Marc-Étienne Ouimette noted[227] in a Brookings-Centre for European Policy Studies (CEPS) Forum for Cooperation on AI (FCAI) public forum on "The American AI stack and the world," sovereignty is not about chasing complete domestic production and control over the entire AI stack; rather, it involves focusing on those areas that a government can realistically influence or control. Doing so calls for careful consideration of capabilities and vulnerabilities and the resulting comparative advantages and disadvantages they create.

To accomplish this, policymakers need to make selective strategic choices, which "should be sector-specific[228] and support a diverse range of model types, grounded in real-world use cases and patterns of adoption." In practice, this often means pursuing a mix of approaches that prioritize near-term, feasible investments—such as applications and deployment—while addressing longer-term objectives that can include targeted reductions in dependencies and vulnerabilities where a country has, or can plausibly develop, comparative advantage.

In this vein, governments are designing sovereignty strategies to manage specific vulnerabilities across layers of the stack. A non-exhaustive list of sovereign policy strategies[229] includes supplier diversification, alliances and partnerships, interoperable technologies, investments in open models, participation in standard setting, industrial subsidies, data-localization laws, regulatory oversight, auditing and certification regimes, public procurement strategies, and export controls. The choice and combination of these instruments vary across jurisdictions, creating a variety of sovereign AI approaches based on jurisdictional motivations and capabilities. Some of these approaches may not take adequate stock of capabilities and may be too scatter-shot or capital-intensive

Many governance approaches lean heavily on domestic talent to facilitate R&D across the stack. Several countries—in both advanced economies like those in Europe as well as in emerging economies—are confronting "brain drain," where talent emigrates due to higher incentives or opportunities elsewhere. Talent is widely distributed, but highly stratified by market, and mobility often depends on education and publication opportunities, as well as ease of immigration pathways. By building talent infrastructure, such as research centers[230] and accelerators,[231] facilitating easier immigration pathways, investing in education, and incentivizing R&D, countries can work toward a domestic talent pipeline.

Open-weight models can also help mitigate mobility challenges, allowing multiple global collaborators to contribute to projects regardless of location and offer shortcuts to development of systems that can service local communities. Open-weight models fill a different role than proprietary models. On average, 70% of model usage[232] is from proprietary models, which will continue to dominate enterprise functions and national security or sensitive usage. However, open-weight models can bring[233] more groups into the market that cannot otherwise afford closed-weight models.

Managed interdependence is a strategy not only for small-to-medium-income countries. Even the AI superpowers have vulnerabilities and disadvantages and can find synergies in pooling their capabilities with those of other countries. In the next subsection, we look at how the U.S. and China are approaching AI sovereignty and how other countries are responding.

Putting managed interdependence into practice

FOR THE UNITED STATES: UPHOLDING AI LEADERSHIP

Currently, the United States is the recognized leader in AI across multiple layers of the AI stack. Rapid innovation and massive private investment have given U.S. firms a first-mover advantage in foundation models. This position provides a strong grip on the domestic market for AI systems and has enabled U.S. AI firms to provide highly competitive offerings in other markets and establish a large global footprint. The AI Action Plan[234] seeks to leverage both of these positions, the former with policies to support innovation and adoption and the latter with a plan to export the "full AI technology stack" to allies and partners.

This competitive position nevertheless faces challenges. U.S. AI firms now face rising competition from numerous smaller, more efficient open-weight or open-source models like China's DeepSeek and others. These models are attractive not only to nations without large-scale information technology infrastructure, but also in the U.S. market. In aggregate, on the Hugging Face open platform, there have been 818 million downloads[235] of Chinese models, compared to 601 million downloads of U.S. models, and 141 million downloads of EU models—potentially reflecting[236] the larger number of Chinese open models. Between August 2024 and August 2025, Chinese open models comprised[237] 17.1% of all Hugging Face downloads, surpassing the 15.8% of downloads from U.S. developers. The various reactions against U.S. AI technology discussed earlier in this report may make these alternatives more attractive as paths to AI sovereignty movement.

To overcome these currents, the U.S. will need to align the AI Action Plan and American AI Exports Program with a strategy of managed interdependence that pairs carefully chosen export agreements[238] with sustained capacity building. Proclaiming American "dominance" in AI is unlikely to reassure allies and customers already concerned about overexposure to U.S. technology and who see the U.S. as a "hegemon."[239] This posturing risks ceding soft power and future markets to China's integrated development partnership offerings.

Moreover, promoting AI as "the full American AI stack" may be perceived as a one-size-fits-all, take-it-or-leave offer. This may not have been the intention; Michael Kratsios, director of the White House Office of Science and Technology Policy and a principal author of the AI Action Plan, explained[240] that the concept emerged in reaction to China's success in exporting turnkey telecommunications systems, like Huawei. However, general-purpose AI systems are nowhere near as fungible as telecom systems, and most countries neither need nor can absorb every layer of the AI stack. AI exports will therefore need to be modular and fine-tuned to local needs and languages (just as they are for enterprise applications) and supported[241] by development-oriented engagement, including training, capacity building, and the provision of compute infrastructure, for the United States to remain a credible long-term partner.

In this context, managing interdependence requires working with governments and stakeholders to scope concrete needs in partnership[242] with participants in the export program. The aim should be to offer specific solutions, such as targeted compute access, sector-specific applications, or governance and assurance capacity, rather than a complete stack. During a Brookings public event[243] on AI, Pablo Chavez, founder and principal of Tech Policy Solutions LLC and an adjunct senior fellow at the Center for a New American Security, referred to "shared sovereignty," citing as examples the U.S.–UAE and U.S.–Saudi Arabia joint venture agreements for the joint construction of data centers by U.S. companies powered by advanced semiconductors. This example demonstrated that the AI export plan operates to promote interdependence, expanding U.S. markets by tailoring offerings to needs and aspirations on the ground and providing players there with agency in the AI solutions deployed.

U.S. diplomatic, commercial, and intelligence capabilities can help to identify local needs where such

targeted interventions would meaningfully reduce partner vulnerabilities. This approach aligns AI exports with development and capacity-building objectives rather than creating new forms of dependencies. The Trade and Development Agency has funding authorized[244] by the recent National Defense Authorization Act that could fund AI projects that can achieve such an effect.

The leading U.S. AI systems have strengths that can be adapted for these purposes. As recent advances in AI distillation demonstrate, the wide array of data used to train foundation models can be used for additional training and fine-tuning. U.S. providers with experience in adapting AI to a variety of enterprise situations and languages may have an advantage in adapting AI to Indo-European languages and others. For example, Microsoft is in the process of expanding the applicability of its LLMs to European languages[245] with less of a digitized corpus than more widely known and translated languages. Most major U.S. developers also offer small or specialized models; six of the 10 top models under 12 billion parameters downloaded[246] from Hugging Face are from U.S. organizations. In addition, the U.S. models have been developed independently of the state, in contrast to Chinese models that are chilled by content controls and therefore aligned to benchmarks[247] "created by removing highly sensitive questions that tend to be censored." These useful selling points provide a structural advantage.

The U.S. also has effectively begun to employ managed interdependence by recognizing persistent vulnerabilities in upstream AI inputs, particularly in the critical minerals supply chain and energy generation. U.S. reliance[248] on imports for mining and processing critical minerals remains near-total, a risk illustrated starkly by the abrupt impact of China's export controls[249] on rare earths and equipment for advanced battery manufacturing. Although some restrictions were later suspended, others remain in force[250] and could easily be reinstated now that China has seen how its leverage succeeded. The U.S. faces additional risks with its reliance[251] on Taiwan for advanced chip fabrication as well as the manufacturing[252] of a wide variety of computer components there, in mainland China, South Korea, and Japan.

In response, the U.S. has induced Taiwan's Taiwan Semiconductor Manufacturing Company (TSMC) to site[253] a chip fabrication plant in Arizona. It has also prioritized domestic mineral production and funded mining and processing companies with equity stakes, among other measures. Diversifying supply chains will require collaboration with like-minded partners, as the Trump administration has done through minerals agreements with Cambodia, Japan, Malaysia, and Thailand to reduce reliance on China and establishing a critical minerals partnership with the Quad allies. Examples include partnerships with the Netherlands on semiconductor equipment, Canada on energy, others for critical minerals, and Japan and South Korea and additional partners on advanced components and memory chips. In June 2025, the G7 energy ministers adopted a Critical Mineral Action Plan[254] aimed at diversifying responsible production and announced a first round of 26 investments over four months. This progression of international agreements shows both urgency and pragmatism in managing interdependence in the AI supply chain. These are nonbinding agreements; however, many of them are "frameworks" and promises of future investment rather than solutions in the works. Making them bear fruit will require sustained diplomacy and execution.

The White House AI Action Plan prioritizes[255] expanding energy generation and energy grid improvements. Other administration policies work against these objectives. For example, blocking wind and solar projects when these sources have accounted for 132.7% of the net increases[256] in U.S. generation over the past 10 years, displacing other energy sources. In addition, U.S. policies toward Canada, a key neighbor, including a 10% tariff[257] on energy imports, have had an impact on a major source of electricity supply and have led to significant reductions[258] in power transmissions from Canada. Continuation of such policies will increase costs to U.S. energy plants. The U.S. should return to an "all-of-the-above" energy strategy.

The U.S. has the presidency of the G20 in 2026. We have noted previously[259] that the G20 is a difficult venue for substantive policy development on AI given the differing interests of its makeup. The U.S. will face added obstacles coming off its boycott of the

Johannesburg G20 meeting a few months prior, and its ongoing contention[260] with other members and international forums. Nevertheless, the presidency might afford some opportunity to reframe AI sovereignty around interoperability, modular exports, and partnerships for "digital solidarity"[261] as part of a theme on "pioneering new innovative opportunities," while signaling a more customer friendly approach to partner countries at different stages of digital development.

FOR THE EUROPEAN UNION: CARVING OUT A SPACE

The EU has made technological sovereignty a key element of its digital strategy and has set in motion the initiatives discussed above across the AI stack, including the proposed Chips Act 2.0, the proposed Cloud and AI Development Act, AI (giga)factories, and Apply AI Strategy, with parallel efforts driven by large member states like the joint task force on European digital sovereignty. After the U.S. and China, the combined EU is the third largest investor[262] in AI.

Many of these initiatives appear promising and complementary, but some may be duplicative or follow disparate timelines, and, in many cases, the approach is insular (e.g., increasing domestic production and ring-fencing markets). To strengthen its strategy, the EU should ensure disciplined investment and measured implementation, while emphasizing managed interdependence via strategic partnerships, which may need to be part of a more gradual approach to reducing dependencies. All of this can build resilience without trying to replicate the entire AI stack.

On critical raw materials, the EU must pursue reasonable and pragmatic solutions through international alliances and partnerships, such as the EU-Mercosur trade agreement[263] (in progress)[264] and the finalized free trade agreement[265] with India. Like-minded countries, including Canada, Japan, Australia, Norway, and the U.S., increasingly emerge as key partners to help the EU secure access to raw materials at the same time as ramping up domestic production over several years. The EU International Digital Strategy,[266] launched in June 2025, should be complemented by data-driven research to identify optimal partnerships based on technological complementarities. It aims to consolidate a network of digital partnerships and dialogues to strengthen cooperation on emerging technologies, such as AI, semiconductors, and quantum. While not exclusively focused on critical raw materials, this network creates spaces to explore supply-chain resilience as part of cooperation on semiconductors and secure technology infrastructure.

Discriminating compute infrastructure investment decisions will be critical to the EU's future AI competitiveness. One important aspect is the site location: Current build-outs do not consistently align[267] with AI excellence hubs or locations with abundant, low-cost energy supplies. The EU should resist spreading compute infrastructure across all member states and instead concentrate deployments where conditions enable low-cost, high-impact capacity tailored to priority use cases. In deploying compute infrastructure, the EU should adopt a hybrid approach to sovereignty that may make use of foreign world-class solutions and that preserves operational interdependence. This requires supplier diversification, interoperability, and portability to enable open solutions at higher layers of the stack. Compute investments should also avoid overreliance on a single chip architecture (e.g., GPUs) by exploring alternatives that may better fit forthcoming industrial applications identified in the Apply AI Strategy.

Across the AI stack, the EU should articulate concrete sovereignty criteria to guide policy development and public procurement. The Tech Sovereignty Catalogue,[268] an initiative by EuroStack proponents, can help operationalize this approach. The Catalogue is a growing register of European-owned digital solutions, characterized by their stack layer and positioned[269] as "market-ready, sovereign by design, and meeting high European standards." To realize its full potential, the Catalogue would benefit from greater transparency about eligibility and assessment processes, avoiding suggestions of full-stack requirements, and creating a formal feedback loop with ongoing policy initiatives. In general, sovereignty criteria should cover ownership structure, data jurisdiction, operational transparency, and control over infrastructure, while making room for strategic international collaboration. To create demand for domestic

capacity at critical control points like the deployment layer, the EU should use public procurement to de-risk investment where needed and accelerate adoption of technologies compatible with European standards, including for interoperability and sustainability.

If sovereignty is framed as freedom of choice—grounded in interoperable solutions and responsible, human-centered AI—a viable still-to-be-implemented[270] initiative is the Digital Commons European Digital Infrastructure Consortium.[271] Launched in December 2025, the consortium brings together France, Germany, the Netherlands, and Italy and is supported by a growing group of candidate members and observers. The initiative aims to coordinate public administrations, open-source communities, and companies to develop open cross-border digital solutions. It can be linked to efforts under the EU's International Digital Strategy, so that resulting solutions could serve as the foundation for co-development projects[272] with aligned partners. The strategy could help advance "digital solidarity" in cloud computing, where EU dependencies are acutely consequential for its AI progress, by engaging with the U.S. on long-standing concerns over data flows and vendor lock-in, motivated by mutual economic gains; such progress, as optimistic as it may sound, can enhance AI sovereignty without a compromise to competitiveness.

While the expansion of a competitive compute and cloud infrastructure can happen gradually, near-term progress for the EU will likely require a focus on specialized models and applications. A similar key intergovernmental initiative is the AI IPCEI[273] (Important Project of Common European Interest), which is aimed at strengthening EU leadership in industrial AI applications and attracts broad member state interest, potentially more agile in its governance and delivery than the EU-level agenda. The initiative should fully leverage synergies with the Apply AI Strategy and be complemented with public awareness campaigns to foster informed adoption and trust. To ensure model adoption, this layer of the stack requires a focus on technical reliability, which should therefore be an R&D priority. Notably, breakthroughs in reliability—which is an ongoing research challenge—offer Europe potential for leadership not only in applications but in foundational models that may be needed to ensure long-term sovereignty. This implies a dual-track approach: prioritizing specialized and application-level innovation in the near term, while sustaining investment and coordination toward frontier foundational models over the medium- to long-term.

The EU's success in AI must rest on a robust talent strategy to nurture and retain European expertise. Talent is the region's outstanding AI asset: 20.9%[274] of AI publication citations in 2023 list European authors, placing it behind China and ahead of the U.S., showing that the continent's universities graduate highly talented engineers and computer scientists. But a lack of opportunities leads to significant talent migration, especially to top foreign AI companies or to scaling up EU startups in the U.S. To retain talent, the EU's public and private capital investment in AI sovereignty needs to include funding for startups and scaleup. The EU is piloting a "Startup and Scaleup Strategy"[275] but needs to ramp up its investment, possibly through a pan-European sovereign technology fund modeled on Germany's. Realizing its full promise ultimately depends on implementing larger reforms in capital markets, as recommended in the Draghi report.[276] This should encompass EU-wide opportunities for startups to raise risk capital. On the side of AI adoption, there is a great need for upskilling across government, industry, and the education sector; programs should emphasize purposeful deployment and public-interest AI (e.g., by including knowledge on how to develop and leverage open-source AI effectively).

European solutions are unlikely to flourish without a more conducive regulatory environment, especially to leverage the power of data. The EU has some significant advantages in data, with national repositories of health data and established networks for trusted pooling of information in sectors like banking. The commission should implement and, where appropriate, simplify, and improve its digital legislation, in ways that enable innovation without weakening protective measures. This should include publishing AI Act guidance pending finalized harmonized standards, including interim guidance for high-risk systems to act as official presumption of conformity; and considering enforcement delays, to enable standards completion,

with a fixed deadline rather than—as proposed[277] in the commission's Digital Omnibus—a flexible delay with an upper bound. Targeted changes in data governance will be equally worthwhile, especially given the key role of data in the Apply AI Strategy. The proposed revision of the GDPR in the Digital Omnibus—which would enable the use of personal data for AI training as a "legitimate interest," subject to protective measures—is a promising effort. GAIA-X's shift from cloud services to data pools for researchers, SMEs, and smaller member states, represents another step toward unlocking access to data.

Commission President Ursula von der Leyen has declared[278] that the EU is seeking "independence." Given the EU's comparative position in AI and the extent to which its AI stack relies on U.S. products, its sovereignty agenda requires a policy mix that gradually reduces dependencies, safeguards Europe's key assets (e.g., world-class network infrastructure, data, talent, and intellectual property), and builds partnerships with other countries that support managed interdependence. Through sustained engagement in international initiatives and standard-setting bodies, the EU can leverage its norm-setting influence to accelerate co-development with aligned partners; success would strengthen the global AI ecosystem by providing integrated and trusted AI infrastructure and services. For example, France taking up the G7 presidency in 2026 represents a channel to translate sovereignty initiatives into agenda-setting power within a body that has launched several international initiatives around AI over the past decade.

FOR CHINA: MOUNTING A CHALLENGE

China has advantages that make it a rival to the U.S. for AI leadership. Its government moved early to invest heavily[279] in AI R&D and ramped up this investment in its current five-year plan.[280] China's large population produces an abundance of homogenous data and of science and technology researchers (now being onshored with the drastic reduction of foreign study in the U.S.)—advantages that AI pioneer Kai-Fu Lee predicted[281] with significant accuracy would enable rapid advances in data-intensive fields like computer vision, autonomous cars and drones, and payments.

China comes the closest of any nation to having its own control of each layer of the AI stack. This is most notable in its leverage over critical minerals; in 2024, it accounted for[282] 60% of rare earth elements mining, and the country has a virtual global monopoly in processing, demonstrated with great effect in its trade battles with the U.S. Although China remains heavily dependent[283] on foreign oil sources to supplement coal, it is expanding its energy supply from renewable and nuclear generation at much faster pace than coal.[284] In these respects, China is strong where the U.S. is most vulnerable and is shoring up its own vulnerabilities where U.S. supply is tight.

At the model and digital infrastructure layers, China has narrowed the gap through these strengths and massive investment. The ability of LLMs and other generative AI to extract information from heterogeneous data sources disrupted the models of iterative learning where China's scale provides an advantage, but Chinese researchers adapted quickly and effectively with the development of DeepSeek and other small but powerful models like Qwen. Such models are widely adopted,[285] even by Silicon Valley developers (as discussed above), because of their availability on open-weight/open-source platforms like Hugging Face and GitHub and their cost-efficiency.

Like the U.S., China sees an opportunity to enhance its soft power by promoting Chinese AI technology through DSR AI projects[286] and the Shanghai Cooperation Organization.[287] In what seems like a deliberate counterpoint to the White House AI Action Plan, China's "Global AI Governance Action Plan"[288] offers many compatible elements with U.S. policy, including strengthening open-source ecosystems and supporting international standards development organizations. Others note differences, including its framing around "global solidarity," inclusion of energy and environmental issues, and mention of the U.N.'s Pact for the Future[289] and development goals. It also gives a nod to "respecting national sovereignty" and stresses AI safety more than the U.S. plan.

China's global governance plan in effect positions its array of smaller, more energy-efficient AI models alongside the notes of multilateralism and

development as alternatives to U.S. technology that are adaptable to sovereign AI aspirations. China had great success in selling cellular telecommunications around the world by delivering Huawei and ZTE equipment[290] and services as turnkey systems. It may see similar opportunities based on these small models and associated services and equipment, but as discussed above, the fungibility of electronic pipelines, switches, and edge devices is far from adapting AI models and applications to the diverse needs of local languages, cultures, and needs, where human skills matter far more than a full AI stack.

China faces AI challenges despite its favorable position on many parts of the AI stack. A key part of China's long-term AI strategy has been to develop semiconductor supplies in China, especially with U.S. export controls limiting access to advanced chips and manufacturing equipment. Huawei and others have made significant strides in this regard. Even so, Chinese semiconductor manufacturers have lagged[291] behind Nvidia's more advanced chips, limiting its competitiveness in the most complex computations. In response, Huawei has focused its latest generation of AI hardware on packaging efficient systems[292] rather than on chip capacity alone.

Chinese AI also has an alignment problem that puts it at a disadvantage compared to models and systems developed under more liberal governments. While Chinese AI policy identifies safety as a major objective, and China has established a network of AI safety researchers, the priority on content control[293] works to the detriment of safety and security. A Cisco study[294] found that DeepSeek intercepted no harmful commands where OpenAI's GPT-o1 preview model intercepted 74%.

In examining China's strategy for promoting AI, Grace Yang of the Free University of Berlin poses the question,[295] "can a system rooted in domestic surveillance and censorship truly earn global trust and become the basis for a national standard of openness?" Concerns around trustworthiness ultimately bounded the adoption of Huawei and ZTE telecommunications equipment due to concerns about the security of the systems at a time when Chinese stated control of enterprises was less pervasive. Since then, the country has significantly ratcheted up[296] state ownership, party influence, and civil-military fusion and has more thorough regulation of content, data, and cybersecurity to ensure that digital technology conforms to party ideology and government requirements.[297] AI systems are no exception.

While the opportunity for low-cost development can be attractive for autocratic countries and convenient for others, the offer has limitations. Countries that sign deals for DSR infrastructure or funding may sacrifice data security[298] or privacy,[299] take on debt risks from opaque financing terms, and entrench authoritarian capabilities in surveillance technologies, including sensing devices and cameras for facial recognition.[300] By embedding Chinese equipment and software into recipient countries' AI stacks, the DSR extends China's regulatory and technological influence in ways that may not align with more rights-protecting models.

These features may be attractive for some authoritarian governments. Other governments may be indifferent and find it expedient to adopt AI from China. Many governments, however, will view Chinese systems distrustfully. China has long promoted "cyber sovereignty," and the movement for AI sovereignty affords an opportunity to reframe that concept as a selling point for Chinese AI technology. But China's concept of digital sovereignty is to AI sovereignty as monarchical sovereignty is to Rousseau's popular sovereignty. For societies concerned about maintaining agency over AI, technology that not only comes from another country but is more likely than most to be under the control of that country's government is hardly an inviting solution.

