The Geopolitics of Compute: Sovereignty, Power and Strategic Dependence in the AI Infrastructure Race

The Economy Research Editorial[1,2]

[1]The Economy Research, 71 Lower Baggot Street, Dublin 2, Co. Dublin, D02 P593, Ireland

[2]Swiss Institute of Artificial Intelligence, Chaltenbodenstrasse 26, 8834 Schindellegi, Schwyz, Switzerland

Abstract

Artificial Intelligence is no longer only a product of algorithms and model architectures; it is increasingly shaped by the physical geography of the infrastructure that enables its training, hosting and regulation. This paper explores the rise of compute sovereignty as an integral feature of twenty-first-century geopolitics. It argues that data centers, advanced semiconductors, electricity grids and cloud computing platforms are now strategic assets through which states exercise regulatory control, economic influence and national-security power. The paper distinguishes surface-level access to AI services and genuine control over the infrastructure supporting advanced AI systems. It describes the concentration of frontier computing in the United States and China, Europe's reliance on foreign cloud providers, semiconductor and rare-earth choke points, and rapidly rising electricity demand as new sources of strategic vulnerability and dependence. The paper concludes by considering how authoritarian control of AI infrastructure affects others and how smaller states can chart a different course. Democratic governments should intervene by treating compute as critical infrastructure through a swift networked supergrid, data center and system architecture build-out, by bolstering semiconductor and global supply chain resilience and by strengthening democratic leadership in AI development by coordinating AI governance and technical standards, entering into strategic investment partnerships with allies committed to open, transparent and sustainable systems and ensuring effective civil-society oversight.

1 Introduction - From Data Centers to Geopolitical Infrastructure

The development of AI has transformed data centers from technical infrastructure into strategic geopolitical assets. Recent conflict scenarios show why data centers are increasingly understood as strategic infrastructure: a strike on major facilities would affect not only operators, but also the banks, telecoms, public services and AI systems that depend on them.[1] The attackers understood that striking these large cloud campuses was about more than just punishment of the tech companies involved: it aimed to undermine the banking, telecoms, government and other infrastructure whose operations depended on those data centers. These targeting tactics are widely observed even outside the Middle East, with Vogt and Kollars noting that attacks on data centers can harm not only the operator but also the organizations that rely on them for storage, networking and AI integration. The key terrain is the compute infrastructure.

While modern AI data centers may appear to the casual observer to just be another warehouse, what lies within are rows of high-density compute racks– in other words, the new factories of the intelligence economy. Running such facilities requires vast resources of power, air conditioning and network capacity, thereby physically tying the facility to the host country.[2] Governments have long been aware that the location of a data center can be an important factor and cloud and AI analytics strategists now include residency and sovereignty considerations among the issues they take into account when choosing a data center location for AI workloads.[3] Policy specialists increasingly discuss sovereign AI: the desire for each nation to keep a tight grasp on its own data and compute resources. Recent industry analysis similarly treats data centers as core infrastructure for AI-native sovereignty. In this respect, the story of AI infrastructure can no longer be told purely as an IT or business story; it is a story of political power and national sovereignty.[4]

However, much of the debate still frames AI as primarily a harmless tool or a productivity increase, ignoring some higher stakes. This framework is flawed because compute location is now a political challenge with serious implications. Computing has long been thought of as a common factor, a commodity similar to cheaper hardware or newer chips that help everyone run faster. The article develops the alternative view that the modern geography of computing provides a strategic channel. The country that possesses the servers and chips at the heart of a powerful AI can impose rules, taxes and standards on all of the digital flows that transit them.[5] It has levers to influence the structure of the AI the world builds, as well as the distribution of its benefits and pitfalls. This is increasingly visible across national security, economic competitiveness and the values embedded in AI systems.

To fix ideas, consider the superpowers today: as of mid-2025, around three-quarters of the world's most powerful AI compute clusters are based in the United States.[6] The US thus has access to most of the raw computing resources powering frontier AI research and innovation. China, by contrast, had significantly less operational capacity, but is mobilizing quickly to narrow the shortfall.[7] Many U.S. allies lag behind: for instance, no individual European state has yet developed an AI data cluster as sizable as the Amazon-Anthropic megacluster in Indiana. Some allies (Australia, South Korea, Italy) had effectively no large AI-specific data hubs in place by 2025. In a situation such as this, even relatively small variations in compute capacity could create significant advantages or disadvantages over time.

The article argues that treating computing as a commodity obscures second-order effects.[8] Unlike, for example, a faster spreadsheet algorithm (which tends to simply make users faster within a stable system), AI computing on the available infrastructure will reconfigure the system to some degree. It will influence incentives and quantitative research in industry, governments and academia. Its technology will evolve education, labor and money in the most fundamental ways. The nation that fields the leading-edge training infrastructure will dictate technical standards and have the option to use them for means of surveillance or war; the nation that doesn't run the train runs the risk of dependence.[9] But if democracies co-invest in resilient AI infrastructure, they can use it to promote free society values, safety norms and shared prosperity.[10]

The analysis first examines why governments increasingly treat AI compute as a strategic national asset and why only a limited number of states can build frontier-scale infrastructure independently. It then considers compute as a geopolitical resource whose location shapes regulatory authority, economic dependence, military capability and control over digital services. Drawing on recent evidence on data-center expansion, energy demand and semiconductor supply chains, the article argues that surface-level access to AI tools should not be confused with the institutional capacity to train, host and govern advanced systems.