FOR OTHER COUNTRIES: TAILORING AI TO NATIONAL AND REGIONAL NEEDS

For the countries that are not yet broad stack leaders, AI sovereignty is a frequently espoused policy goal. But, given the impossibility of complete domestic control over every layer of the stack and the risks of inefficiencies and stranded assets, managing interdependence requires thoughtful choices about what elements of the AI stack are priorities based on consideration of needs and capabilities.

Two sovereign AI strategies have emerged as models for these countries. India's DPI offers one. The other leading strategy is a collective effort where "third place"[301] countries collaborate to produce a "third AI stack" as an alternative[302] to the Chinese and U.S. stacks. The most pragmatic recommendation is for these countries to pursue some mix of these two strategies.

India's Digital Public Infrastructure

While the development of India's DPI model has had its controversies and criticisms,[303] the scale of deployment[304] to over a billion people has garnered the attention of many countries and regions (notably Brazil, Singapore, the UAE, Nigeria, Kenya, and the EU) as a possible template for their own digital infrastructure. India is now engaged in a process to integrate AI into its DPI[305] as described in its AI Mission, which includes the Bhashini initiative[306] to build its own models trained on India's diverse languages and then use these models to improve public services like health and education.

In practice, India's DPI consists of adding domestic applications to an infrastructure that is heavily dependent on foreign—largely U.S.—tech providers including AWS, Google Cloud, and Microsoft Azure, as well as a domestic provider, ESDS. Likewise, India is a large user of GPU chips from Nvidia and is now exploring the use of Google's Tensor Processing Unit (TPU) chips[307] and other accelerators[308] (AMD, Cerebras, SambaNova) as well as China's DeepSeek[309] for AI development. While currently dependent on the U.S., India is purposefully diversifying its dependence across suppliers.

As it rolls out AI applications, India is also exercising managed interdependence with specific initiatives to develop its own national cloud (GI Cloud/MeghRaj) that includes foreign providers but increasingly seeks to shift to Indian firms like Tata, Reliance, and Airtel to bolster[310] its sovereign position. This extends to chip production through the Shakti Project[311] led by IIT Madras, which is developing a 7-nanometer RISC-V instruction set chip expected to be ready by 2028. Notwithstanding these advances and various initiatives, some Indian observers have charged that the pace of substituting foreign for sovereign infrastructure is too slow,[312] underscoring the challenge of competing at the frontier.

India also represents diplomatic success as its visibility and influence in global AI governance has increased through various forums, including as an invited observer[313] to the G7 since 2019, the recent chair and ministerial host to the Global Partnership on AI (GPAI), and its successful G20 presidency where it successfully promoted[314] DPI. As the first developing country to host the AI Action Summit, it furthers its role in guiding the debate and promoting the DPI model. India announced[315] a foundation model designed for the country's multiple languages,[316] developed by Indian firms using Indian data on servers in India that it will launch at the summit. This position has been mirrored by the prominence of the Indian diaspora[317] in the leadership of multinational enterprises, startups, and universities developing AI, as well as in AI policy[318] at the U.N. and other government bodies.

A third AI stack

Another strategy for AI stack builders and layer specialists is to cooperatively develop a Global DPI where each partner contributes to various strata of the AI stack. Collectively, this would amount to a third AI stack through interdependence that is distinct from the U.S. and the Chinese stacks, although some elements might still have some degree of dependence. Since this infrastructure would be built through a consortium of countries and not independently by one, this collective effort is not "sovereign," but rather a strategy for mutualizing interdependence to achieve a higher degree of collective sovereignty than what could be obtained individually

Achieving AI sovereignty on an individual basis, even when relying on foreign tech suppliers and attempting to build sovereign capabilities, would be extremely costly and prone to failure and stranded assets. Collectively the stack builders and layer specialists have select, but deep, expertise[319] in specific segments of the AI stack: Canada and Australia for critical materials, Brazil for renewable energy, Africa in data curation, U.K. in chip design, the Netherlands in chip

fabrication machine tools, Taiwan in chip fabrication, Japan and South Korea in high-bandwidth memory, France and Italy for compute, and so forth. Each country has unique repositories of data in areas like health, mining, agriculture, transportation, and manufacturing. By concentrating on their relative comparative advantage and entering alliances, these countries and others could assure each other strategic interdependence[320] that promotes innovation and competition while collectively ensuring all members leveraging their respective advantages gain sovereignty. By aligning their efforts collectively, they also could muster the needed financial investments, an aggregate demand, and a ready market for the AI models produced.

Building such alliances and orchestrating coordination would be a complex undertaking but can be a feasible strategy—both technically and financially—for most countries to achieve some semblance of AI sovereignty. Antecedents for such an approach exist both in the Airbus Industrie,[321] the International Space Station, and CERN[322] particle physics lab.

These groups are shaped by current expectations about the persistence of hardware scarcity and centralized compute, assumptions that may not hold under all plausible technological trajectories. If compute becomes commoditized and models more portable, sovereignty concerns may shift downward toward data, applications, and governance; if advanced hardware remains scarce or recentralizes (e.g., through quantum), current asymmetries may harden rather than erode. While strategies premised on full-stack control can be fragile depending on future development, diversification and interoperability are consistently needed.

Each of these strategies has strengths and weaknesses. The DPI approach provides a continuum whereby localized AI applications can be quickly built and deployed using foreign providers of essential services like cloud computing. Over time, dependencies can be reduced through diversification of suppliers, including domestic providers. The weakness is that by enriching foreign suppliers that continue to innovate and scale, it may be challenging to provide a viable domestic competitor. The third AI stack strategy relies on diplomatic and technological alliances to achieve sovereignty based on collective and coordinated action, where each participant focuses on their relative comparative advantage. This would reduce costs and provide an alternative to the U.S. and Chinese AI stacks, which can be beneficial for the globe if it stimulates innovation and competition. The risk lies in the political and logistical complexity of building and maintaining such alliances, especially in this geopolitically charged environment.

Pursuing one of these strategies does not preclude using the other. Rather, the most practical approach for most countries would be to undertake both in parallel. Countries could start with a DPI and applications-focused approach, providing them with some sovereignty in the deployment of AI. Over time, they could focus on reducing select vulnerabilities and dependencies in those segments of the stack where they have relative comparative advantage and contribute these to a collective third stack that could provide a higher degree of sovereignty. Both the World Economic Forum[323] and David Shrier of Imperial College[324] London provide useful roadmaps for developing such strategies.

CONCLUSION

Every government—regardless of where it fits on the spectrum of AI strength—needs cooperation to manage transboundary risks, shared supply chains, and global governance and standards. Layers of the AI stack are inherently transnational, based on globally distributed resources and supply chains, software dependencies, and migration of talent and knowledge. No government can realistically achieve full, end-to-end sovereignty across the AI stack.

This reality makes "absolute" technological autonomy a costly and often counterproductive objective. Efforts to localize every layer of the AI stack risk duplicative investment, stranded assets, higher costs, and regulatory fragmentation that would slow diffusion. At the same time, the sovereignty impulse reflects legitimate policy needs, including national security, infrastructure resilience, economic strategy, and the demand that AI systems align with local languages, values, and laws.

The framework advanced in this report, managed interdependence, reconciles these tensions. It treats sovereignty less as complete self-sufficiency and more as a country's capacity to set the terms of its dependencies. It also recognizes that many risks are inherently transnational; model misuse, cybersecurity vulnerabilities, and downstream diffusion of unsafe practices therefore require cooperation even among countries pursuing greater autonomy.

Putting managed interdependence into practice requires mapping dependencies and choke points across the AI stack and then prioritizing interventions where vulnerabilities are highest and substitutes are realistically achievable. Governments should diversify sources for critical inputs, build redundancy where feasible, and use partnerships to reduce exposure to single points of failure. They should embed interoperability and portability, both technically through open standards and compatible architectures, and institutionally through participation in standard-setting and governance coordination. This also includes investment in public-interest capacity including data stewardship, talent pipelines, and governance capacity. Finally, managed interdependence must be anchored in rights-respecting governance so that "sovereignty" does not become a pretext for surveillance, censorship, or erosion of rule-of-law protections.

Well-intentioned sovereignty strategies still may lead to splintering and dysfunction, particularly those that emphasize isolation over resilience. In many cases, diversification can be a positive by leading to redundancies in the system, innovative approaches to governance, or allowing for different approaches based on a country's values and needs. Therefore, the objective is not to prevent countries from seeking greater agency over AI but to channel sovereignty efforts toward strategic capacity-building and cooperative partnerships.

APPENDIXES

Appendix A.

Data and country rankings for categorization

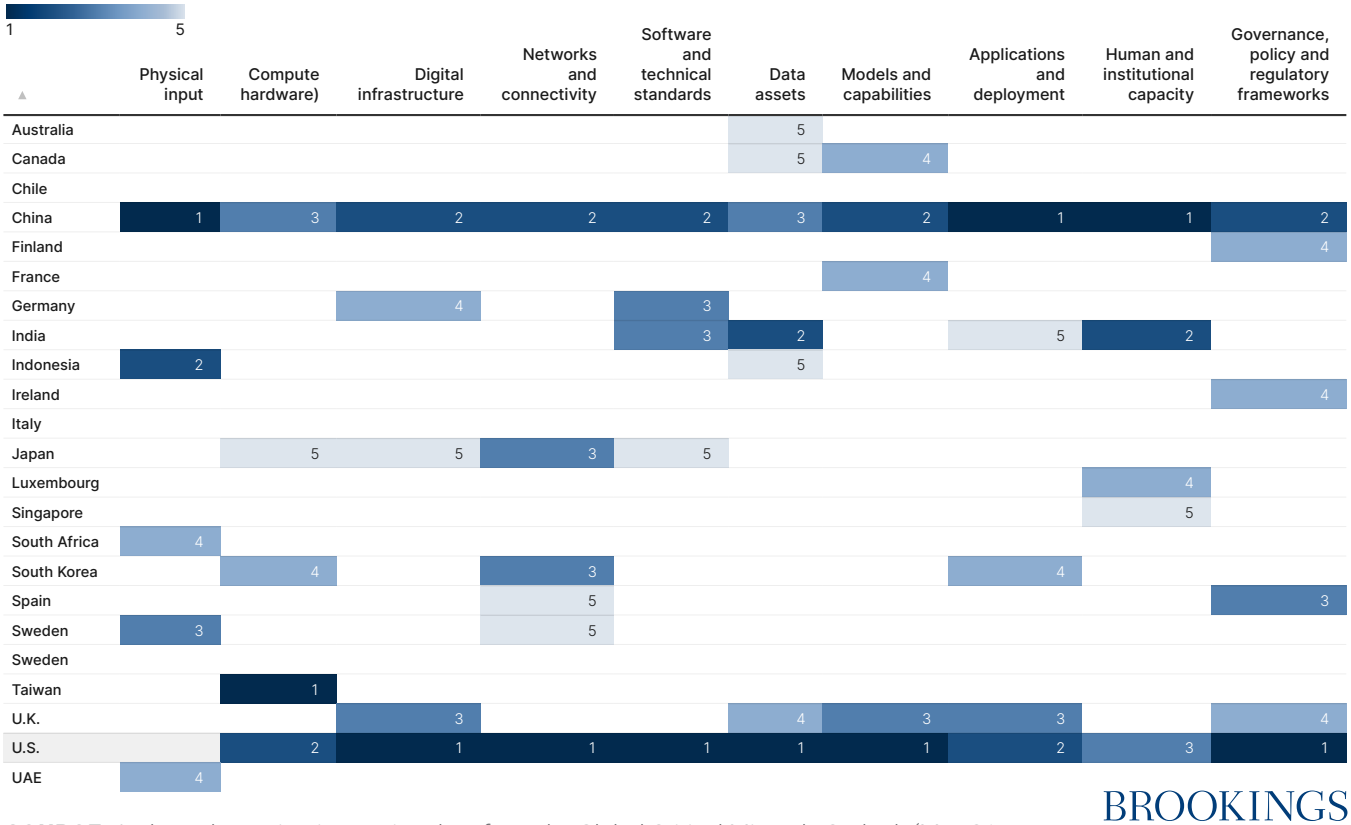
This chart combines rankings from several datasets for each layer of the AI stack. The top five countries were determined by assigning 1-5 points for the top five countries in each dataset and then totaling the points for each dataset relevant to the layer. Finally, the top five countries in the layer were ranked and included in the chart.

Due to the number of datasets used to determine layer leaders, some countries scored in the top five in an individual dataset but not in other datasets used to evaluate the layer and thus were excluded from the cumulative top five.

FIGURE 3

Leaders in each layer of the AI stack[325]

These rankings show leading countries in order from first (1) to fifth (5) based on rankings derived from the data. While demonstrative of leading countries in each layer, this figure is not a definitive assessment of leadership.



BROOKINGS

SOURCE: Authors determinations using data from the Global Critical Minerals Outlook (May 21, 2025), International Energy Agency,[326] Electricity Mix,[327] Market share for logic chip production,[328] by manufacturing stage,[329]

and Cumulative number of large-scale AI systems by country since 2017 (2021-2024, Our World in Data),[330] Stanford AI Index Report (2025, Stanford AI Human-Centered Artificial Intelligence),[331] Data Centers Around the World (May 2021, United States International Trade Commission),[332] Broadband statistics (2024, OECD),[333] Safeguarding Subsea Cables (2024, Center for Strategic and International Studies),[334] Journal of International Communication,[335] GitHub Repositories (January 2026, GitHub),[336] Distribution of Authors per Country (August 2024, Internet Engineering Task Force),[337] ICT service exports (BoP, current US$) (2024, World Bank),[338] Individuals using the Internet (2025, International Telecommunication Union),[339] and Wikimedia statistics (2025, Wikimedia).[340]

Appendix B.
Detailed description of the AI stack

PHYSICAL INPUT: MINERALS, ENERGY, AND WATER

Critical minerals and elements needed for AI hardware[341] are often found in only a few countries. Downstream components like advanced semiconductors, fiber optics, and cooling systems all rely on critical materials.

China controls[342] the vast majority of critical mineral processing, including about 90% of global rare earth processing, 98% of the world's primary gallium production, and around 60% of refined germanium production. The government has used this concentration to exert pressure further up the stack: After the U.S. tightened export controls on advanced chips to China in 2023, the Chinese government retaliated[343] by restricting exports of gallium and germanium to the United States. This concentration means that the entire AI stack is vulnerable to disruptions in critical mineral processing from trade restrictions, geopolitical conflicts, or other instability.

Other countries have invested in mining[344] or discovery[345] capabilities through domestic projects and global partnerships. Given that new mining projects can be costly, slow, and impose human rights[346] and environmental costs[347] on local communities, some countries are turning to new techniques, including AI tools to find deposits[348] and recycling methods.[349]

TABLE B

Projected leading countries critical mineral production and refining in 2030[350]

Mineral type	Top producing/mining countries (in order of production level)	Top refining countries (in order of refining level)
Copper	Chile, Democratic Republic of the Congo, Peru	China, Democratic Republic of the Congo, Chile
Lithium	China, Australia, Chile	China, Chile, Argentina
Nickel	Indonesia, Philippines, Russia	Indonesia. China, Russia
Cobalt	Democratic Republic of the Congo, Indonesia, Russia	China, Finland, Indonesia
Natural graphite	China, Madagascar, Japan	China, Japan, Indonesia
Rare earths	China, Australia, Myanmar	China, Malaysia, United States

SOURCE: International Energy Agency (June 2025)[351]

BROOKINGS

Running advanced AI systems demands high amounts of energy. AI server electricity consumption is projected to grow[352] by 30% annually. The impact is especially acute in the United States—currently the world's largest data-center market—and, in 2024, it was responsible for about 45% of global data-center electricity consumption.[353] The International Energy Agency estimates[354] that U.S. data-center energy demand will increase by 130% by 2030, driven in large part by AI workloads. These figures do not include the water demands[355] for cooling these data centers, which have "direct and indirect implications for biodiversity."

Power availability, political resistance,[356] and permitting timelines are limiting factors in making more energy available. AI companies are clamoring[357] for gigawatts of new capacity in the coming years, while current permitting processes for new power plants and high-voltage transmission lines can take a decade or more in the United States and the European Union, with no guarantee of sustained growth at these elevated rates.

Conversely, China added[358] over 400 gigawatts of new power capacity online in a single year. Other countries, like South Korea[359] and Saudi Arabia,[360] are also investing in new energy production facilities to support AI workloads and to become hubs[361] of AI computation. Others, like France[362] and Italy,[363] have created partnerships with countries that have greater access to energy rather than attempting the expensive task of complete energy sovereignty. Many countries are also committed to decarbonization, which complicates decisions about energy sources and locations[364] of new data centers. For example, Norway has invested in renewable energy projects to complement oil and gas production; the country's hydropower accounts[365] for 90% of its electricity generation.

COMPUTE HARDWARE

AI hardware relies on specialized[366] semiconductors,[367] including accelerators—primarily GPUs, but also domain-specific chips like Google's TPUs and custom application-specific integrated circuits. These accelerators are only effective when paired[368] with advanced memory technologies, particularly high-bandwidth memory (HBM). Modern Nvidia accelerators, for example, are designed[369] around HBM stacks that deliver much higher bandwidth than conventional dynamic random-access memory. Production of HBM is highly concentrated among three firms:[370] SK Hynix and Samsung Electronics in South Korea, and Micron in the United States with operations in Japan. Gains in AI capability are constrained[371] as much by memory bandwidth and energy efficiency as by raw compute throughput.

While the United States dominates[372] AI chip design and accelerators (Nvidia,[373] AMD, Intel, Qualcomm), TSMC fabricates[374] more than 90% of the world's most advanced logic chips, and South Korea leads[375] in advanced memory production. Meanwhile, semiconductor manufacturing equipment is dominated by a few players. Most notably, the Dutch firm ASML[376] is the sole provider of EUV lithography machines needed for advanced logic chips. The raw materials for chip production, like high-purity silicon wafers and photoresists, are largely supplied[377] by firms in Japan, Taiwan, and South Korea. This asymmetric distribution means that no country controls the whole semiconductor stack required for frontier AI systems. This concentration can result in supply-chain choke points and barriers to market entry.

While new entrants are emerging[378] in the AI chip market, few countries possess the end-to-end capacity to design, manufacture, and deploy chips at scale. The strategic importance of this layer is demonstrated by U.S. export controls[379] targeting China and the EU Chips Act,[380] which aims to double Europe's share of production to 20% by 2030. But even if successful, Europe will likely still rely on non-European intellectual property and equipment (e.g., TSMC's planned fabrication plant[381] in Germany). New projects take a long time to get off the ground as well, with fab construction lead time[382] often taking over five years.

DIGITAL INFRASTRUCTURE

Above the physical networks in the stack are the cloud platforms and data centers that store and process data and host AI workloads. The global cloud ecosystem is dominated[383] by a handful of largely U.S.-based[384] hyperscalers. This concentration reflects

not only economies of scale but also the reach of U.S. legal jurisdiction over corporate actors and data flows.[385] Even in Europe, U.S. companies make up[386] 70% of the European cloud market share, while Chinese companies make up[387] most of the remaining 30%.

In response, several EU initiatives aim to develop "sovereign cloud" frameworks. A sovereign cloud is a cloud computing environment[388] specifically designed to help an organization or nation solidify data sovereignty by ensuring that data is subject[389] to the laws and governance structures of that specific jurisdiction. The Franco-German GAIA-X initiative aimed to create a federated, interoperable cloud ecosystem aligned with EU data-protection standards. Yet years after its launch, GAIA-X has struggled[390] to deliver on its promise. Outside of Europe, sovereign cloud efforts often involve[391] direct state partnerships with hyperscalers or national telecommunications providers. Several of China's sovereign cloud providers rely[392] on U.S. chips to implement the cloud infrastructure. Even "sovereign" offerings[393] often depend[394] on foreign hardware and software.

Global demand for data-center capacity could reach[395] 171–219 gigawatts by 2030, nearly tripling demand from 2023. It is projected[396] that 70% of that new demand will come from AI workloads. The resulting boom in data-center construction brings substantial resource demands[397] and risks[398] including land-use pressures and local environmental impacts. As data centers proliferate, some analysts warn of a potential infrastructure surplus, echoing the overcapacity[399] issues that plagued telecommunications networks in the early 2000s. The European Commission's AI gigafactory plan, announced[400] in the 2024 AI Innovation Package, aims to triple the EU's data-center capacity within five to seven years. Similar efforts exist in Asia[401] and the Middle East.[402]

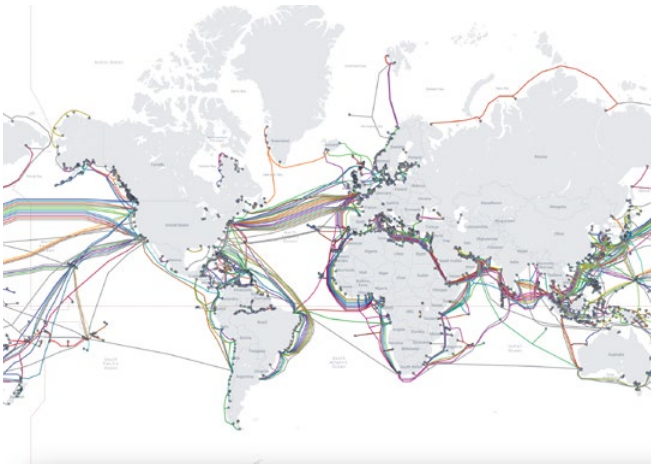
NETWORKS AND CONNECTIVITY

Network infrastructure includes physical infrastructure[403] like fiber-optic cables (both terrestrial and undersea), routers and switches, cellular networks[404] (4G/5G towers[405] and core networks), content delivery networks, internet exchange points, and satellites.

Roughly 95% (some estimates as high as 99%)[406] of international data traffic travels[407] through subsea cables, which are vulnerable to espionage, data tapping, and sabotage. Of the roughly 150–200 faults per year[408] across international submarine cable systems, the bulk of damage is attributed to anchoring and fishing activities rather than international attacks. Still, intentional sabotage can occur, including allegations[409] that a recently damaged undersea cable across the Gulf of Finland was sabotaged. Repair costs can average[410] hundreds of thousands to more than $1 million per incident.

FIGURE 4

TeleGeography submarine cable map



SOURCE: Global Submarine Cable Map, Telegeography (2025)

In the United States, the Federal Communications Commission (FCC) maintains a "Covered List"[411] of communications equipment and services deemed to pose an unacceptable risk under the Secure and Trusted Communications Networks Act framework. The U.S. banned[412] hardware from Chinese firms like Huawei and ZTE from network hardware, scrutinized[413] Chinese-made drones, and encouraged allies[414] to follow suit based on security risks and potential backdoors in this layer. The FCC's $4.98 billion "Rip and Replace"[415] program reimburses smaller providers who are removing and replacing Huawei and ZTE equipment.

Partners have pursued analogous approaches. The European Commission's formal assessment of the 5G Toolbox implementation states[416] that member state decisions to restrict or exclude Huawei and ZTE are "justified and compliant with the 5G Toolbox." The Czech Republic has been vocal in warning against exposure to Chinese technology, issuing warnings[417] about using Chinese-made security cameras in critical infrastructure.

As countries diverge on "trusted vendor" definitions and procurement rules, cross-border operators may face inconsistent requirements. Governments and industry have responded by pursuing supplier diversification strategies (including Open RAN), but diversification brings additional challenges[418] of multi-vendor management and larger integration and assurance burdens.

Even where global connectivity exists on paper, domestic bottlenecks such as unreliable power, bandwidth issues, or poor last-mile coverage can constrain AI adoption. ITU DataHub figures show fixed-broadband subscriptions around 0.60 per 100 people[419] in low-income countries in 2025, compared with 20.1 globally.

DATA ASSETS

High-quality training data could be exhausted[420] in 2026. After that, further model improvements will increasingly require either proprietary or synthetic data. Some countries see synthetic data[421] as a way to expand training corpora and to generate localized content in low-resource languages[422] or domains.[423] This trend suggests a future where nations treat data as a strategic resource, particularly in specialized datasets such as health, law, or national corpora. These datasets can differentiate domestic models and limit reliance on general-purpose commercial data.

Securing such high-quality datasets presents legal and ethical challenges, including disputes over the use of copyrighted[424] and personal data in training. Sovereign data initiatives such as India's Bhashini[425] initiative and Singapore's SEA-LION[426] initiative seek to curate national datasets in local languages and make them available for domestic model development.

Data sovereignty and localization[427] laws are increasing, making data subject[428] to the laws and governance structures of the nation where it is collected and often placing limitations on where data can be moved, processed, or stored. Data sovereignty regimes are often motivated[429] by concerns that foreign governments or companies might exploit[430] data, access it for surveillance,[431] or otherwise violate[432] citizens' privacy and rights. At the same time, data collected within a country can enable faster[433] AI innovation and better model development, especially when used to construct high-quality, domain-specific[434] training datasets.

Nations and creators want sovereignty over their data, preventing its wholesale extraction for training commercial AI models. Using copyrighted materials to train AI models without permission is a current subject of ongoing litigation[435] over infringement claims. Recent research suggests that generative AI models can output substantive amounts of text near-verbatim[436] from copyrighted work, complicating claims that AI output is original[437] or transformative[438] from training materials. Intellectual property laws, especially copyright, differ by country and could be a means for asserting greater sovereignty over data.

However, restrictive data regimes risk[439] fragmenting datasets, increasing operational costs for multinational companies, and limiting multinational datasets needed for research and innovation. Research suggests[440] that, all else equal, larger[441] training datasets tend to improve LLM performance through scaling effects. The United States and China benefit from large user bases[442] generating data and relatively permissive[443] environments[444] for commercial data use, which give them an advantage in training general-purpose models.

At the same time, international data sharing can also be a strength. Some countries are exploring alliances and coordination to pool data resources. For example, Latin American countries have discussed sharing translation datasets to improve Spanish-language AI systems, while the African Union has developed[445] continental data[446] and AI strategies[447] to support African AI projects. Countries that seek access to larger training datasets have supported policies enabling cross-border data flows where legal regimes

are sufficiently compatible. Democratic countries have supported frameworks like the G7's "Data free flow with trust,"[448] which aims to facilitate data exchange across borders among trusted partners and to foster innovation while protecting data rights.

SOFTWARE, MODELS, AND TECHNICAL STANDARDS

AI models are composed of the algorithms, code, weights, and parameters that give AI systems their functionality. Models are designed, trained, fine-tuned, and validated at this layer[449] using machine learning frameworks and libraries.

Today, a large[450] share[451] of cutting-edge foundation models is developed[452] by a handful of firms. This concentration is reinforced by several barriers[453] to entry: access to large computational resources, large datasets, specialized scientific and engineering talent, and sufficient energy resources. Relying on proprietary models can subject[454] recipients to contractual terms, including output limits, service fees, and usage restrictions.

While much attention is directed toward leading foundation models, one author (Kerry) and Saurabh Mishra have pointed out[455] that AI spans "interlocking techniques, tools, and capabilities" with different domains and applications rather than a single monolithic system. This broader view opens additional pathways for sovereign AI strategies, including selective use of openness at different layers of the stack. However, "openness" is not a single alternative. Open-source software, open-weight models, and, more rarely, fully open models that include detailed training documentation and data transparency each offer distinct sovereignty benefits and risks.

Open-source software, where just the source code is made available but often not the weights or training data, underpins[456] 70–90% of modern codebases (the collection of source code for an application or piece of software). In AI systems, this includes operating systems, machine learning frameworks, and orchestration tools. Proponents of open-source software argue it provides greater transparency of implementation, forkability, and reduced dependence on proprietary vendors for maintenance and customization. These benefits, however, do not extend to control over model behavior or training provenance, which remain opaque when weights and data are closed.

Open-weight models expose trained parameters and allow local deployment, fine-tuning, and inference without reliance on proprietary APIs. Access to weights allows empirical testing and fine-tuning, but it does not by itself enable full auditability of training data or embedded biases.

Fully open models, which meaningfully disclose weights, training procedures, evaluation methods, and at least partial data provenance, may support research scrutiny and democratize collaboration. However, their relevance for sovereignty is constrained by the limited ability of most countries to reproduce or independently retrain models at scale, given the concentration of compute, energy, and specialized hardware.

Crucially, openness does not necessarily eliminate dependency risks; it redistributes them across the stack. Many sovereign "open" models, even those released under open licenses, rely on infrastructure maintained by U.S. companies, and almost all models depend[457] on U.S. semiconductor design. The UAE's Falcon model family, for example, was trained[458] on AWS infrastructure. At the software layer, open-source AI ecosystems remain tightly coupled to U.S.-origin frameworks such as PyTorch and TensorFlow, which are themselves optimized[459] for Nvidia GPUs and the CUDA programming stack.

Singapore's SEA-LION[460] large language model shows these trade-offs. The project was initially developed on Meta's Llama open architecture but switched[461] to Alibaba Cloud's Qwen architecture, remaining dependent on foreign technology, even as developers sought[462] to reflect domestic linguistic and cultural contexts.

Proponents of proprietary models often also argue[463] that closed-model approaches strengthen security[464] by making it harder for malicious actors to remove guardrails or weaponize models. Open models may reduce dependence on specific firms but increase

concerns about proliferation, while proprietary models can centralize power in a few actors whose priorities may not align with national or public interests.

Not every country needs to train a GPT-5-class model from scratch to benefit from AI. Many can adopt existing foundation or open-weight models and adapt them to local needs at a far lower cost. Small language models tuned to linguistic, cultural, or sectoral contexts[465] (like a 13B-parameter model optimized for Indonesian) can outperform larger general-purpose models in that niche while requiring significantly less computational power, energy, and money to train and operate. These models are easier to deploy on domestic infrastructure, including edge devices and local servers with limited connectivity, making them useful for agriculture, infrastructure, and defense applications.

For countries seeking AI sovereignty without access to frontier-scale compute, a range of model-adaptation techniques, including distillation, fine-tuning, continued or domain-specific pretraining, and lightweight adaptation layers, offer viable alternatives. By relying on smaller, more targeted datasets and purpose-built adaptation pipelines, governments and firms can also mitigate some privacy and data-protection risks associated with large-scale web scraping and better align AI systems with domestic legal and regulatory requirements. Together, these approaches lower the barriers to building sovereign AI capabilities without attempting to replicate the most capital-intensive layers of the AI stack.

TABLE C

Selection of sovereign AI initiatives[466]

Country	Model Name	Model Type
China	Domestic LLMs (ERNIE, Baichuan, etc.)	Training frontier model and mid-scale models
France	BLOOM LLM	Trained, open-source LLM
Germany	Sovereign Open Source Foundation Models (SOOFI)	Building "advanced AI" open-source model w/100B parameters
India	Param2[467]	Training frontier models Fine-tuning LLMs to Indian languages
Japan	Fugaku-LLM[468]	Pretrained from scratch
Netherlands	GPT-NL[469]	Pretrained from scratch (not yet released)
Poland	PLLuM	LLM
Portugal	Amalia	LLM
Russia	GigaChat, YaLM 2.0	Training a frontier model
Saudi Arabia	HUMAIN Chat	Trained ALLAM model from scratch
Singapore	SEA-LION family of models[470]	V1 pretrained from scratch; V2 based on Llama 3
South Korea	LG AI Research, SK Telecom, Naver, NCSoft, Upstage	Training frontier models
Spain	Family of foundation models, Alia	Some pretrained from scratch; others based on open-source models (not yet released)
Sweden	GPT-SW3 family of models[471]	Some pretrained from scratch; others based on Llama 3
Switzerland	Apertus	Open multilingual model
Taiwan	TAIDE family of models[472]	Based on Llama 2 and Llama 3
United Arab Emirates	Falcon family of models[473]	Pretrained from scratch
United Kingdom	"National Foundation Model Taskforce"	Building foundation models

SOURCE: Adapted from "Sovereign AI in a Hybrid World: National Strategies and Policy Responses" (Pablo Chavez, Lawfare, November 7, 2024). Sources include Lawfare (2024), Euronews (2025), and Digit.in (2026).

BROOKINGS

APPLICATIONS AND DEPLOYMENT

Applications are the AI-enabled services and products that directly interface with users or are deployed across sectors. This is what most people experience as "AI": a translation app on a phone, a recommendation feed on social media, a facial recognition system at an airport, or an AI diagnostic tool in a hospital. At this layer, trained models are integrated into production systems through APIs, dashboards, inference engines, conversational agents, and search or retrieval tools. Most AI applications and software are built on top[474] of a few foundation models, developed by a few firms.

Sovereign AI ambitions need not depend on building foundation models from scratch. The application layer—where AI is customized, deployed, and integrated into services—is far less concentrated and more open to diverse participation. Nations seeking technological autonomy can focus here: developing homegrown applications that serve domestic needs, retain data locally, and comply with national regulations, while leveraging foreign or open-source models as a base. At the same time, an "application-first" strategy often inherits the strongest dependencies from other AI stack layers. If you build on foreign foundation models via APIs or managed platforms, you are exposed to opaque model updates, pricing/terms changes, or foreign legal jurisdiction. In practice, the application layer can be a thin wrapper over someone else's model, giving the real control to a foreign entity.

Businesses are integrating AI into virtually every sector: finance (algorithmic trading,[475] credit scoring),[476] agriculture (crop monitoring via autonomous drones),[477] health care (medical imaging diagnostics,[478] drug discovery),[479] government (chatbots for e-services,[480] predictive policing),[481] transportation (self-driving vehicles,[482] traffic management),[483] and more. Many countries have priority sectors where they want to push AI. Sovereign AI strategies often tailor applications to national priorities and contexts, rather than importing generic products. Many of these applications are dual-use,[484] meaning systems developed for civilian service delivery can be repurposed for surveillance, influence operations, or security or military objectives. Risks from building on foreign models are even greater for dual-use applications, which can inherit censorship policies or safety behaviors from a foreign-controlled base model. Application-level dual-use technologies complicate clean separations between economic and national security policy.

GOVERNANCE, STANDARDS, AND TALENT

Governance, standards, and talent are not discrete layers but crosscutting enablers that intersect with every layer of the AI stack. AI governance—including laws, standards, ethical guidelines, and oversight mechanisms—shapes how AI is developed and deployed. For nations pursuing sovereign AI, robust domestic governance frameworks are essential; they ensure AI systems align with national values, protect citizens, and reduce reliance on foreign regulatory regimes. This may include formal regulation (like the EU's AI Act),[485] industry standards (ISO AI standards,[486] IEEE AI ethics guidelines),[487] testing and certification regimes, audit and compliance infrastructure, and international norms or treaties. Likewise, talent is essential to every stage in AI development, adoption, and governance.

Without clear definitions of "sovereignty" around technology, firms can market themselves as sovereign-ready while remaining embedded in foreign infrastructure, legal jurisdictions, or proprietary standards. In response, some countries and vendors are promoting solutions like the Open Standard Identity APIs[488] (OSIA), which are designed to ensure interoperability across the stack without locking adopters into a single vendor ecosystem.

At the international level, forums like the Organisation for Economic Co-operation and Development[489] (OECD), the G7 Hiroshima AI Process,[490] the Global Partnership on AI (GPAI)[491] and the International Telecommunication Union (ITU),[492] and various[493] U.N.[494] bodies,[495] among others,[496] serve as venues for like-minded nations to coordinate governance approaches. Standards development organizations, like ISO, CEN-CENELEC, and IEEE are developing technical standards[497] for AI safety, transparency, and interoperability. Recent FCAI work[498] conceptualizes these bodies as nodes in a distributed "network architecture" for AI governance, arguing that a decentralized system of overlapping institutions is better suited to a fast-moving technology than a single centralized regulator.

END NOTES

1. Seb, Murray. 2025. “How Artificial Intelligence Impacts the US Labor Market | MIT Sloan.” MIT Sloan. October 9, 2025. https://mitsloan.mit.edu/ideas-made-to-matter/how-artificial-intelligence-impacts-us-labor-market.
2. Microsoft AI Economy Institute. 2026. “Global AI Adoption in 2025 – AI Economy Institute | Microsoft.” Microsoft Corporate Responsibility. Microsoft. January 9, 2026. https://www.microsoft.com/en-us/corporate-responsibility/topics/ai-economy-institute/reports/global-ai-adoption-2025/.
3. “India AI Impact Summit 2026.” 2025. India AI Impact Summit 2026. 2025. https://impact.indiaai.gov.in/.
4. Barlow, John Perry. 1996. “A Declaration of the Independence of Cyberspace.” Electronic Frontier Foundation. February 8, 1996. https://www.eff.org/cyberspace-independence.
5. Goldsmith, Jack L, and Tim Wu. 2006. Who Controls the Internet? Oxford University Press EBooks. Oxford University Press. https://doi.org/10.1093/oso/9780195152661.001.0001.
6. Singer, Scott, and Matt Sheehan. 2025. “China’s AI Policy at the Crossroads: Balancing Development and Control in the DeepSeek Era.” Carnegie Endowment for International Peace. 2025. https://carnegieendowment.org/research/2025/07/chinas-ai-policy-in-the-deepseek-era
7. Information Office of the State Council of the People’s Republic of China. 2010. “The Internet in China.” Www.china.org.cn. June 8, 2010. http://www.china.org.cn/government/whitepaper/node_7093508.htm.
8. Leskin, Paige. 2019. “Here Are All the Major US Tech Companies Blocked behind China’s ‘Great Firewall’ - Business Insider.” Business Insider. Business Insider. October 10, 2019. https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5.
9. Pohle, Julia, and Thorsten Thiel. 2020. “Digital Sovereignty.” Internet Policy Review 9 (4). https://policyreview.info/concepts/digital-sovereignty.
10. Bradford, Anu. 2019a. The Brussels Effect: How the European Union Rules the World. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001.
11. European Union. 2016. “REGULATION (EU) 2016/679 of the EUROPEAN PARLIAMENT and of the COUNCIL.” Europa.eu. April 27, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
12. Murphy, Ronan. 2025. “Mapping the Brussels Effect: The GDPR Goes Global.” CEPA. August 7, 2025. https://cepa.org/comprehensive-reports/mapping-the-brussels-effect-the-gdpr-goes-global/.
13. “Data Localization Laws by Country: What Businesses Must Know.” 2024. Captain Compliance. June 2024. https://captaincompliance.com/education/data-localization-laws-by-country/.
14. Reuters Staff. 2025. “From Australia to Europe, Countries Move to Curb Children’s Social Media Access.” Reuters, December 9, 2025. https://www.reuters.com/world/asia-pacific/australia-europe-countries-move-curb-childrens-social-media-access-2025-12-09/.
15. International Energy Agency. 2025. “Global Critical Minerals Outlook 2025 – Analysis - IEA.” IEA. May 21, 2025. https://www.iea.org/reports/global-critical-minerals-outlook-2025; Ritchie, Hannah, and Pablo Rosado. 2020. “Electricity Mix.” Our World in Data. July 2020. https://ourworldindata.org/electricity-mix; “Market Share for Logic Chip Production, by Manufacturing Stage.” 2021. Our World in Data. 2021. https://ourworldindata.org/grapher/market-share-logic-chip-production-manufacturing-stage; “Cumulative Number of Large-Scale AI Systems by Country since 2017.” 2025a. Our World in Data. https://ourworldindata.org/grapher/cumulative-number-of-large-scale-ai-systems-by-country?tab=table; Nestor Maslej, Loredana Fattorini, Raymond Perrault, Yolanda Gil, Vanessa Parli, Njenga Kariuki, Emily Capstick, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika,

END NOTES

Juan Carlos Niebles, Yoav Shoham, Russell Wald, Toby Walsh, Armin Hamrah, Lapo Santarlasci, Julia Betts Lotufo, Alexandra Rome, Andrew Shi, and Sukrut Oak. 2025a. "The 2025 AI Index Report." AI Index Steering Committee, Institute for Human-Centered AI, Stanford University. April 2025. https://hai.stanford.edu/ai-index/2025-ai-index-report; Daigle, Brian. 2021. "Data Centers around the World: A Quick Look." https://www.usitc.gov/publications/332/executive_briefings/ebot_data_centers_around_the_world.pdf; "Broadband Statistics." 2024. OECD. 2024. https://www.oecd.org/en/topics/sub-issues/broadband-statistics.html; Runde, Daniel, Erin Murphy, and Thomas Bryja. 2024. "Safeguarding Subsea Cables Protecting Cyber Infrastructure amid Great Power Competition." https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-08/240816_Runde_Subsea_Cables.pdf; GitHub. 2025. "Innovationgraph/Data/Repositories.csv at Main · Github/Innovationgraph." GitHub. 2025. https://github.com/github/innovationgraph/blob/main/data/repositories.csv; "Distribution of Authors per Country." 2024. Arkko.com. August 11, 2024. https://www.arkko.com/tools/rfcstats/countrydistr.html; "ICT Service Exports." 2024. World Bank Open Data. 2024. https://data.worldbank.org/indicator/BX.GSR.CCIS.CD?end=2024&start=2024; "Individuals using the Internet." 2024. Itu.int. 2024. https://datahub.itu.int/data/?i=11624; "Wikistats - Statistics for Wikimedia Projects." 2026. Wikimedia.org. 2026. https://stats.wikimedia.org/;

16. Edler, Jakob, Knut Blind, Henning Kroll, and Torben Schubert. 2021. "Technology Sovereignty as an Emerging Frame for Innovation Policy. Defining Rationales, Ends and Means." Research Policy 52 (6): 104765–65. https://doi.org/10.1016/j.respol.2023.104765.
17. Stewart, Sara. 2025a. "Innovative Public Infrastructure for the Common Good." Foreign Policy. FP Analytics. February 5, 2025. https://fpanalytics.foreignpolicy.com/2025/02/05/digital-public-infrastructure/.
18. Gerosa, Marco, Anna Hermansen, Anni Lai, and Adrienn Lawson. 2025a. "The State of Sovereign AI." August 2025. https://www.linuxfoundation.org/hubfs/Research%20Reports/lfr_sovereign_ai25_082525a.pdf?hsLang=en.
19. "CYBER CAPABILITIES and NATIONAL POWER: A Net Assessment." n.d. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf.
20. Levy, Cindy, Matt Watters, and Shubham Singhal. 2025. "Restricted: How Export Controls Are Reshaping Markets." McKinsey & Company. April 3, 2025. https://www.mckinsey.com/capabilities/geopolitics/our-insights/restricted-how-export-controls-are-reshaping-markets.
21. Mulligan, Steve P. 2025. "Cross-Border Data Sharing under the CLOUD Act." Congress.gov. 2025. https://www.congress.gov/crs-product/R45173.
22. Yayboke, Erol, Carolina Ramos, and Lindsey Sheppard. 2021. "The Real National Security Concerns over Data Localization." Center for Strategic and International Studies. July 23, 2021. https://www.csis.org/analysis/real-national-security-concerns-over-data-localization.
23. "AI and the Future of the U.S. Electric Grid." 2025. Rand.org. RAND Corporation. April 4, 2025. https://www.rand.org/pubs/articles/2025/ai-and-the-future-of-the-us-electric-grid.html.
24. "Generative Artificial Intelligence for the Power Grid | Grid Modernization | NREL." 2025. Nrel.gov. 2025. https://www.nrel.gov/grid/generative-artificial-intelligence-for-the-power-grid.
25. "AI and Generative AI: Transforming Europe's Electricity Grid for a Sustainable Future." 2024. Shaping Europe's Digital Future. September 25, 2024. https://digital-strategy.ec.europa.eu/en/library/ai-and-generative-ai-transforming-europes-electricity-grid-sustainable-future.
26. Roberts, Patrick S. 2025. "How AI Is Changing Our

END NOTES

Approach to Disasters." Rand.org. RAND Corporation. August 27, 2025. https://www.rand.org/pubs/commentary/2025/08/how-ai-is-changing-our-approach-to-disasters.html.