2 AI Infrastructure as a National Strategic Asset

Many governments now treat compute as a strategic asset and increasingly place data-center buildout at the center of national AI strategies.[11] This means thinking of a network of datacentres and supercomputers, much as a national industry, to be promoted and responded to by government policy. For instance, the UK has conducted its own analysis and warned of an impending compute gap: if current trends continue, by 2030, the UK risks having a shortfall of as much as 5 gigawatts of AI-appropriate data center capacity.[12] The country currently has just under 2GW and even if this were to double, from 1.84 to 3.3 GW, standing demands could reach 5-8.5GW; a reduction in the UK's share of global AI compute from about 3% to 1-1.5% by 2030 could follow. Achieving the country's own target of approximately 6 GW of capacity by 2030 would require large investments, subsidies and relaxed regulations to overcome existing challenges. Analysts have warned that the UK cannot compete with the United States or China in gigawatt-scale AI infrastructure without addressing high energy costs and slow permitting. One advisor has argued that the UK may need to accept that it will not be an AI superpower, pointing out that, already, the US, Saudi Arabia, the UAE, and other countries are investing billions into AI datacenters and chips.

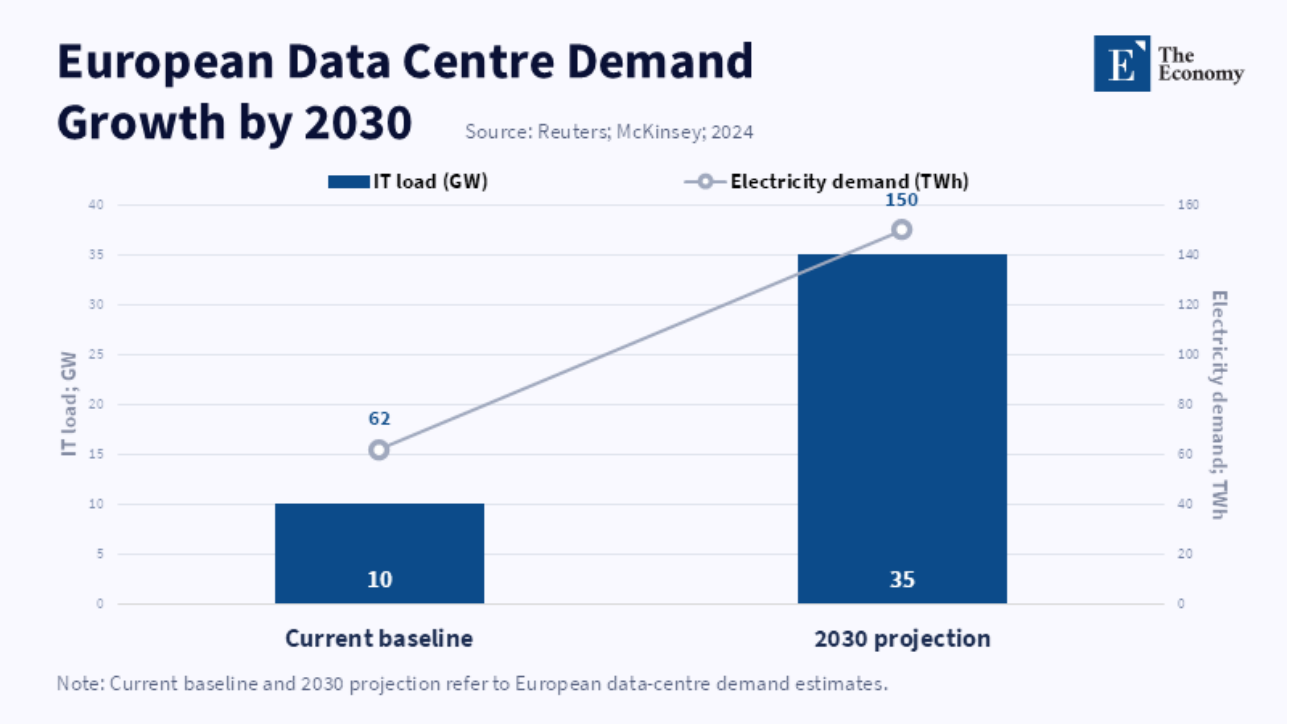

Figure 1: Europe's projected capacity gap shows why AI sovereignty depends on power and grid expansion.

For these reasons, the majority of nations, even ones with limited computing resources, will seek some role for domestically hosted computing. What is driving the preference for sovereign hosting is the logic of sovereignty and resilience.[13] If a country hosts nodes/compute providers, the best way to keep key services under one's own jurisdiction remains. Sovereign data regulation principles are well established and coexist with ad-hoc AI pathways: having a center in a legal jurisdiction makes it subject to that country's tax and privacy rules and it is impossible to disconnect with a simple decree. For example, India's government has been actively funding and hosting new outlets for domestic AI activities and is requiring that sensitive data be processed on local servers. Europe has also begun to assess its compute capacity and fund projects that create a network of European supercomputers like the EuroHPC[14] which will allow it to achieve greater technological independence; even other smaller or less compute-rich countries may face a dilemma of having no meaningful domestic compute capacity if they do not host compute providers domestically and will have to pay to import AI services under terms set by foreign providers. But even nations as small as Niger understand the risk of their lack of compute and might be forced to pay for it, at the whim of whatever moral framework or censorship parameters the host country applies, which is why like India, they are also looking to block off and dominate computing supplies: Deloitte has advised firms to incorporate location and sovereignty requirements into infrastructure decisions.[15]

At the same time, however, only a handful of nation-states are able to out-build the full-blown formation of an AI infrastructure that hearkens back to the space race of the 1960s. And those nation-states are explicitly the U.S. and the People's Republic of China. According to the recent analysis of global computer nodes undertaken by the Carnegie Endowment, nearly three-quarters of all advanced AI compute clusters as of the middle of 2025 lay within the borders of the U.S. with China accounting for roughly 14%. Both possess the financial resources and strategic imperative to leap ahead. The U.S. has committed approximately $52 billion (via the CHIPS and Science Act) for its up-to-date computing infrastructure.[16] China has directed significant strategic capital and

state funding toward domestic chip design and gigawatt-scale AI hubs in its power-rich western provinces.[17] In the Asian region, existing growth rates are rapid with demand being forecast to grow by double digits.[18]