27. Pfaff, C. Anthony. 2025. "The Weaponization of Artificial Intelligence: the next stage of terrorism and warfare." https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf.
28. Hall, Rachel. 2025. "Rogue States Could Use AI to Do 'Real Harm', Warns Ex-Google CEO." The Guardian. The Guardian. February 13, 2025. https://www.theguardian.com/technology/2025/feb/13/former-google-ceo-warns-ai-could-be-used-by-rogue-states-to-harm-people.
29. "Europeans Reeling as Trump Threatens Tariffs on 8 Countries over Greenland Dispute." 2026. Cbsnews.com. January 18, 2026. https://www.cbsnews.com/news/trump-tariffs-europe-greeland/.
30. Khan, Mariam. 2026. "US Military Is 'Always an Option' for Trump to Acquire Greenland, White House Official Says." ABC News. January 6, 2026. https://abcnews.go.com/Politics/us-military-option-acquiring-greenland-white-house-official/story?id=128960041.
31. Ray, Trisha. 2025a. "Sovereign Remedies: Between AI Autonomy and Control." Atlantic Council. April 3, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sovereign-remedies-between-ai-autonomy-and-control/.
32. Ustun, Ali, Arnaud Tournesac, Luca Bennici, Kaavini Takkar, and Newfel Drahmoune. 2025. "The Sovereign AI Agenda: Moving from Ambition to Reality." McKinsey & Company. December 18, 2025. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/the-sovereign-ai-agenda-moving-from-ambition-to-reality.
33. Faisal, Aldo, David Shrier, Ayisha Piotti, and Alex Pentland. 2024a. "Considerations Regarding Sovereign AI and National AI Policy." https://sovereign-ai.org/media/papers/Considerations_regarding_Sovereign_AI_C_Sovereign_AI__Imperial_College.pdf.
34. "Three National Approaches towards Sovereign AI." 2025. The International Institute for Strategic Studies. 2025. https://www.iiss.org/charting-cyberspace/2025/08/three-national-approaches-towards-sovereign-ai/.
35. "Competition, Innovation, and Research | National Telecommunications and Information Administration." 2023. Ntia.gov. 2023. https://www.ntia.gov/programs-and-initiatives/artificial-intelligence/open-model-weights-report/risks-benefits-of-dual-use-foundation-models-with-widely-available-model-weights/competition-innovation-research.
36. "SEA-LION.AI." 2024a. SEA-LION.AI. 2024. https://sea-lion.ai/.
37. Chandran, Rina. 2024. "Biased GPT? Singapore Builds AI Model to 'Represent' Southeast Asians." Context.news. Context. February 8, 2024. https://www.context.news/ai/singapore-builds-ai-model-to-represent-southeast-asians.
38. "TAIDE." 2026. TAIDE. 2026. https://en.taide.tw/.
39. Bastian, Matthias. 2024. "Taiwan's 'Trustworthy AI Dialogue Engine' Aims to Counter China's Grip on AI Ecosystem." The Decoder. January 26, 2024. https://the-decoder.com/taiwans-trustworthy-ai-dialogue-engine-aims-to-counter-chinas-grip-on-ai-ecosystem/.
40. Tobin, Meaghan, and Xinyun Wu. 2026. "Move Fast, but Obey the Rules: China's Vision for Dominating A.I." The New York Times. February 6, 2026. https://www.nytimes.com/2026/02/02/business/china-ai-regulations.html.
41. Faisal, Aldo, David Shrier, Ayisha Piotti, and Alex Pentland. 2024b. "Considerations Regarding Sovereign AI and National AI Policy." https://sovereign-ai.org/media/papers/Considerations_regarding_Sovereign_AI_C_Sovereign_AI__Imperial_College.pdf.
42. OECD. 2024a. "AI Principles." OECD. 2024. https://www.oecd.org/en/topics/ai-principles.html.
43. ———. "About | OECD.AI | HAIP Reporting Frame-

END NOTES

work." 2023. OECD.ai. 2023. https://transparency.oecd.ai/about.

44. Chavez, Pablo. 2024a. "Sovereign AI in a Hybrid World: National Strategies and Policy Responses." Lawfare. 2024. https://www.lawfaremedia.org/article/sovereign-ai-in-a-hybrid-world--national-strategies-and-policy-responses.
45. Kizrak, Merve Ayyüce. 2025. "AI Policy Bulletin." Aipolicybulletin.org. 2025. https://www.aipolicybulletin.org/articles/middle-powers-can-gain-ai-influence-without-building-the-next-chatgpt.
46. Stewart, Sara. 2025. "AI, Energy, and Geopolitics." Foreignpolicy.com. FP Analytics. March 3, 2025. https://fpanalytics.foreignpolicy.com/2025/03/03/artificial-intelligence-energy-geopolitics-data-centers/.
47. Esposito, Mark. 2025. "AI Geopolitics and Data in the Era of Technological Rivalry." World Economic Forum. July 24, 2025. https://www.weforum.org/stories/2025/07/ai-geopolitics-data-centres-technological-rivalry/.
48. Narechania, Tejas N., and Ganesh Sitaraman. 2024a. "An Antimonopoly Approach to Governing Artificial Intelligence." Yale Law & Policy Review. 2024. https://yalelawandpolicy.org/antimonopoly-approach-governing-artificial-intelligence.
49. Feldstein, Steven. 2025. "Digital Democracy in a Divided Global Landscape." Carnegie Endowment for International Peace. 2025. https://carnegieendowment.org/research/2025/05/digital-democracy-in-a-divided-global-landscape?lang=en.
50. Nestor Maslej, Loredana Fattorini, Raymond Perrault, Yolanda Gil, Vanessa Parli, Njenga Kariuki, Emily Capstick, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, Toby Walsh, Armin Hamrah, Lapo Santarlasci, Julia Betts Lotufo, Alexandra Rome, Andrew Shi, and Sukrut Oak. 2025b. "The 2025 AI Index Report." AI Index Steering Committee, Institute for Human-Centered AI, Stanford University. April 2025. https://hai.stanford.edu/ai-index/2025-ai-index-report;
51. Zwetsloot, Remco. 2019. "Keeping Top AI Talent in the United States." Center for Security and Emerging Technology. December 2019. https://cset.georgetown.edu/publication/keeping-top-ai-talent-in-the-united-states/.
52. Larsen, Benjamin Cedric. 2022. "The Geopolitics of AI and the Rise of Digital Sovereignty." Brookings. December 8, 2022. https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/.
53. Roberts, Huw. 2024. "Digital Sovereignty and Artificial Intelligence: A Normative Approach." Ethics and Information Technology 26 (4). https://doi.org/10.1007/s10676-024-09810-5.
54. Cherif, Reda, and Fuad Hasanov. 2024. "The Pitfalls of Protectionism: Import Substitution vs. Export-Oriented Industrial Policy." Journal of Industry, Competition and Trade 24 (1). https://doi.org/10.1007/s10842-024-00414-9.
55. Srivastava, Swati, and Justin Bullock. 2024. "AI, Global Governance, and Digital Sovereignty." https://arxiv.org/pdf/2410.17481.
56. Scassa, Teresa. 2023. "Sovereignty and the Governance of Artificial Intelligence." https://www.uclalawreview.org/wp-content/uploads/securepdfs/2024/05/06-Scassa-No-Bleed.pdf.
57. Bauer, Matthias, and Dyuti Pandya. 2024. "EU Autonomy, the Brussels Effect, and the Rise of Global Economic Protectionism |." Ecipe.org. February 2024. https://ecipe.org/publications/eu-autonomy-brussels-effect-rise-global-economic-protectionism/.
58. Chavez, Pablo. 2024b. "Sovereign AI in a Hybrid World: National Strategies and Policy Responses." Lawfare. 2024. https://www.lawfaremedia.org/article/sovereign-ai-in-a-hybrid-world--national-strategies-and-policy-responses.
59. "AI Action Plan." 2025. AI.gov. 2025. https://www.ai.gov/action-plan.
60. "Promoting the Export of the American AI Technology Stack." 2025. The White House. July 23, 2025.

END NOTES

https://www.whitehouse.gov/presidential-actions/2025/07/promoting-the-export-of-the-american-ai-technology-stack/.

61. "The Department of Commerce Announces American AI Exports Program Implementation." Trade.gov. International Trade Administration. 2025. https://www.trade.gov/press-release/department-commerce-announces-american-ai-exports-program-implementation.
62. Kif Leswing. 2025. "U.S. Government Takes 10% Stake in Intel, as Trump Expands Control over Private Sector." CNBC. August 22, 2025. https://www.cnbc.com/2025/08/22/intel-goverment-equity-stake.html?msockid=32edd8d44fc26acd1e8bce5f4e496b1e.
63. Morescalchi, Daniela. 2025. "Intel and Trump Administration Reach Historic Agreement to Accelerate American Technology and Manufacturing Leadership." Newsroom. August 22, 2025. https://newsroom.intel.com/corporate/intel-and-trump-administration-reach-historic-agreement.
64. Romm, Tony, and Ana Swanson. 2025. "After U.S. Takes Stake in Intel, Trump Pledges 'Many More' Deals." The New York Times, August 25, 2025. https://www.nytimes.com/2025/08/25/us/politics/trump-intel-economy-strategy.html.
65. Brown, Kristin, and Kathryn Watson. 2026. "Trump Announces $12 Billion U.S. Stockpile of Rare Earth Minerals." Cbsnews.com. February 2, 2026. https://www.cbsnews.com/news/trump-rare-earth-minerals-stockpile-12-billion/.
66. McCormick, Dave. 2025. "Fact Sheet: More than $90 Billion in Investments Announced at Senator Mccormick's Pennsylvania Energy and Innovation Summit." Senator Dave McCormick. July 15, 2025. https://www.mccormick.senate.gov/press-releases/fact-sheet-more-than-90-billion-in-investments-announced-at-senator-mccormicks-pennsylvania-energy-and-innovation-summit/.
67. Hakas, Abigail. 2025. "$90 Billion in Investment Announced for AI and Energy in Pennsylvania | Pittsburgh Magazine." Pittsburgh Magazine. July 15, 2025. https://www.pittsburghmagazine.com/90-billion-in-investment-announced-for-ai-and-energy-in-pennsylvania/.
68. OpenAI. 2025. "Announcing the Stargate Project." Openai.com. January 21, 2025. https://openai.com/index/announcing-the-stargate-project/.
69. Bria, Francesca, Paul Timmers, and Fausto Gernone. 2025a. "EuroStack - a European Alternative for Digital Sovereignty." Bertelsmann-Stiftung.de. February 13, 2025. https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty.
70. "Frontiers in Artificial Intelligence for Science, Security and Technology (FASST)." 2024. Energy.gov. 2024. https://www.energy.gov/fasst.
71. Ditchey II, Robert L. 2025. "DOD Introduces New Supercomputer Focused on Biodefense Capabilities." U.S. Department of Defense. 2025. https://www.defense.gov/News/Releases/Release/Article/3875539/dod-introduces-new-supercomputer-focused-on-biodefense-capabilities/.
72. "NASA Advanced Supercomputing Division Website." n.d. NASA Advanced Supercomputing (NAS) Division. https://www.nas.nasa.gov/.
73. "Artificial Intelligence | NSF - National Science Foundation." n.d. U.S. National Science Foundation. https://new.nsf.gov/focus-areas/artificial-intelligence.
74. Habuka, Hiroki, and David U. Socol de la Osa. 2024. "Shaping Global AI Governance: Enhancements and next Steps for the G7 Hiroshima AI Process." Center for Strategic and International Studies. https://www.csis.org/analysis/shaping-global-ai-governance-enhancements-and-next-steps-g7-hiroshima-ai-process.
75. Mohanty, Amlan, and Tejas Bharadwaj. 2024. "The Importance of AI Safety Institutes." Carnegie Endowment for International Peace. June 28, 2024. https://carnegieendowment.org/posts/2024/08/the-importance-of-ai-safety-institutes.

END NOTES

76. "Maintaining American Leadership in Artificial Intelligence." 2019. Federal Register. February 14, 2019. https://www.federalregister.gov/d/2019-02544/p-2.
77. "National Security Strategy of the United States of America." 2025. The White House. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.
78. Akhter, Afreen. 2025a. "From Caution to Competition: Positioning U.S. Development Finance for Industrial Power." Carnegie Endowment for International Peace. December 2025. https://carnegieendowment.org/research/2025/11/from-caution-to-competition-positioning-us-development-finance-for-industrial-power.
79. "DFC's Global Portfolio Surpasses $40 Billion across More than 100 Countries | DFC." 2023. Dfc.gov. December 13, 2023. https://www.dfc.gov/media/press-releases/dfcs-global-portfolio-surpasses-40-billion-across-more-100-countries.
80. Akhter, Afreen. 2025a. "From Caution to Competition: Positioning U.S. Development Finance for Industrial Power." Carnegie Endowment for International Peace. December 2025. https://carnegieendowment.org/research/2025/11/from-caution-to-competition-positioning-us-development-finance-for-industrial-power.
81. "DFC Secures Expanded Authorities with FY26 NDAA Signed into Law | DFC." 2025. Dfc.gov. December 18, 2025. https://www.dfc.gov/media/press-releases/dfc-secures-expanded-authorities-fy26-ndaa-signed-law.
82. "China - U.S. Export Controls." 2025. Www.trade.gov. September 25, 2025. https://www.trade.gov/country-commercial-guides/china-us-export-controls.
83. Sutter, Karen M. 2025a. "U.S. Export Controls and China: Advanced Semiconductors." Congress.gov. 2025. https://www.congress.gov/crs-product/R48642.
84. Villasenor, John. 2024. "The Tension between AI Export Control and U.S. AI Innovation." Brookings. September 24, 2024. https://www.brookings.edu/articles/the-tension-between-ai-export-control-and-u-s-ai-innovation/.
85. Sutter, Karen M. 2025b. "U.S. Export Controls and China: Advanced Semiconductors." Congress.gov. 2025. https://www.congress.gov/crs-product/R48642.
86. "Framework for Artificial Intelligence Diffusion." 2025. Federal Register. January 15, 2025. https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion.
87. "Department of Commerce Announces Rescission of Biden-Era Artificial Intelligence Diffusion Rule, Strengthens Chip-Related Export Controls." 2025. Bis.gov. 2025. https://www.bis.gov/press-release/department-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens.
88. "United States Assumes Presidency of the Group of 20." 2025. United States Department of State. December 18, 2025. https://www.state.gov/releases/2025/12/united-states-assumes-presidency-of-the-group-of-20/.
89. Stein, Jeff, and John Hudson. 2025. "White House Bans U.S. Agencies from All Work on G-20 in South Africa." The Washington Post. May 14, 2025. https://www.washingtonpost.com/business/2025/05/14/white-house-g20-boycott-talks/.
90. "Fact Sheet: President Donald J. Trump Withdraws the United States from International Organizations That Are Contrary to the Interests of the United States." 2026a. The White House. January 7, 2026. https://www.whitehouse.gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-withdraws-the-united-states-from-international-organizations-that-are-contrary-to-the-interests-of-the-united-states.
91. Chang, Wendy, Rebecca Arcesati, and Antonia Hmaidi. 2025. "China's Drive toward Self-Reliance in Artificial Intelligence: From Chips to Large

END NOTES

Language Models." Merics, July. https://doi.org/10.48550/arXiv.2503.0513922.

92. Chan, Kyle, Gregory Smith, Jimmy Goodrich, Gerard DiPippo, and Konstantin F Pilz. 2025a. "Full Stack: China's Evolving Industrial Policy for AI." Rand.org. RAND Corporation. June 26, 2025. https://www.rand.org/pubs/perspectives/PEA4012-1.html.
93. Tobin, Meaghan. 2025a. "China Is Spending Billions to Become an A.I. Superpower." The New York Times, July 16, 2025. https://www.nytimes.com/2025/07/16/technology/china-ai.html.
94. "The Chinese Firewall - Internet Society." 2023. Internet Society. December 13, 2023. https://www.internetsociety.org/resources/internet-fragmentation/the-chinese-firewall.
95. Musoni, Melody, Poorva Karkare, Chloe Teevan, and Ennatu Domingo. 2023. "Global Approaches to Digital Sovereignty: Competing Definitions and Contrasting Policy." https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf.
96. Kurlantzick, Joshua, and James West. 2015. "China's Digital Aid: The Risks and Rewards." Edited by Patricia Lee Dorff. Council on Foreign Relations. 2015. https://www.cfr.org/china-digital-silk-road.
97. "Artificial Intelligence Standardization White Paper (2021 Edition)." 2021. Center for Security and Emerging Technology. October 21, 2021. https://cset.georgetown.edu/publication/artificial-intelligence-standardization-white-paper-2021-edition/.
98. Xu, Xiaofei. 2025. "South China Morning Post." South China Morning Post. June 11, 2025. https://www.scmp.com/economy/china-economy/article/3314001/ai-chips-china-courts-private-tech-firms-help-drive-next-5-year-plan.
99. □□□. 2025. "Guideline to Develop AI-Backed Chinese Language Database." Www.gov.cn. 2025. https://english.www.gov.cn/news/202504/01/content_WS67eb5752c6d0868f4e8f15dd.html.
100. Tobin, Meaghan, and Claire Fu. 2025. "DeepSeek Is Embraced in China by Government Nationwide." The New York Times, March 18, 2025. https://www.nytimes.com/2025/03/18/business/china-government-deepseek.html.
101. Deng, Iris. 2024. "Tencent boosts AI training efficiency without Nvidia's most advanced chips." South China Morning Post. July 2, 2024. https://www.scmp.com/tech/big-tech/article/3268901/tencent-boosts-ai-training-efficiency-without-nvidias-most-advanced-chips.
102. □□□. 2023. "China Accelerates Building of National Computing Power Network." Www.gov.cn. 2023. https://english.www.gov.cn/news/202312/27/content_WS658b72afc6d0868f4e8e28ba.html.
103. Chan, Kyle, Gregory Smith, Jimmy Goodrich, Gerard DiPippo, and Konstantin F Pilz. 2025b. "Full Stack: China's Evolving Industrial Policy for AI." Rand.org. RAND Corporation. June 26, 2025. https://www.rand.org/pubs/perspectives/PEA4012-1.html.
104. □□. 2025. "□□□□□□□□□'□□□□+'□□□□□_□□_□□□□□." Www.gov.cn. 2025. https://www.gov.cn/zhengce/content/202508/content_7037861.htm.
105. Chang, Wendy. 2025. "China's 'AI+' Drive Aims for Integration across Sectors: A Wake-up Call for Europe." Merics. October 2, 2025. https://merics.org/en/comment/chinas-ai-drive-aims-integration-across-sectors-wake-call-europe.
106. Rafiq Dossani, and Shanshan Mei. 2025. "China: An Emerging Software Power." Rand.org. RAND Corporation. October 28, 2025. https://www.rand.org/pubs/commentary/2025/10/china-an-emerging-software-power.html.
107. Meinhardt, Caroline, Sabina Nong, Graham Webster, Tatsunori Hashimoto, and Christopher D. Manning. 2025. "Key Takeaways." https://hai.stanford.edu/assets/files/hai-digichina-issue-brief-beyond-deepseek-chinas-diverse-open-weight-ai-ecosystem-policy-implications.pdf.
108. White & Case. 2024. "AI Watch: Global

END NOTES

Regulatory Tracker - China." White & Case LLP. May 13, 2024. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china.

109. Prado, Borja. 2021. "India's Quest for Digital Sovereignty." Atlantic Council. January 12, 2021. https://www.atlanticcouncil.org/blogs/geotech-cues/indias-quest-for-digital-sovereignty/.

110. "Global AI Governance Action Plan_Ministry of Foreign Affairs of the People's Republic of China." 2025a. Mfa.gov.cn. 2025. https://www.mfa.gov.cn/eng/xw/zyxw/202507/t20250729_11679232.html.

111. "Global AI Governance Initiative_Ministry of Foreign Affairs of the People's Republic of China." 2023. Mfa.gov.cn. 2023. https://www.mfa.gov.cn/eng/zy/gb/202405/t20240531_11367503.html.

112. "The Role China Plays in International Technology Standards Setting | George H. W. Bush Foundation for U.S.-China Relations." 2021. Bushchinafoundation.org. 2021. https://bushchinafoundation.org/recent-activities/chinese-foreign-policy-toward-central-asia-and-the-silk-roads/.

113. Patil, Sameer, and Prithvi Gupta. 2023. "China's Expanding Tech Lead through Digital Silk Road." Orfonline.org. June 23, 2023. https://www.orfonline.org/expert-speak/chinas-expanding-tech-lead-through-digital-silk-road.

114. Patil, Sameer. 2025. "The Digital Silk Road and Smart City Networks in the Indo-Pacific: A Primer." Orfonline.org. Observer Research Foundation (ORF). September 8, 2025. https://www.orfonline.org/research/the-digital-silk-road-and-smart-city-networks-in-the-indo-pacific-a-primer.

115. World Bank. 2024. "GDP (Current US$) | Data." Worldbank.org. World Bank. 2024. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true.

116. "EUR-Lex - 52018DC0237 - Artificial Intelligence for Europe." 2018. Eur-Lex.europa.eu. April 25, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:237:FIN.

117. Bradford, Anu. 2019b. The Brussels Effect: How the European Union Rules the World. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001.

118. European Commission. 2025a. "AI Act." European Commission. August 1, 2025. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

119. Pouget, Hadrien, and Ranj Zuhdi. 2024. "AI and Product Safety Standards under the EU AI Act." Carnegie Endowment for International Peace. March 5, 2024. https://carnegieendowment.org/research/2024/03/ai-and-product-safety-standards-under-the-eu-ai-act?lang=en.

120. "Article 5: Prohibited Artificial Intelligence Practices | EU Artificial Intelligence Act." 2025. EU Artificial Intelligence Act. February 2, 2025. https://artificialintelligenceact.eu/article/5/.

121. European Commission. 2020. "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust." Commission.europa.eu. February 19, 2020. https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

122. Bria, Francesca, Paul Timmers, and Fausto Gernone. 2025b. "EuroStack - a European Alternative for Digital Sovereignty." Bertelsmann-Stiftung.de. February 13, 2025. https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty.

123. "AI Innovation Package | Shaping Europe's Digital Future." 2024. Europa.eu. 2024. https://digital-strategy.ec.europa.eu/en/factpages/ai-innovation-package.

124. CNBC. 2022. "Why the World Relies on ASML for Machines That Print Chips." YouTube. https://www.youtube.com/watch?v=iSVHp6CAyQ8.

125. "The EESC Assesses Europe's 'Third Way' to Digitalisation." 2022. European Economic and Social Committee. June 16, 2022. https://www.eesc.europa.eu/en/news-media/press-releases/

END NOTES

eesc-assesses-europes-third-way-digitalisation.

126. Bria, Francesca, Paul Timmers, and Fausto Gernone. 2025c. “EuroStack - a European Alternative for Digital Sovereignty.” Bertelsmann-Stiftung.de. February 13, 2025. https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty.

127. ———. 2025d. “EuroStack - a European Alternative for Digital Sovereignty.” Bertelsmann-Stiftung.de. February 13, 2025. https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty.

128. ———. 2025e. “EuroStack - a European Alternative for Digital Sovereignty.” Bertelsmann-Stiftung.de. February 13, 2025. https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty.

129. Schwaag-Serger, Sylvia, Luc Soete, and Johan Stierna. 2024. “Scientific Report - for an Innovative, Sustainable and Fair Economy in Europe.” JRC Publications Repository. https://doi.org/10.2760/0336180.

130. “Euro Stack | Building Europe’s Digital Future.” 2026. EuroStack. January 10, 2025. https://euro-stack.eu/wp-content/uploads/2025/01/EuroStack_Pitch_10-January-2025.pdf.

131. Bria, Francesca, Paul Timmers, and Fausto Gernone. 2025f. “EuroStack - a European Alternative for Digital Sovereignty.” Bertelsmann-Stiftung.de. February 13, 2025. https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty.

132. European Commission. 2023b. “Critical Raw Materials Act.” European Commission. 2023. https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/critical-raw-materials-act_en.

133. “The European Interoperability Framework in Detail.” 2026. Interoperable Europe Portal. 2026. https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail.

134. “EU Digital Identity Wallet Home - EU Digital Identity Wallet.” n.d. Ec.europa.eu. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home.

135. Bria, Francesca, Paul Timmers, and Fausto Gernone. 2025g. “EuroStack - a European Alternative for Digital Sovereignty.” Bertelsmann-Stiftung.de. February 13, 2025. https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty.

136. European Commission. 2025a. “The AI Continent Action Plan.” Shaping Europe’s Digital Future. 2025. https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan.

137. “EU Launches InvestAI Initiative to Mobilise €200 Billion of Investment in Artificial Intelligence.” 2025. European Commission - European Commission. 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_467.

138. “Cloud Computing | Shaping Europe’s Digital Future.” n.d. Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/policies/cloud-computing.

139. “Apply AI Strategy.” 2025. Shaping Europe’s Digital Future. 2025. https://digital-strategy.ec.europa.eu/en/policies/apply-ai.

140. “European Commission - Have Your Say.” European Commission - Have Your Say. 2026. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16213-European-Open-Digital-Ecosystems_en.

141. Domen Vake, Bogdan Šinik, Jernej Vičič, and Aleksandar Tošić. 2025. “Is Open Source the Future of AI? A Data-Driven Approach.” Applied Sciences 15 (5): 2790–90. https://doi.org/10.3390/

END NOTES

app15052790.

142. Cottier, Ben. 2024. “How Far Behind Are Open Models?” Epoch AI. November 4, 2024. https://epoch.ai/blog/open-models-report.

143. Elysee. 2025a. “Germany, France and the European Commission Launch Frontier AI Initiative at the Summit on European Digital Sovereignty.” Elysee.fr. November 18, 2025. https://www.elysee.fr/en/emmanuel-macron/2025/11/18/germany-france-and-the-european-commission-launch-frontier-ai-initiative-at-the-summit-on-european-digital-sovereignty.

144. ———. 2025b. “Germany, France and the European Commission Launch Frontier AI Initiative at the Summit on European Digital Sovereignty.” Elysee.fr. November 18, 2025. https://www.elysee.fr/en/emmanuel-macron/2025/11/18/germany-france-and-the-european-commission-launch-frontier-ai-initiative-at-the-summit-on-european-digital-sovereignty.

145. “ASML, Mistral AI Enter Strategic Partnership.” 2025. ASML. September 9, 2025. https://www.asml.com/en/news/press-releases/2025/asml-mistral-ai-enter-strategic-partnership.

146. Hett, Simone. 2025. “SAP and Mistral AI: A New Alliance for European Sovereign AI.” SAP News Center. November 18, 2025. https://news.sap.com/2025/11/sap-mistral-ai-new-alliance-european-sovereign-ai/.

147. Zenner, Kai, J Scott, and Marcus Sekut. 2025. “A Dataset of Eu Legal and Policy Instruments for the Digital World.” https://cdn.ceps.eu/2025/08/CEPS-Zenner-Dataset-July-2025.pdf.

148. Barysas, Martynas, and Michelle Marie Philipp. 2025. “Reducing Regulatory Burden to Restore the EU’s Competitive Edge.” BusinessEurope. April 4, 2025. https://www.businesseurope.eu/publications/reducing-regulatory-burden-to-restore-the-eus-competitive-edge/.

149. “Open Letter on the Digital Omnibus Proposal.” 2025. Union of Entrepreneurs and Employers (ZPP). December 9, 2025. https://zpp.net.pl/en/open-letter-on-the-digital-omnibus-proposal/.

150. Pagallo, Ugo. 2025. “LLMs Meet the AI Act: Who’s the Sorcerer’s Apprentice?” Cambridge Forum on AI: Law and Governance 1. https://doi.org/10.1017/cfl.2024.6.

151. “Digital Omnibus Regulation Proposal.” 2025. Shaping Europe’s Digital Future. 2025. https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal.

152. Teevan, Chloe, Raphael Pouyé, and Gautam Kamath. 2025a. “From India Stack to EuroStack: Reconciling Approaches to Sovereign Digital Infrastructure .” https://ecdpm.org/application/files/2117/3874/5474/From-India-Stack-to-EuroStack-Reconciling-Approaches-Sovereign-Digital-Infrastructure-ECDPM-Discussion-Paper-384.pdf.

153. ———. 2025b. “From India Stack to EuroStack: Reconciling Approaches to Sovereign Digital Infrastructure.” https://ecdpm.org/application/files/2117/3874/5474/From-India-Stack-to-EuroStack-Reconciling-Approaches-Sovereign-Digital-Infrastructure-ECDPM-Discussion-Paper-384.pdf.

154. United Nations. 2024a. “Global Digital Compact | Office for Digital and Emerging Technologies.” Un.org. 2024. https://www.un.org/digital-emerging-technologies/global-digital-compact.

155. “Global DPI Summit 2025.” 2025. Globaldpisummit.org. 2025. https://www.globaldpisummit.org/.

156. ———. 2025c. “From India Stack to EuroStack: Reconciling Approaches to Sovereign Digital Infrastructure.” https://ecdpm.org/application/files/2117/3874/5474/From-India-Stack-to-EuroStack-Reconciling-Approaches-Sovereign-Digital-Infrastructure-ECDPM-Discussion-Paper-384.pdf.

157. “Quad Principles for Development and Deployment of Digital Public Infrastructure - United States Department of State.” 2021. United States Department of State. 2021. https://2021-2025.

END NOTES

state.gov/quad-principles-for-development-and-deployment-of-digital-public-infrastructure/.

158. Ghosh, Debjani. 2025. "A Vision for Sovereign AI: Building India's Self-Reliant AI Future." The Economic Times. 2025. https://economictimes.indiatimes.com/tech/artificial-intelligence/a-vision-for-sovereign-ai-building-indias-self-reliant-ai-future/articleshow/117562048.cms?-from=mdr.

159. "IndiaStack – Technology for 1.2 Billion Indians." n.d. IndiaStack. https://indiastack.org/.

160. Eaves, David, and Beatriz Vasconcellos. 2025. "Digital Public Infrastructure Is the New Global Tech Bet—but Everyone's Betting on Something Different." Tech Policy Press. April 2025. https://www.techpolicy.press/digital-public-infrastructure-is-the-new-global-tech-bet-but-everyones-betting-on-something-different/.

161. "INDIAai | about Us." n.d. Indiaai.gov.in. https://indiaai.gov.in/about-us.

162. Sarvesh M. 2023. "Countries like India Are Investing in Sovereign AI Infra: Nvidia." MEDIANAMA. November 23, 2023. https://www.medianama.com/2023/11/223-nvidia-earnings-call-q3fy24/.

163. Dixit, Pranav. 2023. "Our Goal Is Not to Compete with Sam Altman or Elon Musk, Says MoS IT Rajeev Chandrasekhar on AI." Business Today. December 6, 2023. https://www.businesstoday.in/technology/news/story/our-goal-is-not-to-compete-with-sam-altman-or-elon-musk-says-mos-it-rajeev-chandrasekhar-on-ai-408406-2023-12-06.

164. Grover, Jatin. 2023. "India to Develop Its Own Sovereign AI Infrastructure: Rajeev Chandrasekhar." Financial Express. November 30, 2023. https://www.financialexpress.com/business/digital-transformation-india-to-develop-its-own-sovereign-ai-infrastructure-rajeev-chandrasekhar-3321291/.

165. "India's Critical Mineral Mission: Securing the Minerals of Tomorrow." 2025. https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/sep/doc202596629501.pdf.

166. "AI Safety Summit 2023: The Bletchley Declaration." 2023. GOV.UK. November 1, 2023. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration.

167. "The AI Safety Institute (AISI)." n.d. Www.aisi.gov.uk. https://www.aisi.gov.uk/.

168. Department for Science, Innovation and Technology. 2025. "Sovereign AI Unit." GOV.UK. July 16, 2025. https://www.gov.uk/government/collections/sovereign-ai-unit.

169. "£300 Million to Launch First Phase of New AI Research Resource." 2023. Ukri.org. November 2023. https://www.ukri.org/news/300-million-to-launch-first-phase-of-new-ai-research-resource.

170. Gov.uk. 2025. "Artificial Intelligence Sector Study 2024." GOV.UK. September 3, 2025. https://www.gov.uk/government/publications/artificial-intelligence-sector-study-2024/artificial-intelligence-sector-study-2024.

171. "Who's Leading the Global AI Race?." 2025. Stanford.edu. November 24, 2025. https://hai.stanford.edu/ai-index/global-vibrancy-tool.

172. "The Hiroshima AI Process: Leading the Global Challenge to Shape Inclusive Governance for Generative AI." n.d. The Government of Japan - JapanGov -. https://www.japan.go.jp/kizuna/2024/02/hiroshima_ai_process.html.

173. "Data Free Flow with Trust." 2024a. OECD. 2024. https://www.oecd.org/en/about/programmes/data-free-flow-with-trust.html.

174. "ABCI." 2018. Abci.ai. 2018. https://abci.ai/ja/.

175. "ABCI 3.0: Evolution of the Leading AI Infrastructure in Japan." 2024. Arxiv.org. 2024. https://arxiv.org/html/2411.09134v1.

176. Harris, Dion. 2024. "Japan Enhances AI Sovereignty with Advanced ABCI 3.0 Supercomputer." NVIDIA Blog. July 11, 2024. https://blogs.nvidia.com/blog/abci-aist/.

177. "Release of 'Fugaku-LLM' – a Large Language Model Trained on the Supercomputer 'Fugaku.'" 2020. Fujitsu Global. 2020. https://www.fujitsu.com/global/about/resources/news/press-releas-

END NOTES

es/2024/0510-01.html.

178. "Approval of Plans for Ensuring a Stable Supply of Cloud Programs under the Economic Security Promotion Act." 2024. Meti.go.jp. 2024. https://www.meti.go.jp/english/press/2024/0419_001.html.

179. Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry. 2024. "AI Guidelines for Business Ver1.0." https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_9.pdf.

180. "Press Releases - □□□□□□□□□ >." 2025. Msit.go.kr. 2025. https://www.msit.go.kr/eng/bbs/view.do?bbsSeqNo=42&mId=4&nttSeqNo=1152&sCode=eng.

181. Reuters Staff. 2025b. "South Korea Says SK and Amazon to Invest $5 Billion in Country's Biggest Data Centre." Reuters, June 20, 2025. https://www.reuters.com/business/retail-consumer/south-korea-says-sk-amazon-invest-5-bln-countrys-biggest-data-centre-2025-06-20/.

182. ———. 2026b. "SK Hynix to Invest Nearly $13 Bln in Chip Packaging Plant in South Korea." Reuters, January 13, 2026. https://www.reuters.com/world/asia-pacific/sk-hynix-invest-nearly-13-bln-chip-packaging-plant-south-korea-2026-01-13/.

183. "Press Releases - □□□□□□□□□ >." 2024. Msit.go.kr. 2024. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=1071&searchOpt=ALL.

184. Phillips, Justine, Beomsu Kim, Byungchul Kim, and Hyunuk Lee. 2026. "South Korea Sets AI Standard: PIPC's Guidelines for Generative AI Present Obligations & Opportunity." Bakermckenzie.com. August 26, 2026. https://connectontech.bakermckenzie.com/south-korea-sets-ai-standard-pipcs-guidelines-for-generative-ai-present-obligations-opportunity/.

185. Althoff, Judson. 2024. "Microsoft and G42 Partner to Accelerate AI Innovation in UAE and beyond - the Official Microsoft Blog." The Official Microsoft Blog. April 16, 2024. https://blogs.microsoft.com/blog/2024/04/15/microsoft-and-g42-partner-to-accelerate-ai-innovation-in-uae-and-beyond/.

186. Chavez, Pablo. 2025a. "U.S. AI Statecraft." Center for Security and Emerging Technology. October 2, 2025. https://cset.georgetown.edu/publication/u-s-ai-statecraft/.

187. "Introducing Stargate UAE." 2025. Openai.com. 2025. https://openai.com/index/introducing-stargate-uae/.

188. "Homepage." 2026. MGX. 2026. https://www.mgx.ae/en.

189. "Falcon LLM." n.d. Falconllm.tii.ae. https://falconllm.tii.ae/.

190. "Meet 'Jais', the World's Most Advanced Arabic Large Language Model Open Sourced by G42'S Inception." 2023. MBZUAI. August 30, 2023. https://mbzuai.ac.ae/news/meet-jais-the-worlds-most-advanced-arabic-large-language-model-open-sourced-by-g42s-inception/.

191. Government of Canada. 2022. "Government of Canada Launches Second Phase of the Pan-Canadian Artificial Intelligence Strategy." Www.canada.ca. June 22, 2022. https://www.canada.ca/en/innovation-science-economic-development/news/2022/06/government-of-canada-launches-second-phase-of-the-pan-canadian-artificial-intelligence-strategy.html.

192. Government of Canada, Innovation. 2020. "Canada's AI-Powered Supply Chains Cluster (Scale AI)." Ised-Isde.canada.ca. December 1, 2020. https://ised-isde.canada.ca/site/global-innovation-clusters/en/canadas-ai-powered-supply-chains-cluster-scale-ai.

193. Service Canada. 2022. "The Canadian Critical Minerals Strategy." Www.canada.ca. December 9, 2022. https://www.canada.ca/en/campaign/critical-minerals-in-canada/canadian-critical-minerals-strategy.html.

194. Critical Minerals Office. 2023. "Critical Minerals Strategy 2023–2030." Industry.gov.au. June 19, 2023. https://www.industry.gov.au/publications/

END NOTES

critical-minerals-strategy-2023-2030.

195. "United States-Australia Framework for Securing of Supply in the Mining and Processing of Critical Minerals and Rare Earths." 2025a. The White House. October 20, 2025. https://www.whitehouse.gov/briefings-statements/2025/10/united-states-australia-framework-for-securing-of-supply-in-the-mining-and-processing-of-critical-minerals-and-rare-earths/.

196. "BMFTR-Aktionsplan 'Künstliche Intelligenz.'" 2024. Bundesministerium Für Forschung, Technologie Und Raumfahrt - BMFTR. BMBF. November 25, 2024. https://www.bmftr.bund.de/DE/Forschung/Schluesseltechnologien/KuenstlicheIntelligenz/KiAktionsplan/kiaktionsplan_node.html.

197. Federal Ministry for Economic Affairs and Energy, and Federal Ministry of Research, Technology and Space. "What is the Plattform Industrie 4.0?" n.d. Plattform Industrie 4.0. https://www.plattform-i40.de/IP/Navigation/EN/Home/home.html.

198. "SEA-LION.AI." 2024b. SEA-LION.AI. 2024. https://sea-lion.ai/.

199. Chavez, Pablo. 2024c. "Sovereign AI in a Hybrid World: National Strategies and Policy Responses." Default. 2024. https://www.lawfaremedia.org/article/sovereign-ai-in-a-hybrid-world--national-strategies-and-policy-responses.

200. Ray, Trisha. 2025b. "Sovereign Remedies: Between AI Autonomy and Control." Atlantic Council. April 3, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sovereign-remedies-between-ai-autonomy-and-control/.

201. "Singapore Launches World's First AI Testing Framework and Toolkit to Promote Transparency; Invites Companies to Pilot and Contribute to International Standards Development." n.d. Infocomm Media Development Authority. https://www.imda.gov.sg/resources/press-releases-fact-sheets-and-speeches/press-releases/2022/sg-launches-worlds-first-ai-testing-framework-and-toolkit-to-promote-transparency.

202. "AISI - the Singapore AI Safety Institute." 2025. AISI. January 25, 2025. https://www.sgaisi.sg/.

203. Ismail, Netty Idayu. 2025. "Malaysia's Data Center Hub Tightens Approvals on Water Worries." Bloomberg.com. Bloomberg. November 26, 2025. https://www.bloomberg.com/news/articles/2025-11-26/malaysia-s-data-center-hub-tightens-approvals-on-water-worries.

204. "Cumulative Number of Large-Scale AI Systems by Country since 2017." 2017a. Our World in Data. 2017. https://ourworldindata.org/grapher/cumulative-number-of-large-scale-ai-systems-by-country?tab=table.

205. Nestor Maslej, Loredana Fattorini, Raymond Perrault, Vanessa Parli, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, and Jack Clark. 2024a. "The AI Index 2024 Annual Report." AI Index Steering Committee. Institute for Human-Centered AI. Stanford University. April 2024. https://hai.stanford.edu/ai-index/2024-ai-index-report.

206. ———. 2024b. "The AI Index 2024 Annual Report." AI Index Steering Committee. Institute for Human-Centered AI. Stanford University. April 2024. https://hai.stanford.edu/ai-index/2025-ai-index-report;

207. Humeau, Eugénie, and Tanvi Deshpande. 2024. "AI for Africa: Use Cases Delivering Impact Authors and Contributors." https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/07/AI_for_Africa.pdf.

208. Bria, Francesca, Paul Timmers, and Fausto Gernone. 2025h. "EuroStack - a European Alternative for Digital Sovereignty." Bertelsmann-Stiftung.de. February 13, 2025. https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty.

209. Center for Strategic Studies and Management (CGEE), and Ministry of Science, Technology and Innovations (MCTI). 2022. "Brazilian Digital

END NOTES

Transformation Strategy (E-Digital)." Brasília. 2022. https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/digitalstrategy_2022-2026.pdf.

210. "Banco Central Do Brasil." n.d. Www.bcb.gov.br. https://www.bcb.gov.br/en/financialstability/pixstatistics.

211. Vieira, André. 2025. "Pix Sets New Daily Record with Almost 300 Million Transactions on Black Friday." Brazil Stock Guide. December 2025. https://brazilstockguide.com/insights/pix-sets-new-daily-record-with-almost-300-million-transactions-on-black-friday/.

212. Teevan, Chloe, Raphael Pouyé, and Gautam Kamath. 2025d. "From India Stack to EuroStack: Reconciling Approaches to Sovereign Digital Infrastructure ." https://ecdpm.org/application/files/2117/3874/5474/From-India-Stack-to-EuroStack-Reconciling-Approaches-Sovereign-Digital-Infrastructure-ECDPM-Discussion-Paper-384.pdf.

213. Ministério da Ciência, Tecnologia e Inovação, and Centro de Gestão e Estudos Estratégicos. 2025. "Plano Brasileiro de Inteligência Artificial IA Para O Bem de Todos." https://www.gov.br/mcti/pt-br/centrais-de-conteudo/publicacoes-mcti/plano-brasileiro-de-inteligencia-artificial/pbia_mcti_2025.pdf.

214. "Joint Statement from the Quad Foreign Ministers' Meeting in Washington - United States Department of State." 2025. United States Department of State. July 2, 2025. https://www.state.gov/releases/office-of-the-spokesperson/2025/07/joint-statement-from-the-quad-foreign-ministers-meeting-in-washington/.

215. "Strategic Partnership Agreement between the Government of the United States of America and the Government of the Democratic Republic of the Congo - United States Department of State." 2025. United States Department of State. 2025. https://www.state.gov/strategic-partnership-agreement-between-the-government-of-the-united-states-of-america-and-the-government-of-the-democratic-republic-of-the-congo.

216. Baskaran, Gracelin, and Meredith Schwartz. 2025. "Ahead of APEC, Trump Signs Flurry of Bilateral Minerals Agreements on Asia Tour." Center for Strategic and International Studies. 2025. https://www.csis.org/analysis/ahead-apec-trump-signs-flurry-bilateral-minerals-agreements-asia-tour.

217. "Treasury Announces Financial and Economic Partnership and Capital Markets Sector Collaboration with Saudi Arabia, Welcomes Additional Arrangements to Strengthen the Economic Ties between Our Two Countries." 2025. U.S. Department of the Treasury. November 18, 2025. https://home.treasury.gov/news/press-releases/sb0318.

218. "United States-Australia Framework for Securing of Supply in the Mining and Processing of Critical Minerals and Rare Earths." 2025b. The White House. October 20, 2025. https://www.whitehouse.gov/briefings-statements/2025/10/united-states-australia-framework-for-securing-of-supply-in-the-mining-and-processing-of-critical-minerals-and-rare-earths/.

219. U.S. Mission Lima. 2024. "The United States of America and Peru Sign MOU to Strengthen Cooperation on Critical Minerals - U.S. Embassy in Peru." U.S. Embassy in Peru. August 30, 2024. https://pe.usembassy.gov/the-united-states-of-america-and-peru-sign-mou-to-strengthen-cooperation-on-critical-minerals/.

220. African Union. 2020. "African Union Union Africaine União Africana the Digital Transformation Strategy for Africa (2020-2030)." https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf.

221. Muldoon, James, Ana Valdivia, and Adam Badger. 2025. "The Politics of Artificial Intelligence Supply Chains." AI & Society, September. https://doi.org/10.1007/s00146-025-02625-y.

222. Narechania, Tejas N., and Ganesh Sitaraman. 2024b. "An Antimonopoly Approach to Governing Artificial Intelligence." Yale Law & Policy Review.

END NOTES

2024. https://yalelawandpolicy.org/antimonopoly-approach-governing-artificial-intelligence.

223. Allen, Gregory C. 2022. "Choking off China's Access to the Future of AI." Www.csis.org. October 11, 2022. https://www.csis.org/analysis/choking-chinas-access-future-ai.

224. IBM. 2024. "AI Stack." Ibm.com. November 29, 2024. https://www.ibm.com/think/topics/ai-stack.

225. Kerry, Cameron F., Joshua P. Meltzer, Andrea Renda, Alex Engler, and Rosanna Fanni. 2021a. "Strengthening International Cooperation on AI." Brookings. October 25, 2021. https://www.brookings.edu/articles/strengthening-international-cooperation-on-ai/.