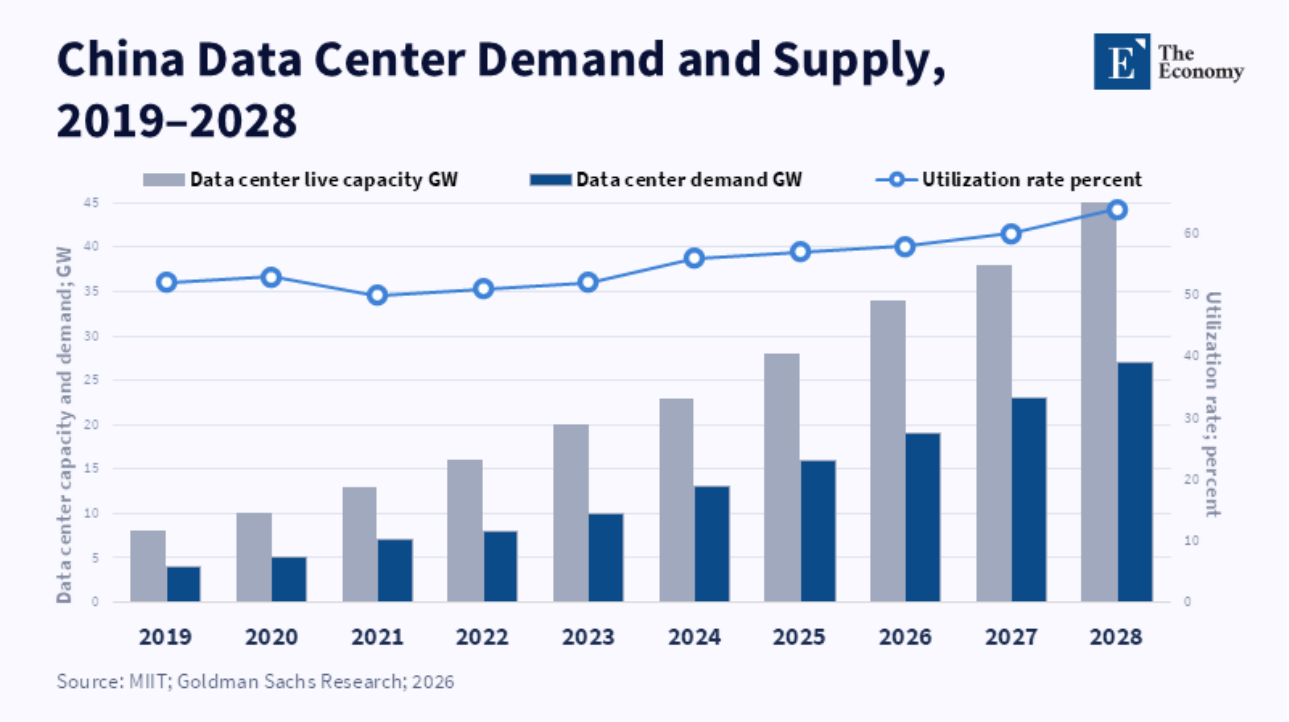

Figure 2: China's rising utilization shows how quickly domestic demand can absorb new data-center capacity.

Even with interest, real-world difficulties persist. Repeatedly, experts find that time-to-power, meaning the speed at which data centers become operational, can matter more than narrow cost incentives.[19] For instance, a simple one-year lead in data center operation, according to Carnegie, can amount to hundreds of millions of dollars, more than tiny profit-gap variations in energy prices or tax incentives. Countries with faster permitting and grid hookups (like the UAE or Finland) can get ahead of slow-onsetting competitors; this is one reason many US friends have not won the big data center contracts. Europe's slow permitting and slow grid connection put 10-year-old major AI data centers behind the U.S. developments.