226. International Energy Agency. 2025. "Global Critical Minerals Outlook 2025 – Analysis - IEA." IEA. May 21, 2025. https://www.iea.org/reports/global-critical-minerals-outlook-2025; Ritchie, Hannah, and Pablo Rosado. 2020. "Electricity Mix." Our World in Data. July 2020. https://ourworldindata.org/electricity-mix; "Market Share for Logic Chip Production, by Manufacturing Stage." 2021. Our World in Data. 2021. https://ourworldindata.org/grapher/market-share-logic-chip-production-manufacturing-stage; "Cumulative Number of Large-Scale AI Systems by Country since 2017." 2025a. Our World in Data. https://ourworldindata.org/grapher/cumulative-number-of-large-scale-ai-systems-by-country?tab=table; Nestor Maslej, Loredana Fattorini, Raymond Perrault, Yolanda Gil, Vanessa Parli, Njenga Kariuki, Emily Capstick, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, Toby Walsh, Armin Hamrah, Lapo Santarlasci, Julia Betts Lotufo, Alexandra Rome, Andrew Shi, and Sukrut Oak. 2025c. "The 2025 AI Index Report." AI Index Steering Committee, Institute for Human-Centered AI, Stanford University. April 2025. https://hai.stanford.edu/ai-index/2025-ai-index-report; Daigle, Brian. 2021. "Data Centers around the World: A Quick Look." https://www.usitc.gov/publications/332/executive_briefings/ebot_data_centers_around_the_world.pdf; "Broadband Statistics." 2024. OECD. 2024. https://www.oecd.org/en/topics/sub-issues/broadband-statistics.html; Runde, Daniel, Erin Murphy, and Thomas Bryja. 2024. "Safeguarding Subsea Cables Protecting Cyber Infrastructure amid Great Power Competition." https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-08/240816_Runde_Subsea_Cables.pdf; GitHub. 2025. "Innovationgraph/Data/Repositories.csv at Main · Github/Innovationgraph." GitHub. 2025. https://github.com/github/innovationgraph/blob/main/data/repositories.csv; "Distribution of Authors per Country." 2024. Arkko.com. August 11, 2024. https://www.arkko.com/tools/rfcstats/countrydistr.html; "ICT Service Exports." 2024. World Bank Open Data. 2024. https://data.worldbank.org/indicator/BX.GSR.CCIS.CD?end=2024&start=2024; "Individuals using the Internet." 2024. Itu.int. 2024. https://datahub.itu.int/data/?i=11624; "Wikistats - Statistics for Wikimedia Projects." 2026. Wikimedia.org. 2026. https://stats.wikimedia.org/;

227. "The American AI Stack and the World." 2025a. Brookings. October 8, 2025. https://www.brookings.edu/events/the-american-ai-stack-and-the-world/.

228. Kerry, Cameron F., and Saurabh Mishra. 2025a. "The Myth of the Monolith: AI Is Not One Thing." Brookings. October 9, 2025. https://www.brookings.edu/articles/the-myth-of-the-monolith-ai-is-not-one-thing/.

229. Kerry, Cameron F., Joshua P. Meltzer, Andrea Renda, Alex Engler, and Rosanna Fanni. 2021b. "Strengthening International Cooperation on AI Executive Summary." https://www.brookings.edu/wp-content/uploads/2021/10/Strengthening-International-Cooperation-AI_ExecutiveSummary_Oct21.pdf.

230. "G42 and Microsoft to Establish Two Research Centres in Abu Dhabi to Advance Development of Responsible Artificial Intelligence." 2024. Mediaof-

END NOTES

fice.abudhabi. Abu Dhabi Media Office. September 17, 2024. https://www.mediaoffice.abudhabi/en/technology/g42-and-microsoft-to-establish-two-research-centres-in-abu-dhabi-to-advance-development-of-responsible-artificial-intelligence/.

231. "Meta, Hugging Face, and Scaleway Announce a New AI Accelerator Program for European Startups." 2024. Meta Newsroom. June 23, 2024. https://about.fb.com/news/2024/06/meta-hugging-face-and-scaleway-announce-a-new-ai-accelerator-program-for-european-startups/.
232. Aubakirova, Malika, Alex Atallah, Chris Clark, Justin Summerville, and Anjney Midha. 2025. "State of AI 2025: 100T Token LLM Usage Study." OpenRouter. December 2025. https://openrouter.ai/state-of-ai.
233. Vidal, Nick. 2024. "Compelling Responses to NTIA's AI Open Model Weights RFC - Open Source Initiative." Open Source Initiative. April 9, 2024. https://opensource.org/blog/compelling-responses-to-ntias-ai-open-model-weights-rfc.
234. "Winning the Race America's AI Action Plan." 2025. The White House. July 2025. https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.
235. American AI Initiative. 2023. "The ATOM Project - American Truly Open Models." Atomproject.ai. 2023. https://www.atomproject.ai.
236. Hays, Seth. 2025. "The AI Kill Switch: Dangerous Chinese Open Source." CEPA. December 15, 2025. https://cepa.org/article/the-ai-kill-switch-dangerous-chinese-open-source/.
237. Longpre, Shayne, Christopher Akiki, Campbell Lund, Atharva Kulkarni, Emily Chen, Irene Solaiman, Avijit Ghosh, Yacine Jernite, and Lucie-Aimée Kaffee. 2025. "Economies of Open Intelligence: Tracing Power & Participation in the Model Ecosystem." https://www.dataprovenance.org/economies-of-open-intelligence.pdf.
238. Chavez, Pablo. 2025b. "Focusing the American AI Exports Program." Consensus Drift. Substack.com. December 4, 2025. https://consensusdrift.substack.com/p/focusing-the-american-ai-exports.
239. World Economic Forum. 2026a. "Davos 2026: Special Address by Mark Carney, PM of Canada." World Economic Forum. January 20, 2026. https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada/.
240. "Unpacking the White House AI Action Plan with OSTP Director Michael Kratsios." 2025. Center for Strategic and International Studies. 2025. https://www.csis.org/analysis/unpacking-white-house-ai-action-plan-ostp-director-michael-kratsios.
241. Okolo, Chinasa. 2026. "Priorities for U.S. Participation in International AI Capacity-Building." Lawfare. 2026. https://www.lawfaremedia.org/article/priorities-for-u.s.-participation-in-international-ai-capacity-building.
242. World Economic Forum. 2026b. "Davos 2026: Special Address by Mark Carney, PM of Canada." World Economic Forum. January 20, 2026. https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada/.
243. "The American AI Stack and the World." 2025b. Brookings. October 8, 2025. https://www.brookings.edu/events/the-american-ai-stack-and-the-world/.
244. Toh, Amos. 2025. "The Good, Bad, and Really Weird AI Provisions in the Annual Defense Policy Bill." Brennan Center for Justice. December 15, 2025. https://www.brennancenter.org/our-work/analysis-opinion/good-bad-and-really-weird-ai-provisions-annual-defense-policy-bill.
245. Smith, Brad. 2025. "Unlocking Data to Advance European Commerce and Culture - Microsoft on the Issues." Microsoft on the Issues. July 21, 2025. https://blogs.microsoft.com/on-the-issues/2025/07/20/eudigitalunlock/.
246. "Models – Hugging Face." 2026. Huggingface.co. 2026. https://huggingface.co/models?num_pa-

END NOTES

rameters=min:0.
247. Team GLM. 2024. “ChatGLM: A Family of Large Language Models from GLM-130B to GLM-4 All Tools.” ArXiv.org. July 30, 2024. https://arxiv.org/pdf/2406.12793v2.
248. U.S. Department of the Interior, and U.S. Geological Survey. 2024. “Mineral Commodity Summaries 2024.” https://pubs.usgs.gov/periodicals/mcs2024/mcs2024.pdf.
249. Kim, Tae-Yoon, Shobhan Dhir, Amrita Dasgupta, and Alessio Scanziani. 2025a. “With New Export Controls on Critical Minerals, Supply Concentration Risks Become Reality – Analysis - IEA.” IEA. October 23, 2025. https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality.
250. Bradsher, Keith. 2025. “China Suspends Some Export Controls on Critical Minerals but Retains Others.” The New York Times, November 7, 2025. https://www.nytimes.com/2025/11/07/business/china-rare-earth-export-controls.html.
251. SIA. 2024. “2024 State of the U.S. Semiconductor Industry.” Semiconductor Industry Association. September 11, 2024. https://www.semiconductors.org/2024-state-of-the-u-s-semiconductor-industry/.
252. Kleinhas, Jan-Peter, and Sabhyata Jha. 2025. “The Chip Landscape Geographical Distribution of Wafer Fabrication Capacity.” OECD. https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/the-chip-landscape_27ef5d87/02dbd028-en.pdf.
253. Butts, Dylan, and Emily Tan. 2026. “TSMC Is Set to Expand Its $165 Billion U.S. Investment — Here’s What We Know.” CNBC. January 16, 2026. https://www.cnbc.com/2026/01/16/tsmcs-arizona-chip-expansion-isnt-done-after-us-investment-cfo.html.
254. “G7 Critical Minerals Action Plan.” 2025. Canada.ca. June 17, 2025. https://g7.canada.ca/en/news-and-media/news/g7-critical-minerals-action-plan/.
255. “America’s AI Action Plan.” 2025. White House. July 2025. https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.
256. “Electricity Data Browser.” 2025. Eia.gov. November 2025. https://www.eia.gov/electricity/data/browser/.
257. Lowell, Michael. 2026. “Trump 2.0 Tariff Tracker.” Trade Compliance Resource Hub. January 27, 2026. https://www.tradecomplianceresourcehub.com/2026/01/27/trump-2-0-tariff-tracker/.
258. “U.S. Electricity Exports to Canada Have Increased since September 2023 - U.S. Energy Information Administration (EIA).” 2025. Eia.gov. March 6, 2025. https://www.eia.gov/todayinenergy/detail.php?id=63684.
259. Kerry, Cameron F., Joshua P. Meltzer, Andrea Renda, Alex Engler, and Rosanna Fanni. 2021c. “Strengthening International Cooperation on AI Progress Report.” https://www.brookings.edu/wp-content/uploads/2021/10/Strengthening-International-Cooperation-AI_Oct21.pdf.
260. “Fact Sheet: President Donald J. Trump Withdraws the United States from International Organizations That Are Contrary to the Interests of the United States.” 2026b. The White House. January 7, 2026. https://www.whitehouse.gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-withdraws-the-united-states-from-international-organizations-that-are-contrary-to-the-interests-of-the-united-states/.
261. Chavez, Pablo. 2022. “Toward Digital Solidarity.” Lawfare. 2022. https://www.lawfaremedia.org/article/toward-digital-solidarity.
262. World Economic Forum, and Bain & Company. 2026a. “Rethinking AI Sovereignty: Pathways to Competitiveness through Strategic Investments.” https://www3.weforum.org/docs/WEF_Rethinking_AI_Sovereignty_Pathways_to_Competitiveness_through_Strategic_Investments_2026.pdf.
263. European Commission. 2024. “EU-Mercosur Trade Agreement.” Policy.trade.ec.europa.eu. De-

END NOTES

cember 6, 2024. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/mercosur/eu-mercosur-agreement_en.

264. Joslyn, Marie. 2026. "Latin America Waiting: What's next for the EU-Mercosur Deal?" Dw.com. Deutsche Welle. January 26, 2026. https://www.dw.com/en/latin-america-waiting-whats-next-for-the-eu-mercosur-deal/a-75666418.

265. "EU and India Conclude Landmark Free Trade Agreement." 2026. European Commission - European Commission. January 26, 2026. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_184.

266. "The International Digital Strategy for the European Union." 2025. Shaping Europe's Digital Future. 2025. https://digital-strategy.ec.europa.eu/en/policies/international-digital-strategy.

267. Renda, Andrea, and Nicoleta Kyosovska. 2025a. "EU Plans for AI (Giga)Factories: Sanctuaries of Innovation, or Cathedrals in the Desert? – CEPS." CEPS. November 3, 2025. https://www.ceps.eu/ceps-publications/eu-plans-for-ai-gigafactories-sanctuaries-of-innovation-or-cathedrals-in-the-desert/.

268. Bakker, David de. 2025. "New Tech Sovereignty Catalogue Announced." European DIGITAL SME Alliance. June 25, 2025. https://www.digitalsme.eu/new-tech-sovereignty-catalogue-announced/.

269. "Tech Sovereignty Catalogue." 2026. Tech Sovereignty Catalogue. February 10, 2026. https://techsov-catalogue.eu/.

270. "Commission to Launch Digital Commons EDIC to Support Sovereign European Digital Infrastructure and Technology." 2025. Shaping Europe's Digital Future. October 29, 2025. https://digital-strategy.ec.europa.eu/en/news/commission-launch-digital-commons-edic-support-sovereign-european-digital-infrastructure-and.

271. "European Digital Infrastructure Consortium (EDIC) | Shaping Europe's Digital Future." n.d. Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/policies/edic.

272. Tanner, Brooke and Andrew W. Wyckoff. 2025a. "Making the Case for a Third AI Technology Stack." Brookings. September 12, 2025. https://www.brookings.edu/articles/making-the-case-for-a-third-ai-technology-stack/.

273. "Berlin Declaration Friends of Industry 2025." 2025. Federal Ministry for Economic Affairs and Energy (BMWE). https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/F/friends-of-industry-berlin-declaration.pdf?__blob=publicationFile&v=20.

274. Nestor Maslej, Loredana Fattorini, Raymond Perrault, Yolanda Gil, Vanessa Parli, Njenga Kariuki, Emily Capstick, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, Toby Walsh, Armin Hamrah, Lapo Santarlasci, Julia Betts Lotufo, Alexandra Rome, Andrew Shi, and Sukrut Oak. 2025d. "The 2025 AI Index Report." AI Index Steering Committee, Institute for Human-Centered AI, Stanford University. April 2025. https://hai.stanford.edu/ai-index/2025-ai-index-report;

275. "EU Startup and Scaleup Strategy." 2025. Research and Innovation. June 4, 2025. https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/jobs-and-economy/eu-startup-and-scaleup-strategy_en.

276. Draghi, Mario. 2024. "The Future of European Competitiveness." EU Commission. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en.

277. "AI Act Service Desk - Frequently Asked Questions." 2024. Europa.eu. 2024. https://ai-act-service-desk.ec.europa.eu/en/faq?combine=&faq_category_id=99.

278. "Special Address by President von Der Leyen at the World Economic Forum." 2026. European Commission - European Commission. 2026. https://ec.europa.eu/commission/presscorner/

END NOTES

detail/en/speech_26_150.

279. Kerry, Cameron F., Joshua P. Meltzer, and Matt Sheehan. 2023. “Can Democracies Cooperate with China on AI Research?” Brookings. January 9, 2023. https://www.brookings.edu/articles/can-democracies-cooperate-with-china-on-ai-research/.

280. □□. 2025. “Full Text: Recommendations of the Central Committee of the Communist Party of China for Formulating the 15th Five-Year Plan for National Economic and Social Development.” Www.gov.cn. 2025. https://english.www.gov.cn/news/202510/28/content_WS6900adb9c6d00ca5f9a07216.html.

281. Lee, Kai-Fu. n.d. “AI Superpowers.” AI Superpowers. https://www.aisuperpowers.com/.

282. Kim, Tae-Yoon, Shobhan Dhir, Amrita Dasgupta, and Alessio Scanziani. 2025b. “With New Export Controls on Critical Minerals, Supply Concentration Risks Become Reality – Analysis - IEA.” IEA. October 23, 2025. https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality.

283. International Energy Agency. 2022. “China - Countries & Regions.” IEA. 2022. https://www.iea.org/countries/china.

284. Li, Ma, Charles Bourgault, and World Economic Forum. 2025. “How China Adds More Renewable Energy than Any Other Economy.” World Economic Forum. December 3, 2025. https://www.weforum.org/stories/2025/12/china-adding-more-renewables-to-grid/.

285. Meinhardt, Caroline, Sabina Nong, Graham Webster, and Tatsunori Hashimoto . 2019. “Beyond DeepSeek: China’s Diverse Open-Weight AI Ecosystem and Its Policy Implications.” Stanford.edu. 2019. https://hai.stanford.edu/policy/beyond-deepseek-chinas-diverse-open-weight-ai-ecosystem-and-its-policy-implications.

286. Au, Adam, and Felicia Feiran Chen. 2025. “China Expands AI Globally through the Digital Silk Road.” East Asia Forum. April 11, 2025. https://eastasiaforum.org/2025/04/11/china-expands-ai-globally-through-the-digital-silk-road/.

287. Cai, Vanessa. 2025. “South China Morning Post.” South China Morning Post. September 2, 2025. https://www.scmp.com/news/china/diplomacy/article/3324033/sco-summit-2025-china-showcase-how-far-bloc-has-come-nearly-quarter-century.

288. “Global AI Governance Action Plan_Ministry of Foreign Affairs of the People’s Republic of China.” 2025b. Mfa.gov.cn. 2025. https://www.mfa.gov.cn/eng/xw/zyxw/202507/t20250729_11679232.html.

289. United Nations. 2024b. “Pact for the Future - United Nations Summit of the Future | United Nations.” United Nations. 2024. https://www.un.org/en/summit-of-the-future/pact-for-the-future.

290. Endresen, Janice. 2021. “Miles Ahead: China, Huawei, and 5G | BusinessFeed.” Cornell SC Johnson. February 15, 2021. https://business.cornell.edu/hub/2021/02/15/miles-ahead-china-huawei-5g/.

291. Tobin, Meaghan. 2025b. “Trump Eases Limits on Nvidia Exports to China at ‘Critical Moment.’” The New York Times, December 9, 2025. https://www.nytimes.com/2025/12/09/business/china-gains-trump-nvidia-chips.html.

292. McGuire, Chris. 2025. “China’s AI Chip Deficit: Why Huawei Can’t Catch Nvidia and U.S. Export Controls Should Remain.” Council on Foreign Relations. December 11, 2025. https://www.cfr.org/article/chinas-ai-chip-deficit-why-huawei-cant-catch-nvidia-and-us-export-controls-should-remain.

293. China Law Translate. 2023. “Interim Measures for the Management of Generative Artificial Intelligence Services.” China Law Translate. July 13, 2023. https://www.chinalawtranslate.com/en/generative-ai-interim/.

294. Kassianik, Paul. 2025. “Evaluating Security Risk in DeepSeek and Other Frontier Reasoning Models.” Cisco Blogs. January 31, 2025. https://blogs.cisco.com/security/evaluating-security-risk-in-deepseek-and-other-frontier-reason-

END NOTES

ing-models.

295. Yang, Grace X. 2025. “The Openness Paradox: Open-Source AI and China’s Quest for Cyber Sovereignty.” Dialogues on Digital Society 1 (3). https://doi.org/10.1177/29768640251376497.

296. Yuan, Shaoyu. 2024. “China Leans into Using AI – Even as the US Leads in Developing It.” Nextgov.com. Nextgov/FCW. August 21, 2024. https://www.nextgov.com/ideas/2024/08/china-leans-using-ai-even-us-leads-developing-it/398953/.

297. Jordi Calvet-Bademunt, and Jacob Mchangama. 2025. “China’s AI Governance Ambitions and Their Implications for Free Expression.” Lawfare. 2025. https://www.lawfaremedia.org/article/china-s-ai-governance-ambitions-and-their-implications-for-free-expression.

298. Gruzer, Marina. 2024. “Bloomsbury Intelligence & Security Institute (BISI).” Bloomsbury Intelligence & Security Institute (BISI). May 27, 2024. https://bisi.org.uk/reports/could-chinas-digital-silk-road-dsr-pose-security-challenges-and-on-central-asian-multi-vector-diplomacy-efforts.

299. Council on Foreign Relations. 2020. “Assessing China’s Digital Silk Road Initiative.” Council on Foreign Relations. 2020. https://www.cfr.org/china-digital-silk-road/.

300. Chilukuri, Vivek, and Ruby Scanlon. 2025. “Countering the Digital Silk Road.” CNAS. 2025. https://www.cnas.org/publications/reports/countering-the-digital-silk-road.

301. Fort, Kristina. 2024. “Boosting the EU’s Position in AI through Third Places Diplomacy.” Tech Policy Press. October 18, 2024. https://www.techpolicy.press/boosting-the-eus-position-in-ai-through-third-places-diplomacy/.

302. Tanner, Brooke and Andrew W. Wyckoff. 2025b. “Making the Case for a Third AI Technology Stack.” Brookings. September 12, 2025. https://www.brookings.edu/articles/making-the-case-for-a-third-ai-technology-stack/.

303. Sajjanhar, Anuradha . 2025a. “India’s Digital Infrastructure Is Going Global. What Kind of Power Is It Building?” Tech Policy Press. July 16, 2025. https://www.techpolicy.press/indias-digital-infrastructure-is-going-global-what-kind-of-power-is-it-building/.

304. ———. 2025b. “India’s Digital Infrastructure Is Going Global. What Kind of Power Is It Building?” Tech Policy Press. July 16, 2025. https://www.techpolicy.press/indias-digital-infrastructure-is-going-global-what-kind-of-power-is-it-building/.

305. “Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem.” 2024. Pmindia.gov.in. March 7, 2024. https://www.pmindia.gov.in/en/news_updates/cabinet-approves-ambitious-indiaai-mission-to-strengthen-the-ai-innovation-ecosystem/.

306. “Bhashini.” 2024a. Bhashini.gov.in. 2024. https://bhashini.gov.in/.

307. “India Scales AI Compute as Chip Race Heats Up, Easing Startup Costs | Communications Today.” 2025. Communications Today. December 8, 2025. https://www.communicationstoday.co.in/india-scales-ai-compute-as-chip-race-heats-up-easing-startup-costs/.

308. Deb, Dhritiman. 2025. “As Google and AMD Challenge Nvidia’s Dominance, India Focuses on Its AI Infrastructure and Chip Utilisation….” Linkedin.com. LinkedIn News. December 8, 2025. https://www.linkedin.com/news/story/india-steps-up-chip-play-7316817/.

309. Singh, Manish. 2025. “India Lauds Chinese AI Lab DeepSeek, Plans to Host Its Models on Local Servers | TechCrunch.” TechCrunch. January 30, 2025. https://techcrunch.com/2025/01/30/india-to-host-china-deepseek-ai-model-locally-in-rare-tech-approval/.

310. PTI. 2026. “India’s Policies Have Put Wind in Its Sails, Says PM Aide Shaktikanta Das.” The Economic Times. Economic Times. January 9, 2026. https://economictimes.indiatimes.com/news/india/indias-policies-have-put-wind-in-its-sails-says-pm-aide-shaktikanta-das/articleshow/126441161.cms?from=mdr.