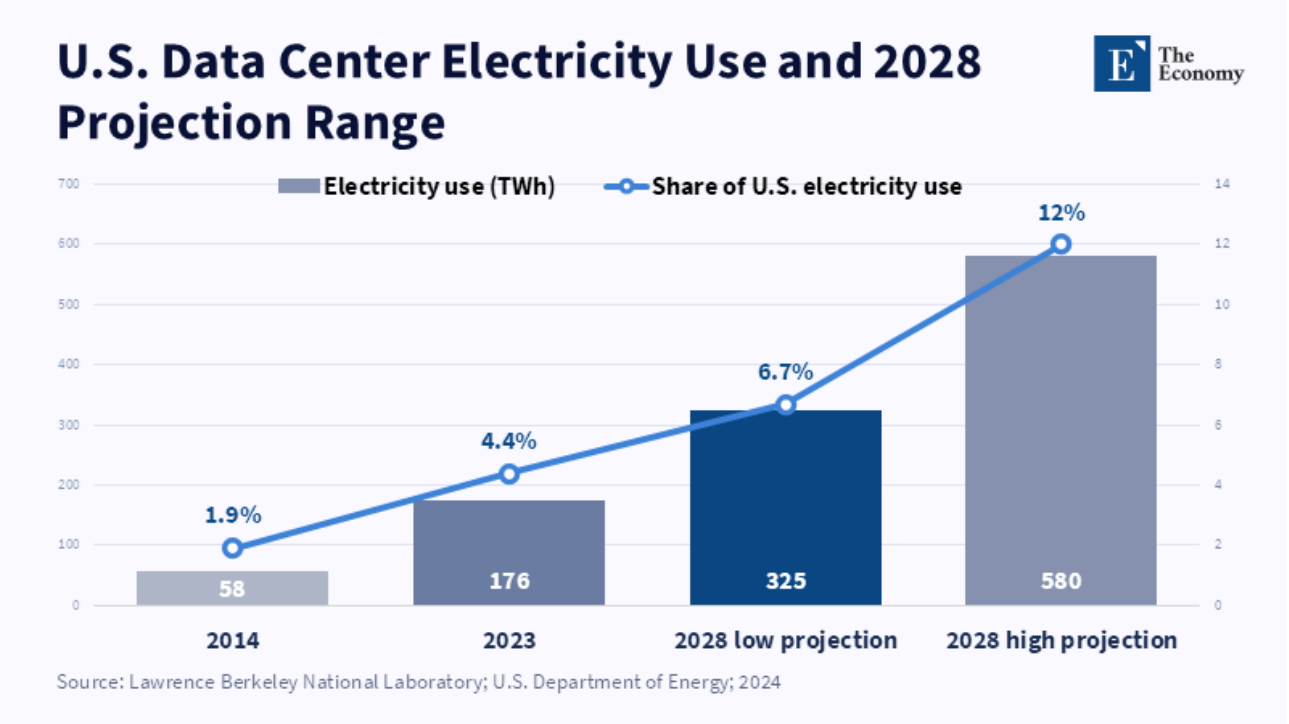

Figure 3: The projected increase in U.S. data-center electricity consumption illustrates how grid access is becoming a central constraint on AI expansion.

As such, the outset of AI infrastructure is widely accepted as a matter of national security. All countries use public money and efforts to encourage collaboration with industry. In the UK, for example, public officials have invested billions of dollars in deepening investment in supercomputing resources and establishing regionally-based "AI Growth Zones" with upgraded grid connections;[20] In Asia, governments are creating public-private forums to address electricity shortages for large data halls. In Malaysia, recent measures created special tariffs for data centers, while preventing new licenses for non-AI data centers, so as to better "align capacity expansion with Malaysia's AI ambitions." China's East Data, West Computing policy has had a similar goal-the provision of new energy-hungry computing infrastructure, which directs the use of renewable energy to the western regions.[21] The common thread is that controlling the IT infrastructure provides the leverage necessary for power in the information age.

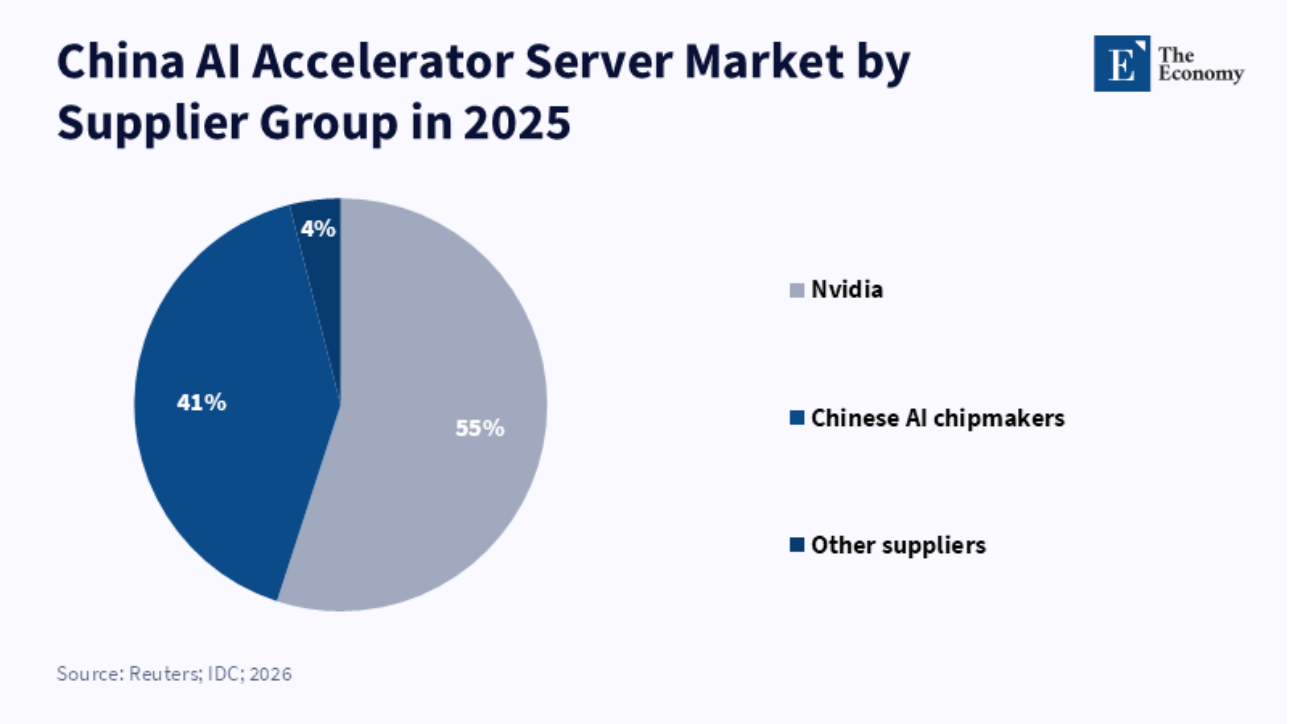

Figure 4: China's accelerator market shows both continued foreign dependence and rapid domestic substitution.

Ultimately, for many countries, the goal is not necessarily to win the build-out race against the U.S. and China, which is unattainable. The goal is to secure a place in the infrastructure race high enough to avoid being dependent. Call it the presence of a domestically available compute ecosystem that can do most of what is needed for government and industry, even if state-of-the-art model training must currently remain elsewhere. A country's relative strength in infrastructure matters far more than the absolute number. It is the ability to secure that strategic position that will determine whether strong U.S. and Chinese competitors will have to bring their suppliers along with them, or whether one day American companies, Chinese companies and any others will be the world's users for those foreign computer systems and transfer technological value away from the U.S. and China. Similarly, like energy, finance and all sorts of other sectors before it, the AI infrastructure race has become part of a broader view of a nation's technological strategy.

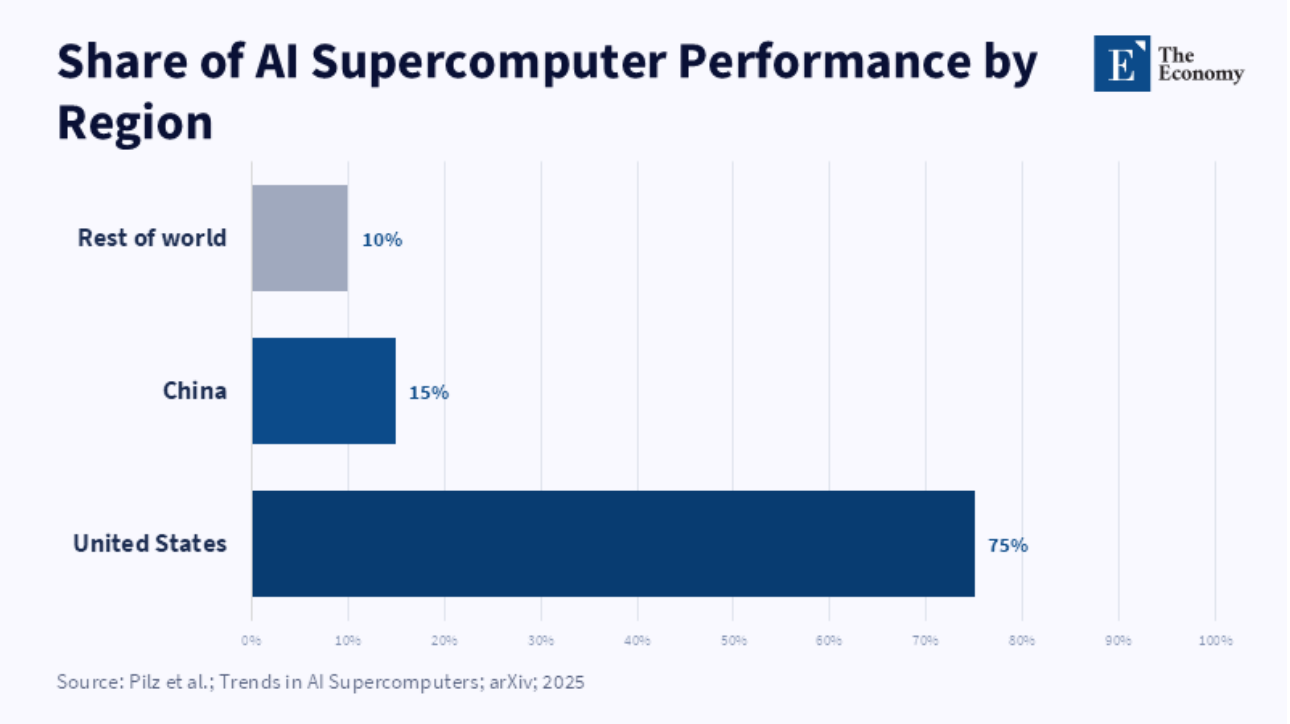

Figure 5: The concentration of advanced AI performance in the United States and China reveals the unequal geography of frontier compute capacity.

3 Compute as the New Strategic Resource

Throughout history, countries have fought over the strategically crucial commodities that powered the technologies of their time: oil powered tanks and jets, while steel and coal crafted railways and ships. AI is catalyzing a comparable paradigm: compute is emerging as the resource that will define the digital century.[22] Recent analysis suggests that technological revolutions often elevate new resources to strategic prominence and AI is producing a similar shift. In this analogy, a server farm would be the new oil refinery, while GPUs and semiconductors would be the new crude. The consequences are comparable to previous ages: nations that direct control over these commodities can tax and regulate them, affect their worldwide trade and infuse their values into the finalized technology.

Fundamentally, this resource is not a well or a mine, but the infrastructure through which machine intelligence is produced, hosted and governed. The AI resource has broad implications; governments can regulate data, limit access and extract intelligence from their networked interactions. Recent compute-policy analysis argues that countries that host compute can tax it, control access to it, and regulate its use.[23] This control is akin to what is exercised over the oil supply chain: setting prices, allocating who gets the fuel and using access as a source of leverage.

Should the infrastructure (and thus control) slip into authoritarian hands, the game changes substantially.[24] The authors of the Carnegie report conclude that ”the countries that host the buildout will shape the future of AI: who controls it, what values it contains, how it is used”. To highlight the end states, the authors compare democratic and authoritarian regimes. The same analysis contrasts a democratic pathway, in which AI may better reflect safety and liberal values, with an authoritarian pathway, in which compute control could

strengthen repression and military dominance. In essence, controlling the AI compute supply is a relatively cheap way to project political power domestically through coercion and externally through force. Just as the control of the world supply of oil conferred physical-world power, control of the global AI compute cloud might confer virtual-world dominance.

The similarities go even further when we ask what dependency enables. There is a striking real-world example: In 2025, China used its dominant position in rare-earth processing and supply to disrupt parts of the global technology supply chain.[25] According to CSIS, China's export restrictions on heavy rare earths led to a serious disruption in industries ranging from automaking to aerospace; U.S., Japanese and European automakers suffered delays that threatened to bring domestic manufacturing to a halt. Suddenly, dozens of US programs, ranging from ballistic missile defense to laptops, faced abandonment. Governments responded by unleashing armies of scientists and engineers and showering billions of taxpayer dollars on supply diversification and stockpiling. The AI parallel would be a single country whose control of GPU exports or cloud infrastructure could bring industry or academic research to a grinding halt.[26]

Figure 6: Concentrated rare-earth production demonstrates how control over upstream inputs can be converted into geopolitical leverage.