END NOTES

311. Shinde, Jayesh. 2025. “India’s Shakti: IIT Madras to Develop Indigenous 7-Nm Chip by 2028.” Digit.in. October 31, 2025. https://www.digit.in/features/general/india-shakti-iit-madras-to-develop-indigenous-7-nm-chip-by-2028.html.
312. TOI Business Desk. 2025. “‘Digital Swaraj Mission’: GTRI Flags Risks of US Tech Dependence; Calls for India’s Cloud and OS Self-Reliance by 2030.” The Times of India. September 14, 2025. https://timesofindia.indiatimes.com/business/india-business/digital-swaraj-mission-gtri-flags-risks-of-us-tech-dependence-calls-for-indias-cloud-and-os-self-reliance-by-2030/articleshow/123880429.cms.
313. Nagao, Satoru. 2023. “India Is Always Invited to G7. Why Is That so Important?” Hudson Institute. May 14, 2023. https://www.hudson.org/foreign-policy/india-always-invited-g7-why-so-important.
314. “G20 Digital Economy Ministers Meeting Outcome Document and Chair Summary (19/08/2023).” 2023. G7g20-Documents.org. August 19, 2023. https://g7g20-documents.org/database/document/2023-g20-india-sherpa-track-digital-economy-ministers-ministers-language-g20-digital-economy-ministers-meeting-outcome-document-and-chair-summary.
315. PTI. 2025. “India’s Sovereign AI Model to Be Ready by February: Meity Secretary.” The Economic Times. Economic Times. October 10, 2025. https://economictimes.indiatimes.com/tech/technology/indias-sovereign-ai-model-to-be-ready-by-february-meity-secretary/articleshow/124452012.cms?from=mdr.
316. “India Launches ‘BharatGen’ AI Model to Revolutionize Multilingual Innovation at BharatGen Summit.” 2025. DDnews.in. February 6, 2025. https://ddnews.gov.in/en/india-launches-bharatgen-ai-model-to-revolutionize-multilingual-innovation-at-bharatgen-summit/.
317. Neufeld, Jeremy, and Lindsay Milliken. 2025. “Most of America’s Top AI Companies Were Founded by Immigrants | IFP.” Institute for Progress. April 16, 2025. https://ifp.org/most-of-americas-top-ai-companies-were-founded-by-immigrants/.
318. “Indian Experts Named to the New AI Advisory Body by the UN.” 2023. IndiaAI. October 23, 2023.
319. Renda, Andrea, and Nicoleta Kyosovska. 2025b. “EU Plans for AI (Giga)Factories: Sanctuaries of Innovation, or Cathedrals in the Desert? – CEPS.” CEPS. November 3, 2025. https://www.ceps.eu/ceps-publications/eu-plans-for-ai-gigafactories-sanctuaries-of-innovation-or-cathedrals-in-the-desert/.
320. Tanner, Brooke, and Andrew W. Wyckoff. 2025c. “Making the Case for a Third AI Technology Stack.” Brookings. September 12, 2025. https://www.brookings.edu/articles/making-the-case-for-a-third-ai-technology-stack/.
321. Schweikart, Larry, and Christina J. Moose. 2023. “European Consortium Creates Airbus Industrie | EBSCO.” EBSCO Information Services, Inc. | Www.ebsco.com. 2023. https://www.ebsco.com/research-starters/history/european-consortium-creates-airbus-industrie.
322. CERN. 2019. “About | CERN.” Home.cern. October 11, 2019. https://home.cern/about.
323. World Economic Forum and Bain & Company. 2026b. “Rethinking AI Sovereignty: Pathways to Competitiveness through Strategic Investments.” https://www3.weforum.org/docs/WEF_Rethinking_AI_Sovereignty_Pathways_to_Competitiveness_through_Strategic_Investments_2026.pdf.
324. Faisal, Aldo, David Shrier, Ayisha Piotti, and Alex Pentland. 2024c. “Considerations Regarding Sovereign AI and National AI Policy.” https://sovereign-ai.org/media/papers/Considerations_regarding_Sovereign_AI_C_Sovereign_AI__Imperial_College.pdf.
325. International Energy Agency. 2025b. “Global Critical Minerals Outlook.” IEA. May 21, 2025. https://www.iea.org/reports/global-critical-minerals-outlook-2025.

END NOTES

326. Ritchie, Hannah, and Pablo Rosado. 2020. "Electricity Mix." Our World in Data. July 2020. https://ourworldindata.org/electricity-mix.
327. "Market Share for Logic Chip Production, by Manufacturing Stage." 2021b. Our World in Data. 2021. https://ourworldindata.org/grapher/market-share-logic-chip-production-manufacturing-stage.
328. "Market Share for Logic Chip Production, by Manufacturing Stage." 2021c. Our World in Data. 2021. https://ourworldindata.org/grapher/market-share-logic-chip-production-manufacturing-stage.
329. "Market Share for Logic Chip Production, by Manufacturing Stage." 2021d. Our World in Data. 2021. https://ourworldindata.org/grapher/market-share-logic-chip-production-manufacturing-stage.
330. Nestor Maslej, Loredana Fattorini, Raymond Perrault, Yolanda Gil, Vanessa Parli, Njenga Kariuki, Emily Capstick, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, Toby Walsh, Armin Hamrah, Lapo Santarlasci, Julia Betts Lotufo, Alexandra Rome, Andrew Shi, and Sukrut Oak. 2025e. "The 2025 AI Index Report." AI Index Steering Committee, Institute for Human-Centered AI, Stanford University. April 2025. https://hai.stanford.edu/ai-index/2025-ai-index-report;
331. Daigle, Brian. 2021. "Data Centers around the World: A Quick Look." https://www.usitc.gov/publications/332/executive_briefings/ebot_data_centers_around_the_world.pdf.
332. "Broadband Statistics." 2024. OECD. 2024. https://www.oecd.org/en/topics/sub-issues/broadband-statistics.html.
333. Runde, Daniel, Erin Murphy, and Thomas Bryja. 2024. "Safeguarding Subsea Cables Protecting Cyber Infrastructure amid Great Power Competition." https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-08/240816_Runde_Subsea_Cables.pdf.
334. Runde, Daniel, Erin Murphy, and Thomas Bryja. 2024. "Safeguarding Subsea Cables Protecting Cyber Infrastructure amid Great Power Competition." https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-08/240816_Runde_Subsea_Cables.pdf.
335. Ruiz, Jeanette B., and George A. Barnett. 2014. "Who Owns the International Internet Networks?" The Journal of International Communication 21 (1): 38–57. https://doi.org/10.1080/13216597.2014.976583.
336. GitHub. 2025. "Innovationgraph/Data/Repositories.csv at Main · Github/Innovationgraph." GitHub. 2025. https://github.com/github/innovationgraph/blob/main/data/repositories.csv.
337. "Distribution of Authors per Country." 2024. Arkko.com. August 11, 2024. https://www.arkko.com/tools/rfcstats/countrydistr.html.
338. "ICT Service Exports." 2024. World Bank Open Data. 2024. https://data.worldbank.org/indicator/BX.GSR.CCIS.CD?end=2024&start=2024.
339. "Individuals using the Internet." 2024. International Telecommunication Union. 2024. https://datahub.itu.int/data/?i=11624;
340. "Wikistats - Statistics for Wikimedia Projects." 2026. Wikimedia.org. 2026. https://stats.wikimedia.org/;
341. SFA Oxford. 2025. "Critical Minerals in Artificial Intelligence | SFA (Oxford)." SFA (Oxford). 2025. https://www.sfa-oxford.com/knowledge-and-insights/critical-minerals-in-low-carbon-and-future-technologies/critical-minerals-in-artificial-intelligence/.
342. Stewart, Sara. 2025c. "Artificial Intelligence and the Critical Minerals Crunch." Jcdream.org. FP Analytics. July 18, 2025. https://jcdream.org/reports/ai-and-the-critical-minerals-crunch.
343. Tan, Catherine. 2024. "Breaking the Circuit: US-China Semiconductor Controls - Foreign Policy Research Institute." Foreign Policy Research Institute. September 16, 2024. https://www.fpri.

END NOTES

org/article/2024/09/breaking-the-circuit-us-china-semiconductor-controls/.

344. "Energy Department Announces $355 Million to Expand Domestic Production of Critical Minerals and Materials." 2025. Energy.gov. November 17, 2025. https://www.energy.gov/articles/energy-department-announces-355-million-expand-domestic-production-critical-minerals-and.

345. European Commission. 2023a. "Critical Raw Materials." Single-Market-Economy.ec.europa.eu. European Commission. 2023. https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials_en.

346. Institute for Advanced Study. 2025. "RARE/EARTH: The Geopolitics of Critical Minerals and the AI Supply Chain." YouTube. June 9, 2025. https://www.youtube.com/watch?v=GxVM3cAxHfg.

347. Carayannis, Tatiana, Alondra Nelson, and Marie-Therese Png. 2025. "AI and Geopolitics." Institute for Advanced Study. April 8, 2025. https://www.ias.edu/stsv-lab/aigeopolitics.

348. Stewart, Sara. 2025d. "Artificial Intelligence and the Critical Minerals Crunch." Jcdream.org. FP Analytics. July 18, 2025. https://jcdream.org/reports/ai-and-the-critical-minerals-crunch.

349. International Energy Agency. 2024. "Recycling of Critical Minerals – Analysis." International Energy Agency. November 18, 2024. https://www.iea.org/reports/recycling-of-critical-minerals.

350. ———. 2025c. "Global Critical Minerals Outlook 2025." June 2025. https://iea.blob.core.windows.net/assets/ef5e9b70-3374-4caa-ba9d-19c72253bfc4/GlobalCriticalMineralsOutlook2025.pdf.

351. ———. 2025c. "Global Critical Minerals Outlook 2025." June 2025. https://iea.blob.core.windows.net/assets/ef5e9b70-3374-4caa-ba9d-19c72253bfc4/GlobalCriticalMineralsOutlook2025.pdf.

352. International Energy Agency. 2025a. "Executive Summary – Energy and AI – Analysis." IEA. 2025. https://www.iea.org/reports/energy-and-ai/executive-summary.

353. ———. 2025b. "Executive Summary – Energy and AI – Analysis." IEA. 2025. https://www.iea.org/reports/energy-and-ai/executive-summary.

354. ———. 2025c. "Executive Summary – Energy and AI – Analysis." IEA. 2025. https://www.iea.org/reports/energy-and-ai/executive-summary.

355. Zewe, Adam. 2025. "Explained: Generative AI's Environmental Impact." MIT News. Massachusetts Institute of Technology. January 17, 2025. https://news.mit.edu/2025/explained-generative-ai-environmental-impact-0117.

356. "Data Center Watch." 2025. Data Center Watch. 2025. https://www.datacenterwatch.org/report.

357. Accomando, Jane, and Erin McClelland. 2025. "Artificial Intelligence and Data Centers Predicted to Drive Record High Energy Demand." Morganlewis.com. February 20, 2025. https://www.morganlewis.com/blogs/datacenterbytes/2025/02/artificial-intelligence-and-data-centers-predicted-to-drive-record-high-energy-demand.

358. Anthropic. 2025. "Build AI in America." https://www-cdn.anthropic.com/0dc382a2086f6a054eeb17e8a531bd9625b8e6e5.pdf.

359. Fitch, Asa, and Timothy W. Martin. 2025. "AI Data Center with up to 3 Gigawatts of Power Is Envisioned for South Korea." The Wall Street Journal. February 18, 2025. https://www.wsj.com/tech/ai/ai-data-center-with-up-to-3-gigawatts-of-power-is-envisioned-for-south-korea-5141bd77.

360. MB Staff. 2025. "PIF Launches HUMAIN to Lead Saudi AI Infrastructure and Arabic LLM Development." MENAbytes. May 12, 2025. https://www.menabytes.com/pif-humain/.

361. Datta, Arnab, and Tim Fist. 2025. "Compute in America: A Policy Playbook | IFP." Institute for Progress. February 3, 2025. https://ifp.org/special-compute-zones/.

362. Reuters Staff. 2025a. "France, UAE Agree to Develop 1 Gigawatt AI Data Centre." Reuters, February 6, 2025. https://www.reuters.com/technology/artificial-intelligence/france-uae-agree-develop-

END NOTES

1-gigawatt-ai-data-centre-2025-02-06/.

363. Rahman, Fareed. 2025. "UAE to Invest $40bn in Italy across Sectors such as Energy and AI." The National. The National News. February 24, 2025. https://www.thenationalnews.com/business/economy/2025/02/24/uae-to-invest-40-billion-in-italy-across-sectors-such-as-energy-and-ai/.

364. Barth, Adam, Chhavi Arora, Gayatri Shenai, Jesse Noffsinger, and Pankaj Sachdeva. 2025. "The Data Center Balance: How US States Can Navigate the Opportunities and Challenges." McKinsey & Company. August 8, 2025. https://www.mckinsey.com/industries/public-sector/our-insights/the-data-center-balance-how-us-states-can-navigate-the-opportunities-and-challenges.

365. "Norway's Critical Role in Ensuring Europe's Energy Security and Sustainability." 2024. Energy-council.com. December 20, 2024. https://energy-council.com/articles/norways-critical-role-in-ensuring-europes-energy-security-and-sustainability/.

366. "The AI Technology Stack and Why It Matters for AI Policy and Governance." 2025. https://www.itic.org/documents/artificial-intelligence/ITI_AITechnologyStack.pdf.

367. Authors, Saif, Alexander Khan, and Mann. 2020. "AI Chips: What They Are and Why They Matter an AI Chips Reference." https://cset.georgetown.edu/wp-content/uploads/CSET-An-AI-Chips-Primer-What-They-Are-and-Why-They-Matter.pdf.

368. Renda, Andrea, and Nicoleta Kyosovska. 2025c. "EU Plans for AI (Giga)Factories: Sanctuaries of Innovation, or Cathedrals in the Desert?." CEPS. November 3, 2025. https://www.ceps.eu/ceps-publications/eu-plans-for-ai-gigafactories-sanctuaries-of-innovation-or-cathedrals-in-the-desert/.

369. NVIDIA. 2022. "NVIDIA Hopper Architecture In-Depth." NVIDIA Technical Blog. March 22, 2022. https://developer.nvidia.com/blog/nvidia-hopper-architecture-in-depth/.

370. Leswing, Kif. 2026. "AI Memory Is Sold Out, Causing an Unprecedented Surge in Prices." CNBC. January 10, 2026. https://www.cnbc.com/2026/01/10/micron-ai-memory-shortage-hbm-nvidia-samsung.html.

371. Renda, Andrea, and Nicoleta Kyosovska. 2025d. "EU Plans for AI (Giga)Factories: Sanctuaries of Innovation, or Cathedrals in the Desert?." CEPS. November 3, 2025. https://www.ceps.eu/ceps-publications/eu-plans-for-ai-gigafactories-sanctuaries-of-innovation-or-cathedrals-in-the-desert/.

372. Suhas, A. R., Joel Martin, and Niti Jhunjhunwala. 2024. "Semiconductors—the next Frontier of Geopolitics." HFS Research. March 22, 2024. https://www.hfsresearch.com/research/semiconductor-supply-chain-diversification/.

373. The Economist. 2024. "Why Do Nvidia's Chips Dominate the AI Market?" The Economist. February 27, 2024. https://www.economist.com/the-economist-explains/2024/02/27/why-do-nvidias-chips-dominate-the-ai-market.

374. Lee, Chun-Yi, and Leo Shaw. 2023. "6. Securing the Semiconductor Supply Chain in an Era of Geopolitical Uncertainty." China Strategic Risks Institute. May 4, 2023. https://www.csri.global/launch-report/7-how-can6-securing-the-semiconductor-supply-chain-in-an-era-of-geopolitical-uncertainty-governments-help-investors-manage-esg-risks-in-china.

375. Renda, Andrea, and Nicoleta Kyosovska. 2025e. "EU Plans for AI (Giga)Factories: Sanctuaries of Innovation, or Cathedrals in the Desert?." CEPS. November 3, 2025. https://www.ceps.eu/ceps-publications/eu-plans-for-ai-gigafactories-sanctuaries-of-innovation-or-cathedrals-in-the-desert/.

376. Patrick, Gabriel. 2024. "Top 7 Semiconductor Manufacturing Equipment Companies Empowering Electronics Production." Verified Market Research. August 2024. https://www.verifiedmarketresearch.com/blog/top-semiconductor-manufacturing-equipment-companies/.

377. Thadani, Akhil, and Gregory C. Allen. 2023.

END NOTES

"Mapping the Semiconductor Supply Chain: The Critical Role of the Indo-Pacific Region." Center for Strategic and International Studies, May. https://www.csis.org/analysis/mapping-semiconductor-supply-chain-critical-role-indo-pacific-region.

378. Leswing, Kif. 2024. "Nvidia Dominates the AI Chip Market, but There's More Competition than Ever." CNBC. June 2, 2024. https://www.cnbc.com/2024/06/02/nvidia-dominates-the-ai-chip-market-but-theres-rising-competition-.html.
379. Xiong, Wei, David D Wu, and Jeff Yeung. 2024. "Semiconductor Supply Chain Resilience and Disruption: Insights, Mitigation, and Future Directions." International Journal of Production Research 63 (9): 1–24. https://doi.org/10.1080/00207543.2024.2387074.
380. European Commission. n.d. "European Chips Act." European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.
381. Blanchard, Ben, Thomas Escritt, and Thomas Escritt. 2023. "Germany Spends Big to Win $11 Billion TSMC Chip Plant." Reuters, August 8, 2023, sec. Technology. https://www.reuters.com/technology/taiwan-chipmaker-tsmc-approves-38-bln-germany-factory-plan-2023-08-08/.
382. "Information on Projects Funded to Strengthen U.S. Supply Chain ." 2025. United States Government Accountability Office. December 2025. https://www.gao.gov/assets/gao-26-107882.pdf.
383. Wooden, Andrew. 2024. "Big Three Hyperscalers Dominate Globally – except for China." Telecoms.com. 2024. https://www.telecoms.com/public-cloud/big-three-hyperscalers-dominate-globally-except-for-china.
384. Echikson, William. 2025. "Stormy Clouds: The Transatlantic Tussle over Cloud Computing." CEPA. June 4, 2025. https://cepa.org/article/stormy-clouds-the-transatlantic-tussle-over-cloud-computing/.
385. Daskal, Jennifer, and Richard Salgado. 2025. "CLOUD Act: Answers to Frequently Asked Questions." July 2025. https://www.crossborderdataforum.org/wp-content/uploads/2025/07/2025-CLOUD-Act-Answers-to-Frequently-Asked-Questions.pdf.
386. Synergy Research Group. 2025. "European Cloud Providers' Local Market Share Now Holds Steady at 15%." Srgresearch.com. 2025. https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15.
387. Buchholz, Katharina. 2025. "Infographic: Where Chinese or American Tech Is Used in Cloud Data Storage." Statista Daily Data. Statista. May 5, 2025. https://www.statista.com/chart/34404/share-of-cloud-availability-zones-by-national-origin-of-provider/?srsltid=AfmBOoqPhmYrb-Gt2e-9zUkJYL2Q1s9xIA8VQPNnRBRvHudrWjmwu-wjmT.
388. Zeichick, Alan. 2023. "What Is a Sovereign Cloud? Why Is It Important?" Oracle.com. Oracle. October 13, 2023. https://www.oracle.com/cloud/sovereign-cloud/what-is-sovereign-cloud/.
389. "Sovereign AI, Identity, and Cyber Compliance | International Insurance Society." 2025. Internationalinsurance.org. September 15, 2025. https://www.internationalinsurance.org/insights_cyber_sovereign_ai_identity_and_cyber_compliance.
390. Goujard, Clothilde , and Laurens Cerulus. 2021. "Inside Gaia-X: How Chaos and Infighting Are Killing Europe's Grand Cloud Project." POLITICO. POLITICO. October 26, 2021. https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/.
391. Abbott, Ben. 2024. "A Sovereign Cloud Boom Is Happening in APAC." TechRepublic. August 23, 2024. https://www.techrepublic.com/article/sovereign-cloud-boom-apac/.
392. Popko, John. 2025. "The Myth of Sovereign AI: Countries Rely on U.S. And Chinese Tech." Rest of World. September 12, 2025. https://restofworld.org/2025/chinese-us-tech-foreign-ai-dependence/.

END NOTES

393. Buckle, Marcus. 2025. “Sovereign Cloud on a Global Scale: Designing for Resilience, Trust and Innovation.” Ibm.com. October 9, 2025. https://www.ibm.com/think/insights/sovereign-cloud-on-a-global-scale.
394. Hanna. 2025. “‘Sovereign Cloud’ or ‘Sovereign Washing’? A Trojan Horse at Europe’s Digital Gates. | Tuta.” Tuta. June 27, 2025. https://tuta.com/blog/sovereign-washing.
395. Srivathsan, Bhargs , Marc Sorel, and Pankaj Sachdeva. 2024. “AI Power: Expanding Data Center Capacity to Meet Growing Demand.” McKinsey & Company. October 29, 2024. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand.
396. Noffsinger, Jesse, Mark Patel, and Pankaj Sachdeva. 2025. “The Cost of Compute: A $7 Trillion Dollar Race to Scale Data Centers.” McKinsey & Company. April 28, 2025. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-cost-of-compute-a-7-trillion-dollar-race-to-scale-data-centers.
397. “Investigating the Ecological Impacts of Data Centers – MIT Climate & Sustainability Consortium.” 2025. Mit.edu. March 20, 2025. https://impactclimate.mit.edu/2025/03/20/investigating-the-ecological-impacts-of-data-centers/.
398. Stewart, Josie, Brooke Tanner, and Nicol Turner Lee. 2025. “As Energy Demands for AI Increase, so Should Company Transparency.” Brookings. July 14, 2025. https://www.brookings.edu/articles/as-energy-demands-for-ai-increase-so-should-company-transparency/.
399. Hecker, Anne, Jonathan Frick, Jue Wang, Balaji Thirumalai, and Karen Harri. 2024. “Sovereign AI Is the next Fault Line in the Global Tech Sector.” Bain & Company. September 25, 2024. https://www.bain.com/insights/sovereign-ai-is-the-next-fault-line-in-the-global-tech-sector-tech-report-2024/.
400. Chee, Foo Yun. 2025. “Europe’s AI Gigafactory Push Attracts 76 Bids, EU Tech Chief Says.” Reuters, June 30, 2025. https://www.reuters.com/sustainability/boards-policy-regulation/europes-ai-gigafactory-push-attracts-76-bids-eu-tech-chief-says-2025-06-30/.
401. Ng, Spencer, Hwee Yee Ong, and Yijing Ng. 2025. “Asia-Pacific’s US$100 Billion Data Center Developments to Reshape Funding Models.” S&P Global. September 25, 2025. https://www.spglobal.com/ratings/en/regulatory/article/asia-pacifics-us100-billion-data-center-developments-to-reshape-funding-models-s101641380.
402. Nazzaro, Miranda. 2025. “Trump Signs AI Data Center Agreement with UAE.” The Hill. May 16, 2025. https://thehill.com/policy/technology/5303724-trump-administration-uae-ai-data-center/.
403. “What is an AI stack?” 2026. Hpe.com. 2026. https://www.hpe.com/au/en/what-is/ai-stack.html.
404. Nocetti, Julien. 2022. “Europe and the Geopolitics of 5G: Walking a Technological Tightrope.” Ifri.org. January 31, 2022. https://www.ifri.org/en/studies/europe-and-geopolitics-5g-walking-technological-tightrope.
405. Altowaijri, Saleh M., and Mohamed Ayari. 2025. “The Synergistic Impact of 5G on Cloud-To-Edge Computing and the Evolution of Digital Applications.” Mathematics 13 (16): 2634. https://doi.org/10.3390/math13162634.
406. “EUR-Lex - 52025JC0009 - EN - EUR-Lex.” 2025. Europa.eu. 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A-52025JC0009&.
407. Beyer, Jessica. 2025. “Undersea Alliances: Japan, the U.S., and the Geopolitics of Submarine Cable Security - the Henry M. Jackson School of International Studies.” The Henry M. Jackson School of International Studies. October 23, 2025. https://jsis.washington.edu/news/undersea-alliances-japan-the-u-s-and-the-geopolitics-of-submarine-cable-security/.
408. “Press Release.” 2024. ITU. 2024. https://www.