Europe illustrates this dependence particularly clearly. Today, most serious AI development on the continent takes place on servers provided by U.S. or Chinese cloud infrastructure providers.[27] If in some future time these companies decide to cease providing their services (for instance, in light of escalated sanctions or geopolitical tensions), the consequences could be dire: this could trigger severe relocation pressure or encourage entire projects to suddenly head overseas. This is akin to the rare-earth scenario: the artificial embargo or shortage of digital resources will probably result in similar disruption, forcing firms to relocate workloads and governments to seek emergency alternatives to prepare for a crisis. In fact, experts in law have pointed out that national authorities may lose direct control over the legal and operational conditions governing sensitive data once specific

digital infrastructure is foreign-owned: thus, European regulators, for instance, have long been concerned that U.S. legislation (such as the CLOUD Act) could constrict American cloud companies' flow or disconnection of European digital data.[28] The power to control AI computing resources is fast becoming as strategically important as controlling other critical infrastructure networks.

An analogy that can be drawn here is the one of a new resource curse. While in the age of oil, countries looked under the metaphorical barrel: if oil was shipped to your country, you did well, if it was not, you paid the political price. Now think about the fact that the dominant resource today is knowledge and the byproduct of the computation is knowledge too. And now, the output of these systems would be withheld or taxed - the data centers would become virtual gatekeepers of innovation. The host country can therefore become a gatekeeper of innovation, able to direct domestic industry, limit rivals and set the rules for digital commerce. Just as energy markets once generated collective governance through producer alliances, compute is now producing calls for allied coordination around semiconductors, data centers and digital grids.[29]

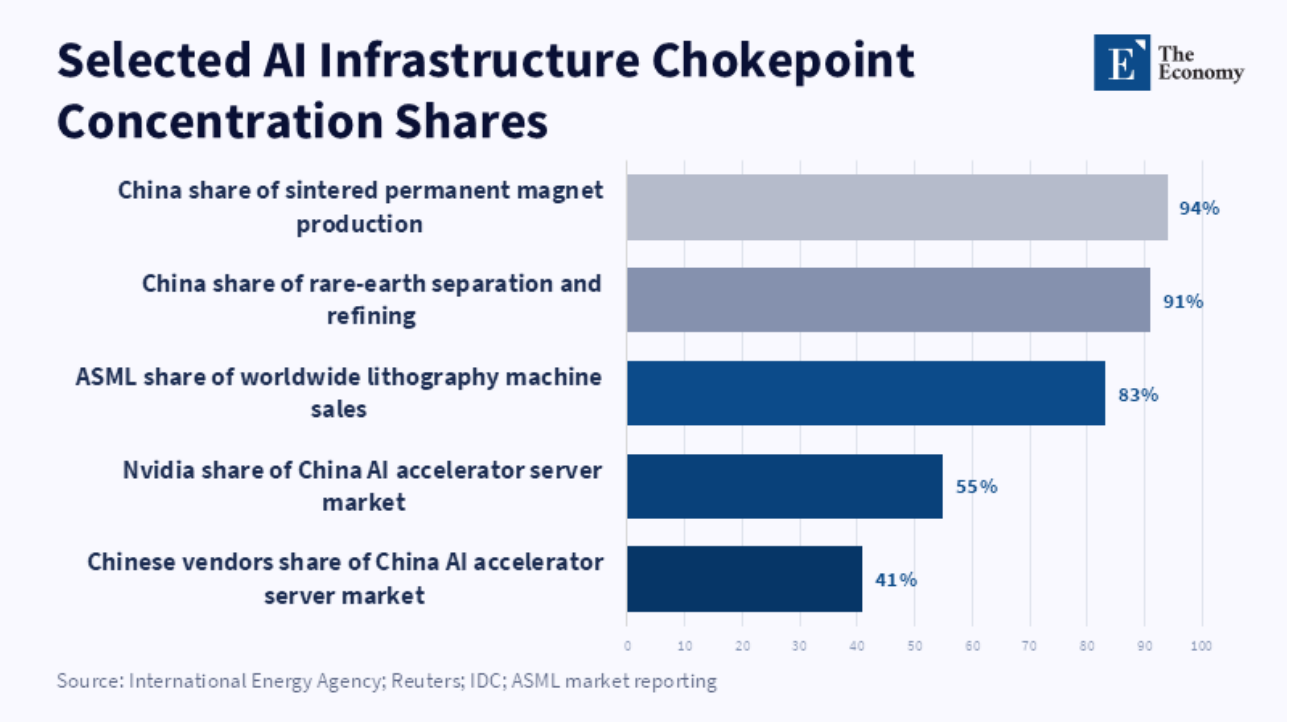

Figure 7: AI infrastructure relies on highly concentrated hardware, minerals and manufacturing equipment.

Lastly, even computing itself has material inputs and climate effects and these too feed into strategic calculations. Top-end GPUs, advanced wafers and lithography equipment are concentrated in a small number of firms and jurisdictions[30] (say, NVIDIA builds the majority of AI chips, while a handful of firms like TSMC and Samsung build the immense majority of high-end wafers and ASML sells all the most sophisticated lithography machinery). These chokepoints give allied governments leverage to restrict access to strategically sensitive hardware and manufacturing inputs, as the United States has already done through export controls on advanced chips and chipmaking equipment.[31] Likewise, the power demand of an AI farm is enormous. In 2024, the IEA estimated that data centers used around 415 TWh, roughly 1.5% of global electricity consumption, with demand projected to rise to around 945 TWh or roughly 3% by 2030.[32] Its strategic qualities have therefore been inherited wholesale from oil: heavy, globally networked and dominated by a handful of producers. In

short, computing has become a strategic asset.