END NOTES

itu.int/en/mediacentre/Pages/PR-2024-11-29-advisory-body-submarine-cable-resilience.aspx.

409. Reuters Staff. 2026a. "Finnish Police Release Russia-Linked Ship Held in Cable Sabotage Case." Reuters, January 12, 2026. https://www.reuters.com/business/media-telecom/finnish-police-release-russia-linked-ship-held-in-cable-sabotage-case-2026-01-12/.

410. "Damage to Submarine Cables from Dragged Anchors." 2025. International Cable Protection Committee. February 24, 2025. https://www.iscpc.org/publications/icpc-viewpoints/damage-to-submarine-cables-from-dragged-anchors/.

411. "List of Equipment and Services Covered by Section 2 of the Secure Networks Act." 2021. Federal Communications Commission. March 9, 2021. https://www.fcc.gov/supplychain/coveredlist.

412. Luong, Ngor. 2024. "Forging the 5G Future: Strategic Imperatives for the US and Its Allies." Atlantic Council. September 4, 2024. https://www.atlanticcouncil.org/in-depth-research-reports/report/forging-the-5g-future-strategic-imperatives-for-the-us-and-its-allies/.

413. Kennedy, Scott. 2024. "How America's War on Chinese Tech Backfired." Foreign Affairs. November 26, 2024. https://www.foreignaffairs.com/united-states/how-americas-war-chinese-tech-backfired.

414. Allen, Gregory C. 2024. "The True Impact of Allied Export Controls on the U.S. And Chinese Semiconductor Manufacturing Equipment Industries." Csis.org. November 26, 2024. https://www.csis.org/analysis/true-impact-allied-export-controls-us-and-chinese-semiconductor-manufacturing-equipment.

415. "Secure and Trusted Communications Networks Reimbursement Program | Federal Communications Commission." n.d. Www.fcc.gov. https://www.fcc.gov/supplychain/reimbursement.

416. "Communication from the Commission: Implementation of the 5G Cybersecurity Toolbox." 2023. Shaping Europe's Digital Future. 2023. https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox.

417. National Cyber and Information Security Agency. 2025. "350-647/2025-E." National Cyber and Information Security Agency. September 3, 2025. https://nukib.gov.cz/download/publications_en/EN_2025-09-03_warning.pdf.

418. Quad Critical and Emerging Technology Working Group. 2023. "Open RAN Security Report Outcome from Quad Critical and Emerging Technology Working Group." NTIA. https://www.ntia.gov/sites/default/files/publications/open_ran_security_report_full_report_0.pdf.

419. "Data Explorer - ITU DataHub." 2026. Itu.int. 2026. https://datahub.itu.int/data/?c=701&i=19303.

420. Metz, Cade, Cecilia Kang, Sheera Frenkel, Stuart A. Thompson, and Nico Grant. 2024. "How Tech Giants Cut Corners to Harvest Data for A.I." The New York Times, April 6, 2024, sec. Technology. https://www.nytimes.com/2024/04/06/technology/tech-giants-harvest-data-artificial-intelligence.html.

421. Woodman, Lauren, and Arun Sundararajan. 2025. "Artificial Intelligence and the Growth of Synthetic Data." World Economic Forum. October 15, 2025. https://www.weforum.org/stories/2025/10/ai-synthetic-data-strong-governance/.

422. Gibert, Ona de, Joseph Attieh, Teemu Vahtola, Mikko Aulamo, Zihao Li, Raúl Vázquez, Tiancheng Hu, and Jörg Tiedemann. 2025. "Scaling Low-Resource MT via Synthetic Data Generation with LLMs." Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing, 27662–80. https://doi.org/10.18653/v1/2025.emnlp-main.1408.

423. An Dao, Tuan, Hiroki Teranishi, Yuji Matsumoto, Florian Boudin, and Akiko Aizawa. 2025. "Overcoming Data Scarcity in Named Entity Recognition: Synthetic Data Generation with Large Language Models." August 1, 2025.

END NOTES

424. Gerosa, Marco, Anna Hermansen, Anni Lai, and Adrienn Lawson. 2025b. "The State of Sovereign AI." August 2025. https://www.linuxfoundation.org/hubfs/Research%20Reports/lfr_sovereign_ai25_082525a.pdf?hsLang=en.
425. "Bhashini." 2024b. Bhashini.gov.in. 2024. https://bhashini.gov.in/.
426. Staff Reporter. 2025. "AI Singapore Launches Qwen SEA LION V4." Singapore Business Review. November 24, 2025. https://sbr.com.sg/information-technology/news/ai-singapore-launches-qwen-sea-lion-v4.
427. McKinsey & Company. 2022. "Data Localization and New Competitive Opportunities | McKinsey | McKinsey." Www.mckinsey.com. June 30, 2022. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities.
428. Iyengar, Ashok. 2022. "Data Sovereignty at the Edge." Ibm.com. August 18, 2022. https://www.ibm.com/think/insights/data-sovereignty-at-the-edge.
429. Hummel, Patrik, Matthias Braun, Max Tretter, and Peter Dabrock. 2021. "Data Sovereignty: A Review." Big Data & Society 8 (1): 205395172098201. https://doi.org/10.1177/2053951720982012.
430. Hutchinson, Jonathon, Milica Stilinovic, and Joanne E Gray. 2024a. "Data Sovereignty: The next Frontier for Internet Policy?" Policy & Internet 16 (1): 6–11. https://doi.org/10.1002/poi3.386.
431. Aaronson, Susan Ariel. 2021. "Data Is Disruptive: How Data Sovereignty Is Challenging Data Governance." Hinrichfoundation.com. 2021. https://www.hinrichfoundation.com/research/wp/digital/data-is-disruptive-how-data-sovereignty-is-challenging-data-governance.
432. Hutchinson, Jonathon, Milica Stilinovic, and Joanne E Gray. 2024b. "Data Sovereignty: The next Frontier for Internet Policy?" Policy & Internet 16 (1): 6–11. https://doi.org/10.1002/poi3.386.
433. "Enhancing Access to and Sharing of Data in the Age of Artificial Intelligence." 2025. OECD. 2025. https://www.oecd.org/en/publications/enhancing-access-to-and-sharing-of-data-in-the-age-of-artificial-intelligence_23a70dca-en.html.
434. Schrepel, Thibault. 2025. "Artificial Intelligence and Data Policies: Regulatory Overlaps and Economic Tradeoffs - Network Law Review." Network Law Review. September 3, 2025. https://www.networklawreview.org/jin-wagman-zhong-ai/.
435. Fiddler, Dayton, and Cobun Zweifel-Keegan. 2025. "IAPP." Iapp.org. August 27, 2025. https://iapp.org/news/a/fair-use-or-free-ride-the-fight-over-ai-training-and-us-copyright-law.
436. Ahmed, Ahmed, Cooper A Feder, Sanmi Koyejo, and Percy Liang. 2026. "Extracting Books from Production Language Models." ArXiv.org. 2026. https://arxiv.org/abs/2601.02671.
437. Schneider, Jacob W. S. 2023. "Generative AI's Output: How Is It Created, and What IP Rights Should It Receive?" Holland & Knight. October 3, 2023. https://www.hklaw.com/en/insights/publications/2023/10/generative-ais-output-how-is-it-created-and-what-ip-rights.
438. Bartz, Andrea, Charles Graeber, and Kirk Johnson. 2025. "States District Court Northern District of California United States District Court Northern District of California." https://storage.courtlistener.com/recap/gov.uscourts.cand.434709/gov.uscourts.cand.434709.231.0_4.pdf.
439. Del Giovane, Chiara, Janos Ferencz, and Javier López-González. 2023. "The Nature, Evolution and Potential Implications of Data Localisation Measures." OECD. November 2023.
440. Kaplan, Jared, Sam McCandlish, Tom Henighan, Tom B. Brown, Benjamin Chess, Rewon Child, Scott Gray, Alec Radford, Jeffrey Wu, and Dario Amodei. 2020a. "Scaling Laws for Neural Language Models." https://arxiv.org/pdf/2001.08361.pdf.
441. ———. 2020b. "Scaling Laws for Neural Language Models." https://arxiv.org/pdf/2001.08361.pdf.

END NOTES

442. Wu, Jason Jia-Xi. 2025. "Techno-Federalism: How Regulatory Fragmentation Shapes the U.S.-China AI Race." Harvard Law School National Security Journal. https://journals.law.harvard.edu/nsj/wp-content/uploads/sites/82/2025/12/Wu-17-Harv.-Natl-Sec.-J.-1-2025-1.pdf.

443. Chin-Rothmann, Caitlin. 2024. "Protecting Data Privacy as a Baseline for Responsible AI." Csis.org. July 18, 2024. https://www.csis.org/analysis/protecting-data-privacy-baseline-responsible-ai.

444. He, Miao, and Yongfang Chen. 2025. "Personal Data Protection in China: Progress, Challenges and Prospects in the Age of Big Data and AI." Telecommunications Policy, October, 103076–76. https://doi.org/10.1016/j.telpol.2025.103076.

445. King'Ori, Mercy. 2024. "The African Union's Continental AI Strategy: Data Protection and Governance Laws Set to Play a Key Role in AI Regulation." Future of Privacy Forum. November 18, 2024. https://fpf.org/blog/global/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/.

446. African Union. 2022. "AU Data Policy Framework for an Integrated, Prosperous and Peaceful Africa." https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf.

447. ———. 2024. "Continental Artificial Intelligence Strategy." Au.int. August 9, 2024. https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy.

448. "Data Free Flow with Trust." 2024b. OECD. 2024. https://www.oecd.org/en/about/programmes/data-free-flow-with-trust.html.

449. "What is an AI stack?" 2025. Hpe.com. March 10, 2025. https://www.hpe.com/au/en/what-is/ai-stack.html.

450. Bria, Francesca, Paul Timmers, and Fausto Gernone. 2025i. "EuroStack - a European Alternative for Digital Sovereignty." Bertelsmann-Stiftung.de. February 13, 2025. https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty.

451. Vipra, Jai, and Anton Korinek. 2023. "Market Concentration Implications of Foundation Models: The Invisible Hand of ChatGPT." Brookings. September 7, 2023. https://www.brookings.edu/articles/market-concentration-implications-of-foundation-models-the-invisible-hand-of-chatgpt/.

452. Nestor Maslej, Loredana Fattorini, Raymond Perrault, Vanessa Parli, Anka Reuel, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Juan Carlos Niebles, Yoav Shoham, Russell Wald, and Jack Clark. 2024c. "The AI Index 2024 Annual Report." AI Index Steering Committee. Institute for Human-Centered AI. Stanford University. April 2024. https://hai.stanford.edu/ai-index/2024-ai-index-report.

453. Zheng, Kena. 2025. "Antitrust in Artificial Intelligence Infrastructure – between Regulation and Innovation in the EU, the US, and China." Computer Law & Security Review 59 (October): 106211. https://doi.org/10.1016/j.clsr.2025.106211.

454. Lemley, Mark A, and Peter Henderson. 2025. "The Mirage of Artificial Intelligence Terms of Use Restrictions." ArXiv (Cornell University), January. https://doi.org/10.2139/ssrn.5049562.

455. Kerry, Cameron F., and Saurabh Mishra. 2025b. "The Myth of the Monolith: AI Is Not One Thing." Brookings. October 9, 2025. https://www.brookings.edu/articles/the-myth-of-the-monolith-ai-is-not-one-thing/.

456. Perlow, Jason. 2022. "A Summary of Census II: Open Source Software Application Libraries the World Depends on - Linux Foundation." Www.linuxfoundation.org. March 7, 2022. https://www.linuxfoundation.org/blog/blog/a-summary-of-census-ii-open-source-software-application-libraries-the-world-depends-on.

457. Khan, Saif. 2020. "AI Chips: What They Are and Why They Matter." Center for Security and Emerging Technology. April 2020. https://cset.georgetown.edu/publication/ai-chips-what-they-are-and-

END NOTES

why-they-matter/.

458. Almazrouei, Ebtesam, Olivier Cruchant, and Will Badr. 2023. "Technology Innovation Institute Trains the State-of-The-Art Falcon LLM 40B Foundation Model on Amazon SageMaker | Amazon Web Services." Amazon Web Services. June 7, 2023. https://aws.amazon.com/blogs/machine-learning/technology-innovation-institute-trains-the-state-of-the-art-falcon-llm-40b-foundation-model-on-amazon-sagemaker/.

459. "NVIDIA Optimized Frameworks." 2026. NVIDIA Docs. 2026. https://docs.nvidia.com/optimized-frameworks/index.html.

460. "NRF Singapore." 2023. Nrf.gov.sg. 2023. https://www.nrf.gov.sg/about/about-nrf-singapore/nrf-singapore/.

461. TechNode Feed. 2025. "Singapore's National AI Program Drops Meta Model and Switches to Alibaba's Qwen." TechNode. November 25, 2025. https://technode.com/2025/11/25/singapores-national-ai-program-drops-meta-model-and-switches-to-alibabas-qwen/.

462. Noor, Elina, and Binya Kanitroj. 2025. "Speaking in Code: Contextualizing Large Language Models in Southeast Asia." Carnegie Endowment for International Peace. January 6, 2025. https://carnegieendowment.org/russia-eurasia/research/2025/01/speaking-in-code-contextualizing-large-language-models-in-southeast-asia.

463. Bommasani, Rishi, Sayash Kapoor, Kevin Klyman, Shayne Longpre, Ashwin Ramaswami, Daniel Zhang, Marietje Schaake, Daniel E. Ho, Arvind Narayanan, and Percy Liang. 2023. "Issue Brief Considerations for Governing Open Foundation Models | Stanford HAI." Hai.stanford.edu. Stanford University. December 2023. https://hai.stanford.edu/issue-brief-considerations-governing-open-foundation-models.

464. Ly, Jason. 2024. "Open Foundation Models: Implications of Contemporary Artificial Intelligence." Center for Security and Emerging Technology. March 12, 2024. https://cset.georgetown.edu/article/open-foundation-models-implications-of-contemporary-artificial-intelligence/.

465. Tanner, Brooke, and Cameron F. Kerry. 2025. "Can Small Language Models Revitalize Indigenous Languages?" Brookings. March 19, 2025. https://www.brookings.edu/articles/can-small-language-models-revitalize-indigenous-languages/.

466. Chavez, Pablo. 2024a. "Sovereign AI in a Hybrid World: National Strategies and Policy Responses." Lawfare. 2024. https://www.lawfaremedia.org/article/sovereign-ai-in-a-hybrid-world--national-strategies-and-policy-responses; Desmarais, Anna. 2025. "Which European countries are building their own sovereign AI to compete in the tech race?" Euronews. January 12, 2025. https://www.euronews.com/next/2025/12/01/which-european-countries-are-building-their-own-sovereign-ai-to-compete-in-the-tech-race; Malhotra, Siddarth. 2026. "India AI Impact Summit 2026: BharatGen's Sovereign AI Model Explained." Digit.in. February 13, 2026. https://www.digit.in/features/general/india-ai-impact-summit-2026-bharatgens-sovereign-ai-model-explained.html.

467. Malhotra, Siddarth. 2026. "India AI Impact Summit 2026: BharatGen's Sovereign AI Model Explained." Digit.in. February 13, 2026. https://www.digit.in/features/general/india-ai-impact-summit-2026-bharatgens-sovereign-ai-model-explained.html.

468. "Fugaku-LLM (Fugaku-LLM)." 2025. Huggingface.co. January 10, 2025. https://huggingface.co/Fugaku-LLM.

469. "GPT-NL: Een Betrouwbare LLM." 2025. GPT-NL. 2025. https://gpt-nl.nl/commitments/.

470. "Aisingapore (AI Singapore)." 2026. Huggingface.co. February 6, 2026. https://huggingface.co/aisingapore.

471. AI Sweden Model Hub. 2026. "Organization Card." Huggingface.co. 2026. https://huggingface.co/AI-Sweden-Models.

472. "Taide (TAIDE)." 2025. Huggingface.co. November 18, 2025. https://huggingface.co/taide.

END NOTES

473. "Tiiuae (Technology Innovation Institute)." 2025. Huggingface.co. May 21, 2025. https://huggingface.co/tiiuae.
474. Struta, Iuri. 2024. "GenAI Investors Target App-Makers in 2024 as Foundation Model Focus Fades." S&P Global. April 16, 2024. https://www.spglobal.com/market-intelligence/en/news-insights/articles/2024/4/genai-investors-target-app-makers-in-2024-as-foundation-model-focus-fades-81163387.
475. Chen, James. 2019. "Algorithmic Trading Definition." Investopedia. 2019. https://www.investopedia.com/terms/a/algorithmictrading.asp.
476. Helmi Ayari, Pr. Ramzi Guetari, and Pr. Naoufel Kraïem. 2025. "Machine Learning Powered Financial Credit Scoring: A Systematic Literature Review." Artificial Intelligence Review 59 (1). https://doi.org/10.1007/s10462-025-11416-2.
477. Hafeez, Abdul, Mohammed Aslam Husain, S. P. Singh, Anurag Chauhan, Mohd. Tauseef Khan, Navneet Kumar, Abhishek Chauhan, and S. K. Soni. 2022. "Implementation of Drone Technology for Farm Monitoring & Pesticide Spraying: A Review." Information Processing in Agriculture 10 (2). https://doi.org/10.1016/j.inpa.2022.02.002.
478. Krishna Agrawal, Kumar, Adam Yala, and Maggie Chung. 2025. "UC Berkeley and UCSF Researchers Release Top-Performing AI Model for Medical Imaging." Berkeley.edu. November 20, 2025. https://cdss.berkeley.edu/news/uc-berkeley-and-ucsf-researchers-release-top-performing-ai-model-medical-imaging.
479. Ferreira, Fábio J. N., and Agnaldo S. Carneiro. 2025. "AI-Driven Drug Discovery: A Comprehensive Review." ACS Omega 10 (23). https://doi.org/10.1021/acsomega.5c00549.
480. Anna Grøndahl Larsen, and Asbjørn Følstad. 2024. "The Impact of Chatbots on Public Service Provision: A Qualitative Interview Study with Citizens and Public Service Providers." Government Information Quarterly 41 (2): 101927–27. https://doi.org/10.1016/j.giq.2024.101927.
481. "The Policing Project." 2024. The Policing Project. October 2, 2024. https://www.policingproject.org/ai-explained-articles/2024/9/6/how-policing-agencies-use-ai.
482. Tuhin, Muhammad. 2025. "How AI Is Used in Autonomous Vehicles." Science News Today. April 25, 2025. https://www.sciencenewstoday.org/how-ai-is-used-in-autonomous-vehicles.
483. "AI Lab Areas - Autonomous Traffic Management." 2022. University of Texas at Austin. 2022. https://www.cs.utexas.edu/~ai-lab/?Autonomous-Traffic.
484. "Privacy International | Action Privacy International." 2025. Privacyinternational.org. November 10, 2025. https://privacyinternational.org/report/5704/dual-use-tech-anduril-example.
485. European Parliament. 2025. "EU AI Act: First Regulation on Artificial Intelligence." European Parliament. February 19, 2025. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
486. International Organization for Standardization. 2023. "ISO/IEC 42001:2023." ISO. 2023. https://www.iso.org/standard/42001.
487. IEEE. 2024. "The IEEE Global Initiative 2.0 on Ethics of Autonomous and Intelligent Systems." IEEE Standards Association. August 13, 2024. https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/.
488. "OSIA Specification." n.d. OSIA. https://osia.readthedocs.io/en/stable/01%20-%20intro.html.
489. ———. 2024b. "Artificial Intelligence." OECD. 2024. https://www.oecd.org/en/topics/policy-issues/artificial-intelligence.html.
490. "Hiroshima AI Process." n.d. Www.soumu.go.jp. https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html.
491. "Global Partnership on Artificial Intelligence." n.d. OECD. https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html.
492. "Artificial Intelligence." n.d. ITU. https://www.

END NOTES

itu.int/en/action/ai/Pages/default.aspx.

493. United Nations. 2023. “AI Advisory Body.” United Nations. December 2023. https://www.un.org/en/ai-advisory-body.

494. UNESCO. n.d. “Ethics of Artificial Intelligence.” UNESCO. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics.

495. “Artificial Intelligence | UNECE.” 2023. Unece.org. 2023. https://unece.org/artificial-intelligence.

496. Villalobos, Jaime. 2023. “International AI Institutions.” Institute for Law & AI. September 29, 2023. https://law-ai.org/international-ai-institutions/.

497. Kerry, Cameron F. 2024. “Small Yards, Big Tents: How to Build Cooperation on Critical International Standards.” Brookings. March 11, 2024. https://www.brookings.edu/articles/small-yards-big-tents-how-to-build-cooperation-on-critical-international-standards/.

498. Kerry, Cameron F., Joshua P. Meltzer, Andrea Renda, and Andrew W. Wyckoff. 2025. “Network Architecture for Global AI Policy.” Brookings. February 10, 2025. https://www.brookings.edu/articles/network-architecture-for-global-ai-policy/.

1775 Massachusetts Ave NW,
Washington, DC 20036
(202) 797-6000
www.brookings.edu