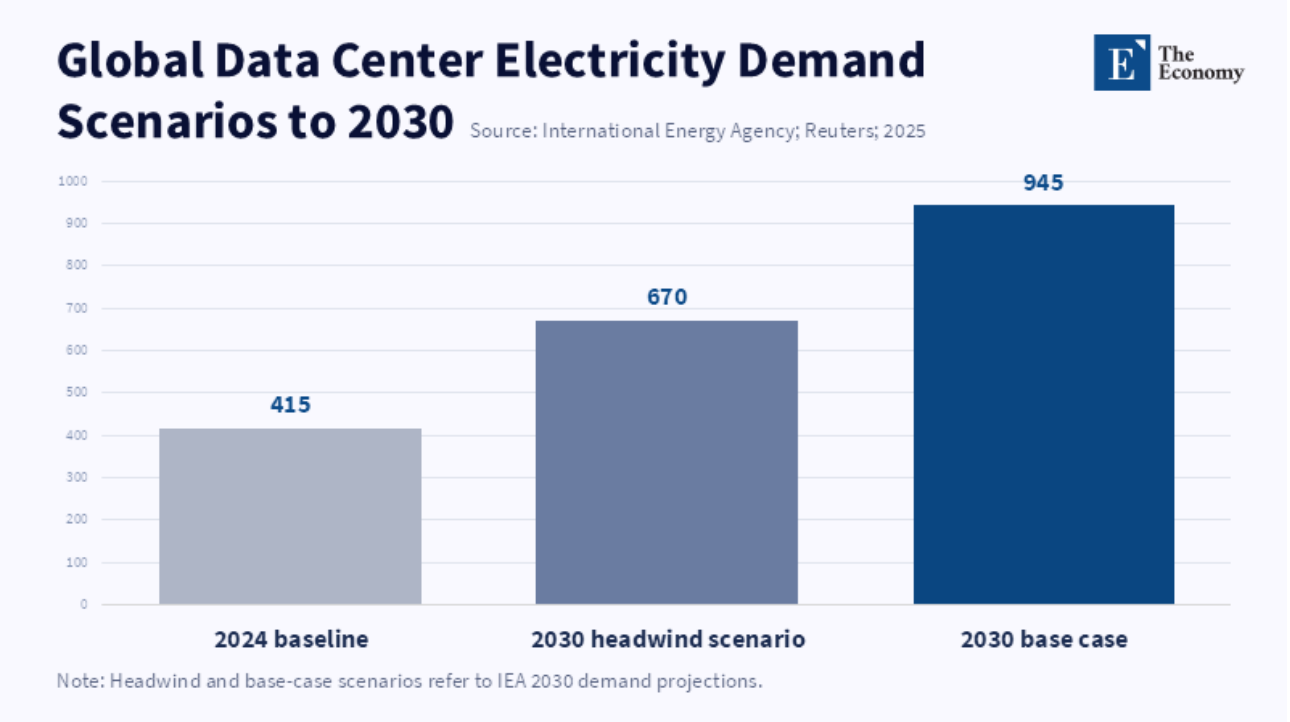

Figure 8: Even slower-growth scenarios point to a sharp rise in global data-center electricity demand.

4 Conclusion – Compute Sovereignty and Democratic Leverage

The preceding analysis shows that AI compute is not neutral background infrastructure. Its allocation among countries will determine who gains from AI and who remains on the back foot. The belief that AI is only another productivity tool, comparable to a fresh set of 3-D printers or the next wave of automation-is far too narrow; as the article has shown, AI infrastructure is currently acting as a traditional geopolitical resource-which gives leverage to the host governments (which may be in power or in the opposition), guides international relations and shapes the distribution of winners and losers beyond the immediate benefits to productivity. The shape of AI development in the coming years and perhaps the shape of the digital world order itself, will be – to a significant extent – decided by the rivalry over who makes, hosts and directs the engines of intelligence.

The analysis yields several important lessons of strategic necessity: first, that democracies need to understand that the security of their AI is in their computing infrastructure and connections. They cannot rest on open markets, other markets and profit alone - they must develop with purpose. Domestically, this means making it easy to permit data centers, investing in green power and digital grids and perhaps providing targeted support (e.g., conditional tax incentives, fast-tracking) for strategic projects, not just subsidizing incumbents, to build capacity and competitiveness. Domestic measures include looking to avoid regional or national disparities in computing build that could needlessly develop the edge for nations or worsen pollution - through linking data centers to national renewables targets, for example - and adopting transparent governance standards. Internationally, awareness is growing that the democratic interests in this regard will require cooperation. Recognizing that no single democracy - not even the United States - can build the world's AI infrastructure alone, an ongoing analysis finds that allies will need to share their resources and expertise so that since the

building blocks for AI infrastructure are so large, the U.S. cannot succeed alone. Plans for a compute coalition, a network of allied democracies co-investing in transborder data center campuses and coordinating regulatory standards, need to be seriously explored.[33] To avoid duplicating capacity and to inhibit any authoritarian attempt to corner the global market, a compute coalition could distinguish its member nations from this aim by intentionally apportioning compute projects among them accordingly. Countries that are otherwise too small to compete on their own could also find themselves integral players.[34]

Secondly, the geopolitical framing forces us to see some of these short-term gains differently. A university or firm might, say, find it expedient to train AI in the lowest-cost country, only to have effectively exported that cost. If this creates a future supply bottleneck-or if it means them ceding future oversight to regulation-the overall cost could be even higher. Educators and policy-makers must brace for this new reality: curricula in the STEM fields, as well as research efforts, should include training in topics like data sovereignty and infrastructure security. Policies to encourage inclusive AI training should be comprehensive in closing the digital divide created when only a tiny handful of cities or countries have access to world-class computing.[35] Policy makers, also, must understand that policies that boost AI uptake (via subsidies, use of public services) without trying to guarantee access to computing may exacerbate inequalities or create dependencies.[36] At best, countries lacking infrastructure are reduced to customers of AI; at worst, they constitute vulnerable clients. As a corollary, regulation on AI use should be coupled with policies around AI ownership-that is, who creates, controls, manages and regulates AI. Additionally, national governments and international institutions should promote open standards and interoperability, so that more small countries or independent researchers can access the high-powered, global compute networks without being commoditized into proprietary ecosystems.[37] Much debate around the superiority of centralization or decentralization of AI infrastructure is emerging, against the backdrop of open source here: this episodic push-back suggests some may want to see a distributed network. With a centralized versus distributed infrastructure debate on the table, policymakers should integrate the open-systems dilemma into planning for AI governance.

Finally, the compute strategy must be coupled with a sustainability and governance strategy. AI's rising compute demands are increasing pressure on global energy systems.[38] Without integration of energy and technology planners, we could instigate crises like the glut of embargoed rare-earth minerals shared by previous economists and strategists: for instance, envisage the continued AI implementation exceeding the capacity of renewables, forcing grids to partially turn to coal or gas and flatten climate targets. Conversely, countries could be enticed to battle others for cheap solar and wind potential, igniting green resource battles. Neither is a good outcome. The optimal scenario is multilateral: coordinate power grid development with data infrastructure ambitions, use efficiency as a principle and agree on methods for global resource sharing.

In conclusion, the coming era is not just one of more intelligent code, but of more intelligent strategy. The battle for the outcome of AI will come down to computation as well as code. Past experiences- from coal conflicts to computer chip sanctions- serve as reminders that a surrender of control over key resources means subjugation. Democracies worldwide need to treat AI computing as a matter of strategic importance. This will involve acts of urgency to build robust, decentralized and responsible compute infrastructure and diplomacy across nations to guide this infrastructure on a path aligned with the rule of law. The next decade will thus require increased

diplomacy, new frameworks for transnational cooperation, and active participation by civil society. Civil society organizations should be brought into the fold early on, so that AI infrastructure expansion does not come at the expense of privacy, labor rights, or local communities.[38] In parallel, there should be developments with research into alternative forms of computing architectures, new sources of energy and solutions in the domain of governance. Only these measures will enable the promise of AI to be celebrated for all and not cheaply exploited by a few. The policy window is narrow, so that the future balance of power in the world is not determined solely by the innovation of the engines, but also by their locations and the perceptions of their creators and regulators.

References

[1] Trusilo, D. and Danks, D. (2024) 'Commercial AI, Conflict, and Moral Responsibility: A Theoretical Analysis and Practical Approach to the Moral Responsibilities Associated with Dual-Use AI Technology', *arXiv*.

[2, 32, 38] International Energy Agency (2025) *Energy and AI*. Paris: International Energy Agency.

[3, 13, 27] Richardson, A., Yi, H., Nie, M., Wisdom, S., Price, C., Weijers, R., Veld, S. and Baker, M. (2025) 'How Sovereign Is Sovereign Compute? A Review of 775 Non-U.S. Data Centers', *arXiv*.

[4] Cruzes, S. (2026) 'AI Infrastructure Sovereignty', *arXiv*.

[5, 10, 19, 22, 23, 24, 29, 33, 34] Phillips-Robins, A., Tawil, T. and Winter-Levy, S. (2026) *The Compute Coalition: How to Build the Future of AI in the Free World*. Washington, DC: Carnegie Endowment for International Peace.

[6, 7] Pilz, K.F., Sanders, J., Rahman, R. and Heim, L. (2025) 'Trends in AI Supercomputers', *arXiv*.

[8] Pilz, K., Heim, L. and Brown, N. (2023) 'Increased Compute Efficiency and the Diffusion of AI Capabilities', *arXiv*.

[9] Buchanan, B. and Imbrie, A. (2022) *The New Fire: War, Peace, and Democracy in the Age of AI*. Cambridge, MA: MIT Press.

[11] Department for Science, Innovation and Technology (2025) *AI Opportunities Action Plan*. London: UK Government.

[12] Department for Science, Innovation and Technology (2025) *UK Compute Roadmap*. London: UK Government.

[14] European High Performance Computing Joint Undertaking (2025) *AI Factories*. Luxembourg: EuroHPC Joint Undertaking.

[15] Deloitte (2025) *Building a Modern Data Center Strategy in the AI Era*. Deloitte.

[16] U.S. Congress (2022) *CHIPS and Science Act of 2022*. Public Law 117-167. Washington, DC: United States

Congress.

[17, 18] Goldman Sachs Research (2026) *The Outlook for Data Centers in Asia*. Goldman Sachs.

[20] Department for Science, Innovation and Technology (2025) *AI Growth Zones*. London: UK Government.

[21] National Development and Reform Commission (2022) *East Data, West Computing Project*. Beijing: Government of the People's Republic of China.

[25] Reuters (2025) 'Auto Companies Face Shortages Due to China's Rare-Earth Restrictions', 5 June.

[26] Liu, J. and Lee, J.-A. (2026) 'Strategic Stalemates: The Paradox of Export Controls in the U.S.–China AI Race', *arXiv*.

[28] U.S. Congress (2018) *Clarifying Lawful Overseas Use of Data Act*. Public Law 115-141. Washington, DC: United States Congress.

[30] Semiconductor Industry Association (2025) *State of the U.S. Semiconductor Industry*. Washington, DC: Semiconductor Industry Association.

[31] U.S. Department of Commerce, Bureau of Industry and Security (2022) 'Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items', *Federal Register*, 87(197), pp. 62186–62215.

[35] Ahmed, N. and Wahed, M. (2020) 'The De-democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research', *arXiv*.

[36] OECD (2024) *Governing with Artificial Intelligence: Are Governments Ready?* Paris: OECD Publishing.

[37] European Parliament and Council of the European Union (2023) 'Regulation (EU) 2023/2854 on Harmonised Rules on Fair Access to and Use of Data', *Official Journal of the European Union*, L 2023/2854.

[39] UNESCO (2021) *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO.