RICE UNIVERSITY'S
Baker Institute for Public Policy

AI Geoeconomics: Allied Electricity and Secure Data Centers

Working Paper

AI Geoeconomics: Allied Electricity and Secure Data Centers

Gabriel Collins, J.D.[1]
Baker Botts Fellow in Energy and Environmental Regulatory Affairs

Christopher Bronk[2]
Nonresident Scholar

This publication was produced in collaboration with Rice University's Baker Institute for Public Policy. It has not been through editorial review. Wherever feasible, this material was reviewed by outside experts before it was released. Any errors are the authors' alone.

AI Geoeconomics: Allied Electricity and Secure Data Centers

Gabriel Collins and Christopher Bronk

"We asked ourselves, if we had the powers akin to the 2017 Chinese Intelligence Law to direct a company which supplies 5G equipment to telco networks, what could we do with that and could anyone stop us? … . We concluded that we could be awesome, no one would know and, if they did, we could plausibly deny our activities, safe in the knowledge that it would be too late to reverse billions of dollars' worth of investment."

— Simeon Gilding, former head of the Australian Signals Directorate's signals intelligence and offensive cyber missions[3]

Executive Summary

Global information power depends on more than just software; it requires secure physical foundations — AI compute and the electricity grids that power it. This manuscript argues that the U.S. risks ceding strategic advantage to China by neglecting the "Cloud-Grid Nexus." With PRC-linked entities already positioned to potentially influence power grids and 147 power plants across Southeast Asia, a critical digital battleground, the threat of hardware-enabled espionage and coercion is acute. To counter this, the authors propose a "Datacenters and Dynamos" strategy. This geoeconomic framework advocates for integrated U.S. and allied export financing to deploy secure computing capacity alongside reliable power generation. By treating data centers and power grids as a unified security asset, Washington can work to ensure the global AI ecosystem runs on "allied rails," preventing a repeat of the 5G infrastructure crisis and securing the physical layers of information power.

Introduction

Information power is key strategic terrain. The four core dimensions of “information power” are narratives and content, software and IT services, advanced telecommunications and computing hardware, and now, AI.[4] Dominating hardware and AI facilitate software penetration through platform effects. Giga-sized hyperscale platforms, in turn, facilitate narrative and content operations on a national and globally meaningful scale. This is in large part why platforms like Facebook, Instagram, Telegram, TikTok, and Twitter/X are so important as influence tools.[5]

Hardware matters too — just ask Israeli spyware vendor NSO, whose infrastructure and accounts were shut down in 2021 by Amazon Web Services after an Amnesty International forensic investigation showed NSO to be conducting Pegasus spyware operations using AWS.[6] Controlling the hardware facilitates pre-eminence in other parts of the influence stack and opens the door to purposeful, covert manipulation of information flows.

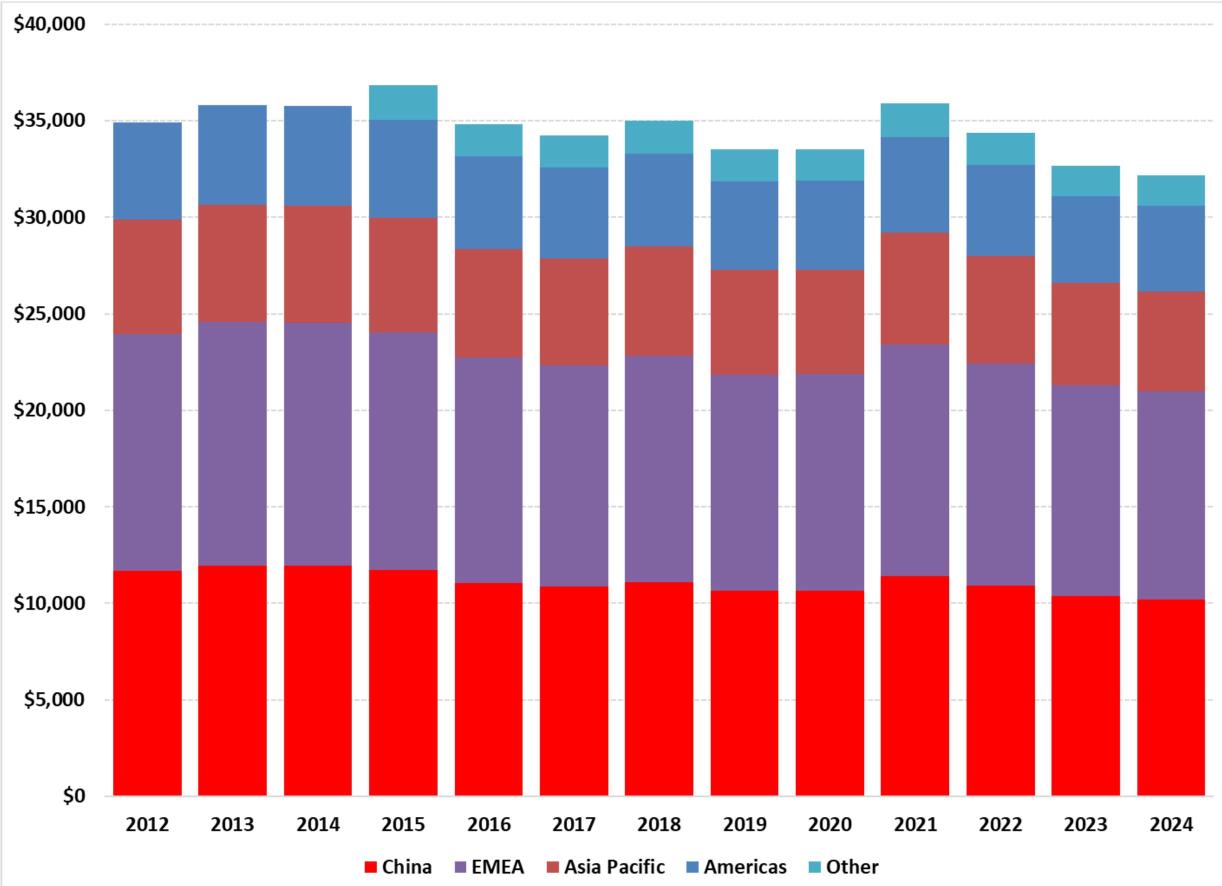
Given the importance of dominating the “atoms” hardware space as well as the “bits” software and standards space, failing to globally compete with China in the 5G infrastructure buildout globally was one of the largest mistakes U.S. tech policy made in the past 25 years.

If Huawei gear glowed red, most of the global 5G network infrastructure outside of the Five Eyes countries would be red or at least uncomfortably purple. Entrenchment of espionage-capable gear through national networks is a major challenge not just for governments, but even at the corporate level.[7] That itself is a grave concern given that prosperity generated by commercial activity is foundational to national power in a world where after a 30-year interlude, Great Power competition is back to the forefront.

Digital and telecommunications infrastructure is a life-critical, competition-critical assets class, but China’s activity abroad did not stimulate Washington’s security immune system until it was basically too late for a cost-effective, proactive response. It is now critical to avoid similar mistakes with the global hyperscale AI computing architecture and power grid security, lest the U.S. fall behind China in the strategically critical information power arena.

The competitive frontier relentlessly advances. Huawei continues installing gear at a rapid pace all around the world. For more than a decade, it has “wired the world,” sold more gear outside China than within it. Cumulative revenues from Huawei’s non-China business divisions have totaled over USD 300 billion since 2012. Looking at Huawei’s revenues alone does not demonstrate “wired the world”. Need to know what its competitors sold or Huawei’s share of global revenues. Moreover, Huawei’s revenues are on a slight downward trend and were lower in 2024 than in 2012 – that too, by itself, does not automatically mean dominance.

Figure 1 — Huawei Revenues By Region, Million USD



Source: Huawei Annual Reports, Author's Analysis.

5G Illustrates the Security Costs of Losing Control of the Stack

The challenge is global. And it literally comes up to U.S borders. The author's review of ImportGenius customs data suggests that close to a billion dollars of Huawei gear has been imported into Mexico. A 2024 U.S. Institute of Peace report estimates that 80% of phone calls in Mexico go through a Huawei device.[8] Moreover, the threat of remote espionage enabled by Huawei and PRC-origin telecoms equipment is real. Consider the example of the African Union headquarters. *Le Monde* reports that in January 2017, IT personnel at the African Union HQ building in Addis Ababa, Ethiopia (which was bult by Chinese firms) discovered that the servers were unusually saturated each night between midnight and 2am local time.[9]

Investigators subsequently found that the onsite servers were exfiltrating data at mass scale each night to servers located in Shanghai.[10] In addition to the digital surveillance, Algerian and Ethiopian experts inspecting the facility during the July 2017 African Union summit found microphones clandestinely placed under desks and in the walls.

China's ability to leap ahead with installations of 5G gear in dozens of telecom networks globally presents a tremendous response challenge, as few countries could afford what might be billion dollar or higher "rip out and replace" efforts to install gear from trusted, non-PRC providers. Indeed, the German government is now considering whether to use public funds to support removal of Huawei gear from Germany's networks, an endeavor that could cost nearly $2.5 billion, according to at least one estimate.[11]

AI's rapid emergence as a new contested digital ground does not ameliorate the Huawei problem but it does offer U.S. policymakers an opportunity to capture as much global AI "compute territory" as possible and push for AI ecosystems to run as much as possible on an American and allied hardware and software stack.

In that spirit, this analysis addresses the need for secure AI compute architecture as well as its conjoined network twin, secure and reliable electricity grids. The two fit together closely as part of a global "information power relations" competition between China and the United States.

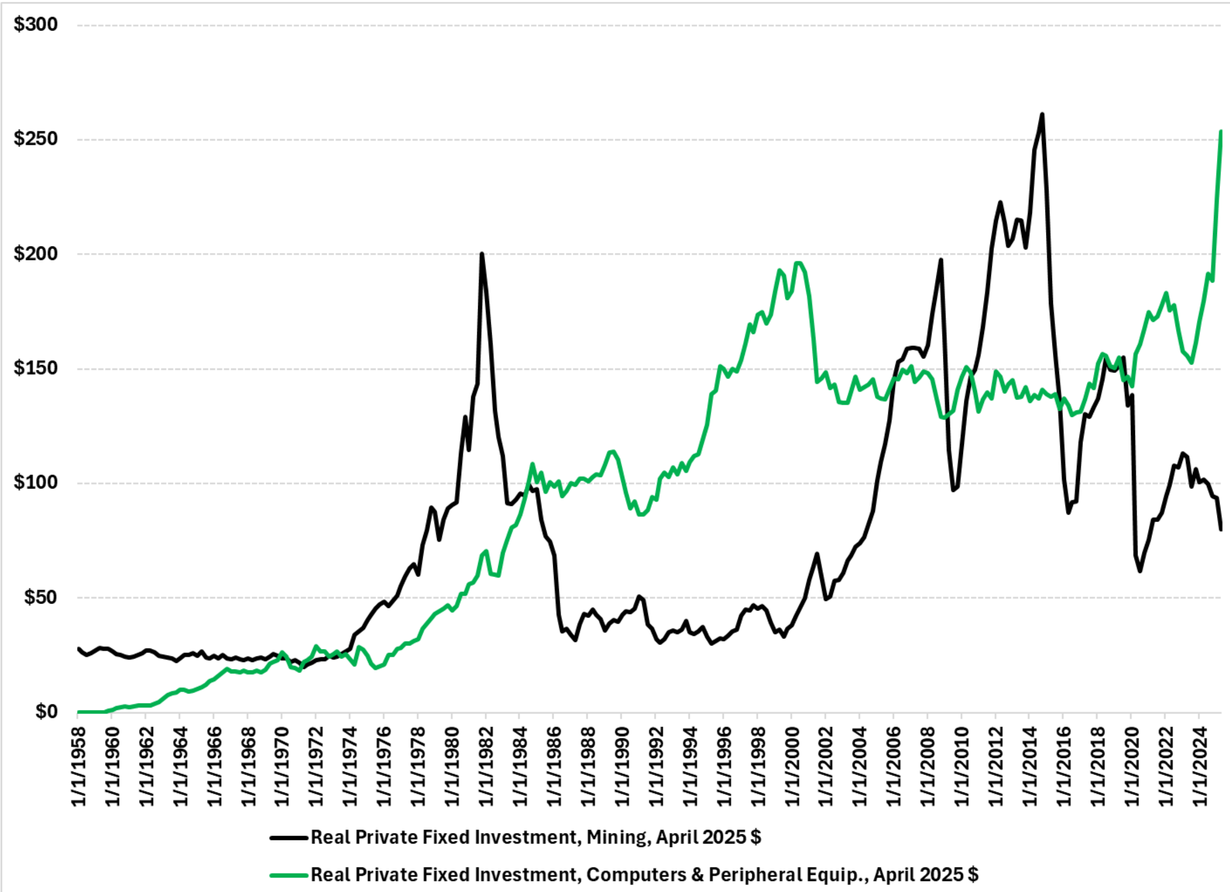
Hyperscale-AI Computing Is a Critical Emerging US-China Competition Space

From an American perspective, the competitive stakes are extraordinarily greater in the AI computing space than they were in 5G telecoms because computing capability breakthroughs substantially transcend political boundaries in a way that networking ones may not. Computing at hyperscale of the sort needed to advance AI research and development is dominated by a small number of corporations largely in the United States.

The high-performance computing needed for hyperscale-AI computing is dominated by the largest global digital infrastructure providers — which predominantly hail either from the United States or the People's Republic of China.[12]

Hyperscale data centers are to AI what aircraft manufacturing plants plus airports are to aviation: the centers of literal physical production and the hubs through which inputs and outputs are routed. Both are incredible strategic assets. The amount of capital investment in digital infrastructure assets is unprecedented and is unfolding at an incredible pace which substantially exceeds even the capital deployment rate during the peak of the U.S. oil & gas shale boom.

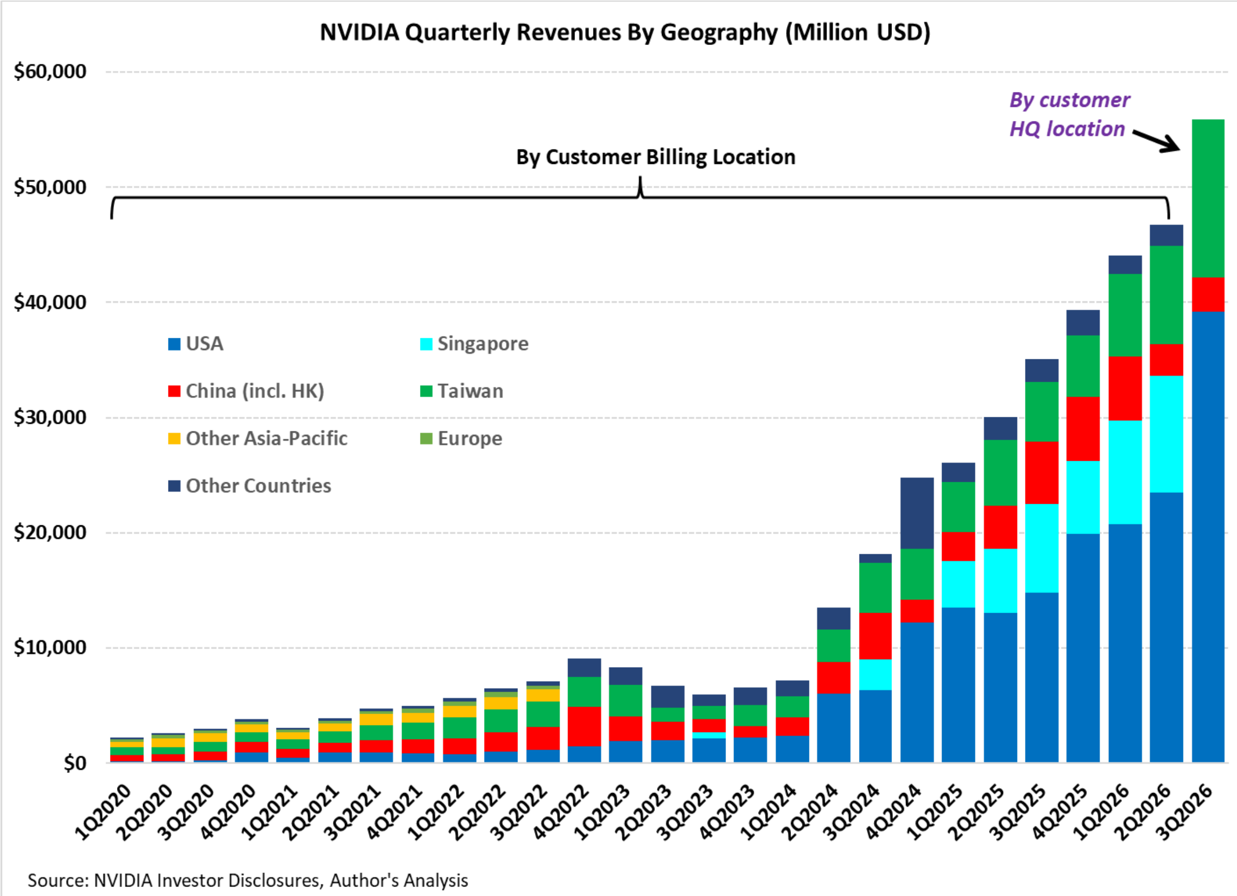
Figure 2 — Capital Investment in US Mining (Dominated by Oil & Gas) and IT, 1958–2025



Source: U.S. Bureau of Economic Analysis, Private fixed investment: Nonresidential: Information processing equipment and software: Computers and peripheral equipment [B935RC1Q027SBEA], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/B935RC1Q027SBEA. U.S. Bureau of Economic Analysis, Private fixed investment: Nonresidential: Structures: Mining exploration, shafts, and wells [E318RC1Q027SBEA], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/E318RC1Q027SBEA.
Note: Seasonally adjusted average rate. Inflation-adjusted to Billion April 2025 $.

Graphics processing units made by NVIDIA remain the prime mover of global AI compute and the past two years' quarterly sales data reflect the global competition between China and the U.S. Customers whose billing location (a loose proxy for headquarters) is in the U.S. account for about half of NVDIA sales, firms in Taiwan for 18%, entities in Singapore for 22%, and companies in China for 6% (Figure 3).

Figure 3 — NVIDIA Semiconductor Sales Locations Reflect US-China Tech Competition



Source: NVIDIA Financial Reports, Author's Analysis

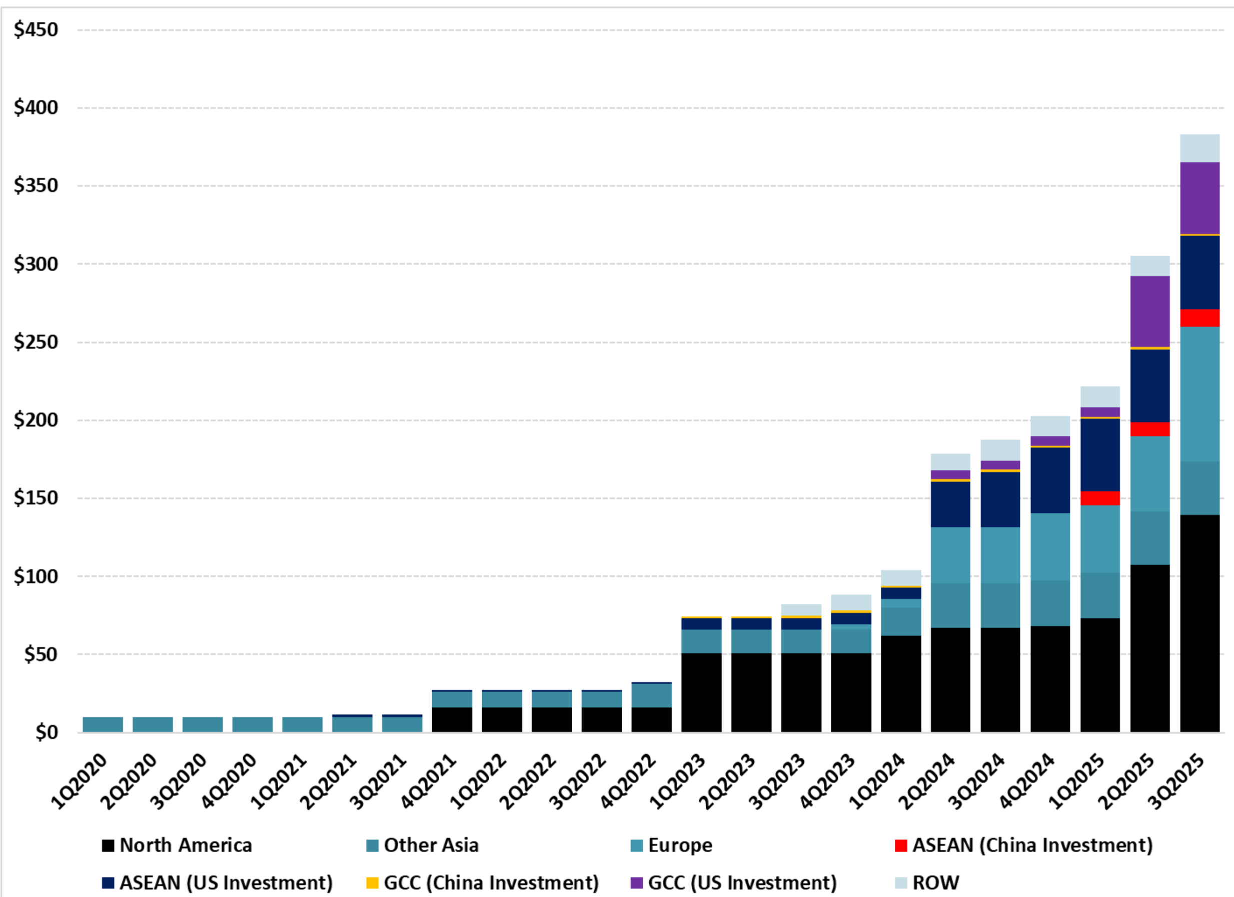
The billing location data are important because while U.S. hyperscalers are buying chips for deployments in datacenters all around the world (led by the U.S. domestic market but sited throughout Asia and Europe as well), the buyers from other places are typically more likely to deploy chips in the place of billing (China, Japan, Europe), or near it (Singapore). It is also worth noting that as of its Fiscal 2026 quarter (ending on 27 October 2025), NVIDIA began reporting sales by location of customer headquarters.

This change saw the China/HK share remain similar to the prior quarter but the U.S. share rose substantially, suggesting that U.S. firms are among the key datacenter builders and physical chip suppliers for datacenter buildouts in multiple locations abroad, including Southeast Asia. Of special note, the disappearance of a separate Singapore geographic report easily fit within the upswing in sales attributed to US-based firms and based on deviation from the simple numerical pattern of prior quarters' sales, may have in fact driven much of the departure from trend.

Singapore stood out under the prior reporting structure because nearby Malaysia has seen an explosion of datacenter capacity in recent years, including higher-end AI computing capabilities sought by Chinese customers who are restricted from importing cutting-edge chips with American content into China. As one local investor told the South China Morning Post in April 2025, "*Chinese companies are the primary clients of data centres in Malaysia and other South-east Asian areas*."[13]

Chinese entities coming "over the wires" to access compute abroad is the key concern that underpins U.S. and PRC positioning with regard to the two most intense zones of frontier compute competition globally: the Persian Gulf Countries and the ASEAN Region in Southeast Asia. These are not the biggest markets for US AI computing providers (Figure 4). They are, however, the ones in which China has the highest capacity to contest American digital infrastructure presence and where, absent safeguards, PRC entities have the best opportunities to clandestinely access world leading American-linked computing power for training AI models. U.S. firm lead the investment race now but as Chinese fabs improve chip quality, particularly for AI inference workloads, the advantage could rapidly narrow.

Figure 4 — Major AI Computing/Datacenter Investments Announced by U.S. and China-Based Hyperscalers Since 2020, Billion USD (Cumulative)



Source: Company Reports, Data Center Knowledge, Datacenter Dynamics, Reuters, WSJ, Local Media, Author's Analysis.

Concerns about Chinese companies attaining "backdoor access" to powerful computing clusters using U.S.-linked chips spiked after a Chinese developer released the DeepSeek chatbot in 2025. Regardless of how and where DeepSeek was specifically trained, it raised questions about the fungibility of computing power. AI model training attracts special concerns because a company that might not be able to import high-end GPU chips into China could still train its models in data centers located abroad, if the operators had the topline chips but more lax "know your customer" requirements than an operator based in the U.S., Europe, Korea, Japan, or Taiwan might.

US concerns about Chinese entities' potential backdoor access to high-end computing power reached a crescendo during the Biden Administration, culminating in the January 2025 promulgation of the so-called AI Diffusion Rule. The rule would have severely restricted US-linked firms' ability to provide cutting edge semiconductors to customers in most parts of the world.[14]

It would also have required datacenter companies based on the US to maintain at least 50% of their computing capacity within the US and no more than 25% outside of what were classified as "Tier 1" countries (Australia, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Italy, Japan, the Netherlands, New Zealand, Norway, Republic of Korea, Spain, Sweden, Taiwan, and the United Kingdom).[15]

It aimed to ensure that *"…the world's AI runs on American rails*" and to reduce the risk that competing AI training centers would emerge in areas with plentiful energy and capital, but less commitment to excluding malign actors from frontier AI training infrastructure.[16] American hyperscalers were assumed to have more robust security protocols and if that failed, lie clearly within US law enforcement jurisdiction. The rule is moot now, as the Trump Administration rescinded it in May 2025 before it took effect but its parameters illuminate core strategic motivations for US policies aimed at ensuring continuing AI supremacy.

To retain and expand its leadership in AI requires industrial policy that addresses failures to develop or retain critical industries that have moved abroad from the United States for decades. If an arms race is afoot in the construction of revolutionary AI technologies, then the threat of a strategic failure in that space would have serious consequences for American economic vitality and the power that is derived from it. While US political leaders on both sides of the aisle were unhappy with purchases of Huawei and ZTE 5G telecommunications hardware by traditional US allies, the reality was that no US firm was offering competitive alternatives. American diplomats and military officials instead encouraged allies to purchase specialized gear from firms in Sweden and Finland.

Digital Infrastructure is Key Geoeconomic Terrain

Among areas where the U.S. can offer credible alternatives to Chinese infrastructure — or preclude it almost entirely — AI hyperscale compute stands out. The stakes are enormously high.[17] Former Google CEO and Chairman Eric Schmidt explains, "*Faster airplanes did not help build faster airplanes, but faster computers will help build faster computers*."[18] At the frontier of the discipline, compute demands for training frontier AI models continue to multiply each year. At the same time, China enjoys an asymmetric domestic electricity advantage relative to the U.S because of its larger grid, present structural underuse, and ability to build generation and transmission much faster than American utilities can.

As such, being able to add computing capacity globally can help offset slow U.S. power generation and transmission expansions and thus help retain competitive AI edge vis-a-vis China.] Ensuring that as much of the global AI system as possible runs on rails outside the PRC is also an abiding U.S. national interest that motivates a desire to minimize its presence in cloud computing ecosystems outside of China and its key allies.

Data Centers Are the Airports of the AI Age: Control Matters

The "data centers-airports" analogy finds meaning in the history of great power competition as powerful nation states competed to control critical geoeconomic terrain and exclude adversaries from those positions.[19] In the early days of World War II, Washington sought to extirpate German and Italian ownership of airlines in Latin America. Multiple geoeconomic tools were brought to bear on the problem sought.

In the case of Bolivia, US authorities worked over a period of approximately 9 months in 1941 to: (1) help the Bolivian government nationalize the German-founded L.A.B. airline with a stock buyout at fair market price to eliminate German equity ownership[20], (2) replace German management, (3) have Panagra [a Pan-American Airlines subsidiary] take over routes, and (4) provide financing for Bolivia to purchase additional aircraft and expand ground facilities.[21]

The US took broadly similar steps in Argentina, Brazil, and Colombia–where a delicate dance was required given that Pan Am Airlines secretly held a controlling interest in *Sociedad Colombo-Alemana de Transportes Aéreos* (SCADTA).[22] Digital infrastructure competition between the U.S. and China at this point has not yet entailed displacement of owners from assets but nonetheless features intense competition as hyperscalers from each country chase growth in key markets. The best way to minimize the competitive threat from China-origin AI systems is to ensure that U.S. and allied country firms dominate the compute infrastructure. This means leveraging programs like OpenAI for Countries and doing so in a way that supports a diverse ecosystem of vetted, U.S.-aligned hyperscale options for meeting rapidly growing global demand for AI compute.

In addition, keeping the U.S.-origin AI training compute as inaccessible as possible to PRC firms gives U.S. and allied country developers a competitive advantage. DeepSeek revealed that the phenomenon of "Chinese engineered AI models trained on U.S. chips" is a real risk and that tighter control of compute hardware is essential. Furthermore, U.S. policy should seek to keep PRC hyperscalers at a disadvantage in contested spaces like ASEAN and the GCC while also embracing vetted Chinese AI researchers and developers who want to work and contribute to the U.S.-aligned ecosystem. It's much better to welcome them in Silicon Valley than to force them to Hangzhou. AI hardware is an area of singular U.S. advantage that should be maintained as part of a global "secure grids, secure hyperscale-AI computing" strategic policy.

Key US-China Cloud Computing Competition Zones

Gulf Region AI computing development is focused in two countries: Saudi Arabia and the UAE. Both countries are energy-rich, well-capitalized, and ambitious middle powers who are working to navigate an increasingly intense US-China digital infrastructure competition. At the moment, they are hedging their digital infrastructure bets. In 2021, *Intelligence Online* reported that the G42 Group, the UAE's AI national champion, was developing its applications on cloud infrastructure provided by Huawei.[23] Saudi Arabia, meanwhile, granted Huawei a Class C license for providing cloud services, meaning that the company could even store the kingdom's top secret-level information.[24]

More recently, the tide appears have turned back toward the U.S., especially for the highest end AI. For instance, Google Cloud has committed to a $10 billion partnership with Saudi Arabia's Public Investment Fund to build cloud infrastructure and AI services in Saudi Arabia.[25] While neither party discloses the datacenter capacity, Google pledged to build in the Kingdom what we estimate to be between 400 MW and roughly a gigawatt of AI computing capacity. This is not a big number from the perspective of the U.S. domestic datacenter buildout, but it would be transformative for Saudi AI ambitions while also keeping the country's AI ecosystem "running on American rails."

In the UAE, the country's leadership has also tacked back towards the U.S., with OpenAI announcing in May 2025 that it would be partnering with G42 as well as Oracle, NVIDIA, Cisco, and Softbank to build a 1-gigawatt AI compute cluster in Abu Dhabi.[26] OpenAI expects the first 200 MW of the complex to come online in 2026.[27] Both the Saudi and UAE examples reflect a clear evolution toward deploying corporate power backed by diplomatic capital to rope allies and partners into a broadly American AI umbrella with multiple potential corporate partners inside the ecosystem, be they Google, Microsoft, OpenAI, Oracle, etc.

Indeed, the "OpenAI for Countries" framework released by the ChatGPT operator in May 2025 lays out a 5-part structure centered on: (1) building American-backed domestic AI computing capabilities, (2) providing AI applications (like ChatGPT) customized for local markets, (3) cooperation on safety and security controls for AI tools, (4) creation of national start-up funds, and (5) encouraging partner countries to invest in OpenAI's global Stargate Project.[28] While OpenAI's plan hews to its specific corporate interests, other partnerships between U.S. AI infrastructure firms and foreign entities are likely to feature similar parameters.

The New Seven Sisters: Hyperscalers as Strategic Actors

The emerging global power of the U.S. hyperscalers in the current AI boom suggests they are rapidly on course to create something roughly akin to the Seven Sisters' reign over the global oil industry from 1928 through the early 1970s. For reference, the Seven Sisters were: Standard Oil of New Jersey, Royal Dutch Shell, Anglo Persian Oil Company, Standard Oil of New York, Standard Oil of California, Gulf Oil and Texaco.[29] This corporate constellation controlled the bulk of the world's oil production, transportation, and refining capacity for the first seven or so decades of the Oil Age.[30]

Much like the original Seven Sisters depended on access to oil wells, the new Digital Seven Sisters depend on access to secure, uninterrupted gigawatt-scale power. But the hyperscalers' position could become even more powerful and harder to dislodge. As oil companies, the Seven Sisters were commercial guests in the countries that held the largest global reserves — like Kuwait, Iran, Iraq, Saudi Arabia, and the UAE. As the early 1970s OPEC revolution showed, the oil majors could be kicked out and replaced with national producers.[31]

The U.S. tech ecosystem, combining world-class chip expertise, eminently capable hyperscale datacenter operators, an ample software development labor force and deep capital markets is much more deeply embedded because it controls the core supply-side resources — foremost among them, the chips that power AI training and operation. The only plausible exceptions would be (1) if PRC companies developed homegrown AI chips competitive with American ones or (2) if China conquered Taiwan and U.S. firms lost unfettered access to chips from TSMC fabs on the island.[32]

ASEAN countries do not have the same energy availability or the deep pockets of Gulf oil exporters. What they do have is a high level of cultural, economic, and physical proximity to China while also being key US partners and a prime global destination for American investment. Furthermore, they themselves are large digital markets, with a collective ASEAN regional population roughly the size of Europe's. Finally, they do not have national AI champions equivalent to the UAE's G42. In the GCC countries, the 10 largest datacenter operators control about 2/3 of operational datacenter locations at present. In contrast, the 10 largest operators in the ASEAN region only control about 30% of currently operational locations. The ASEAN datacenter ecosystem offers ample opportunity for PRC entities to slip in as joint venture partners or via other minority interest structures where they are not the name on the facility but could plausibly have preferred access to computing power.

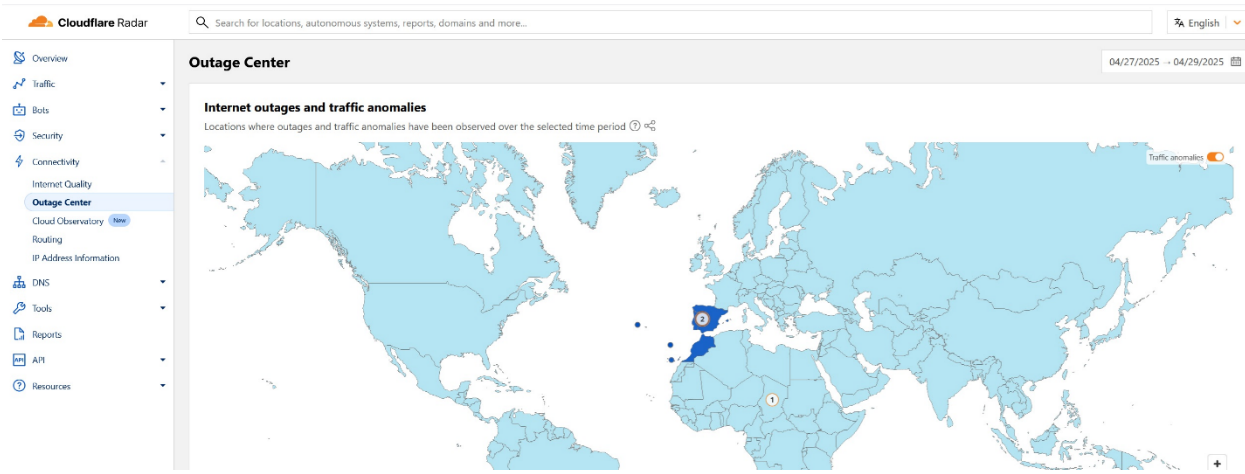
The only companies currently executing projects at this scale with cutting-edge chips or that will be able to do so for years to come are those run by, or at least intimately involving U.S. hyperscalers. With the U.S. government's increasing and bipartisan attention to the AI race, it is highly likely that these firms will maintain stricter know your customer policies than non-U.S., non-treaty ally country firms would. U.S. hyperscalers long-term commercial interests are more aligned with the national interest of restricting Chinese firms' access to high-power AI model training capabilities.

The Grid-Cloud Nexus: Digital Competition Meets Energy Competition

Beijing and Washington are now engaged in an existential competition for global pre-eminence. Electricity is a critical vector in that struggle because it underpins basic functions in modern life — provision of water, heating, cooling, lighting — and also is a critical input for the global AI competition.[33] In areas currently lacking sufficient electricity, the smaller kilowatt and megawatt applications will likely see energy be delivered in "island" form. Imagine the rural village in Africa installing solar panels plus batteries to power water wells, refrigeration, and other basic services.[34] But the combination of human need, industrialization, and AI compute deployments collectively require gigawatts of power for smaller countries, tens to hundreds of gigawatts for medium powers, and terawatts for the biggest economies.

Under these conditions, larger power grids will be very important and commensurately vulnerable. If a small, isolated grid fails, a small number of homes and/or businesses suffer outages. When a large grid fails, millions of customers can lose power rapidly — as happened in the Iberian Peninsula in April 2025. Homes, factories, transportation, and internet service are all lost and billions of dollars in damage accrue within minutes and hours (Exhibit 5).[35] Backup generators helped maintain basic cloud services for the roughly 12-hour event but users reported latency and access issues.[36] For anyone using cloud-based AI, the loss or significant degradation of Internet service isolates datacenters leaving customers adrift. In an industry where "uptime" is everything, resilience and redundancy are far more than nice to have.

Figure 5 — 28 April 2025 Blackout Broke the Internet in Spain



Source: Cloudflare.

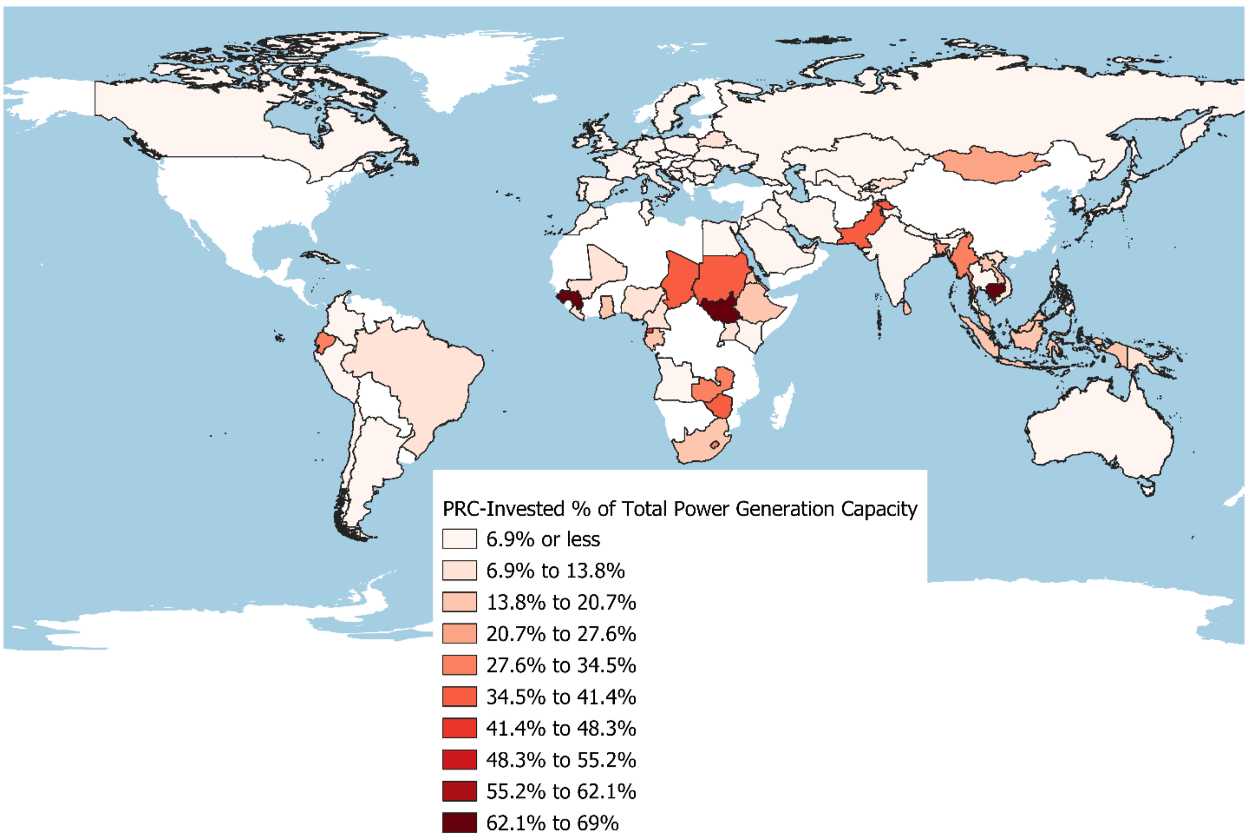
Access to electric power is a fundamental need of cloud and hyperscale operators. To maintain security of electricity supplies involves multiple activities: (1) electricity generation, (2) bulk power transmission, (3) local power distribution, and (4) power management by customers. Each of these segments is subject to potential security risks including from cyber and kinetic action directed against them.[37] The most consequential of these is the generation and bulk transmission of electricity.

In electricity generation, a single digit (smaller countries) or double to low-triple digit number of generators (larger countries) produce a material portion of national electricity output. In the bulk power segment, a similar number of large transformers play a similarly important role, and as seen during the Ukraine War, loss of even a few key large transformers can destabilize a power grid and black key customers out potentially for days. Those attacks have shown repeatedly the enormous vulnerability of electricity production and distribution nodes.

As a major producer of power generation and distribution technologies, Chinese firms have been leaning into the global electrification wave, particularly in Belt and Road countries but beyond them as well. PRC-domiciled companies have invested across the electricity supply chain in multiple markets around the world, spanning generation, bulk transmission, and distribution to end users.[38] PRC entities' have so far built or bankrolled 745 power generation facilities worldwide with roughly 177 gigawatts of combined capacity.[39] Investments come from owner/operators like the PRC grid companies as well as bank financing for projects constructed by (predominantly) PRC-based firms.

Chinese-built power plants now are operating 96 countries. The ones with the largest share of PRC-invested/funded generation capacity are Cambodia (66% of the national total installed base), Pakistan (40%), Sudan (38%), Ecuador (30%), Zambia (30%), and Myanmar (29%). PRC companies also own significant stakes in power grid operators that collectively serve millions of customers in countries including Australia, Brazil, Greece, Italy, Laos, Peru, the Philippines, Portugal, and Oman (Figure 6). Several of these countries are U.S. treaty allies.

Figure 6 — Key PRC-Invested Generation Assets Abroad



Source: Boston University, Media Reports, State Grid Corporation, World Nuclear Association.

China-based entities also have attained presence in multiple national power grids around the world. In some instances, this is a product of being an equipment provider. The U.S. market would be one example, where high voltage transformers, grid-scale solar inverters, and PRC-origin grid scale storage batteries have all crept into the bulk power system over the past 15 years.[40] In other cases, Chinese presence comes through purchasing equity ownership stakes in electricity grid operators. For instance, in December 2007, China State Grid Corporation's international subsidiary purchased a 40% stake in National Grid Corporation of the Philippines (NGCP) and obtained a 25-year operating concession that effectively puts it in charge of the country's grid.[41]

Between 2010 and 2021, State Grid Corporation's international subsidiary invested more than USD 12 billion in Brazil's power grid, obtaining substantial ownership interests in 20 transmission asset operators, including the world's longest ultra-high voltage direct current powerline linking the Belo Monte Hydropower project with Rio de Janiero and other key demand centers in southeastern Brazil.[42]

China Yangtze Power purchased a controlling interest in Peru's Luz de Sur electric utility from San Diego-based Sempra Energy in 2019, which among other things, conferred management of nearly 30% of Peru's electricity transmission system.[43] This transaction was notable because it was part of Sempra's approximately USD 5 billion divestment of its electricity supply assets in Chile and Peru, which State Grid International and China Yangtze Power, respectively purchased.[44] Finally, in 2021, China Southern Grid reportedly acquired a 25-year concession to operate Laos's primary electricity transmission system, Électricité du Laos Transmission Company Ltd.[45]

On the electricity consumption side, Chinese companies are also collectively the world's largest manufacturers of smart meters for measuring electricity usage in homes and businesses. These units typically have remote access capabilities and, in many cases, can detect detailed power use characteristics in real time.[46] The breadth of their units' distribution throughout multiple national electricity marketplaces plus the depth of their data collection capabilities — and the fact that their manufacturers are subject to China's 2017 National Security Law and its data sharing requirements — raise distinct security implications.[47] These are discussed in the subsequent section.

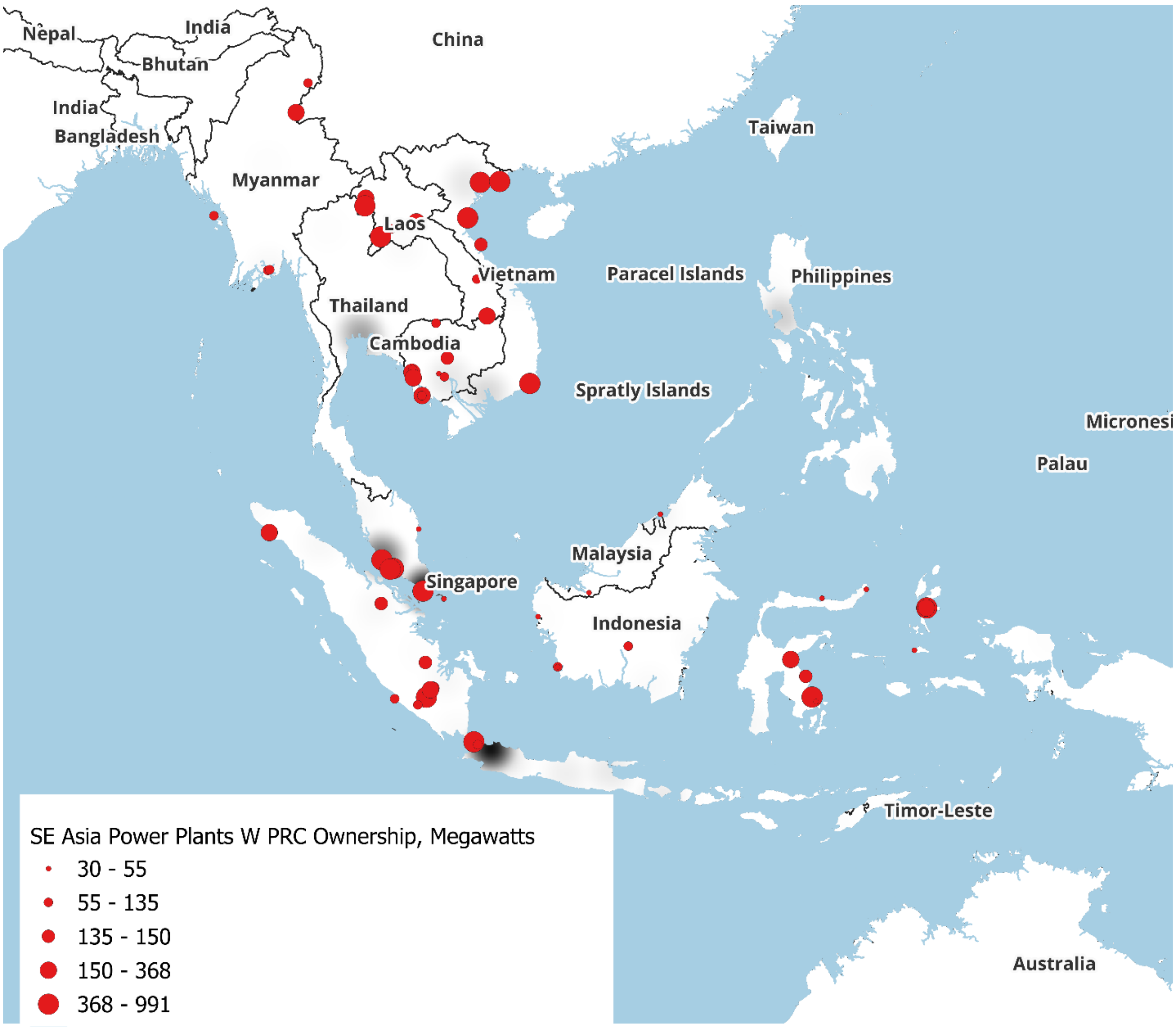
The Cloud-Grid Nexus: Southeast Asia Case Study

PRC entities' presence in bulk power systems around the world raises the question: "*what does PRC-linked power generation and transmission presence look like in the key contested cloud computing zone of Southeast Asia?*" Southeast Asia's emerging datacenter hotspots are: (1) the Johor area in southern peninsular Malaysia, (2) the Jakarta area, (3) Singapore, (4) the Bangkok area in Thailand, and (5) the Kuala Lumpur area, again in Malaysia. Of these, Johor, Jakarta, and Bangkok stand out for investment already announced and likely to come. Consider the growth in data center electricity loads in Johor. Local scholars estimate that datacenters in the Johor area used 10 megawatts of electricity in early 2021, growing to 1,300 MW by November 2024, and projected to reach 2,700 MW by 2027.[48]

To assess the competitive challenge, we took comprehensive data from *Global Energy Monitor* to locate every operational grid-scale power plant in the ASEAN countries, sorted the data manually to identify power plants that were majority or minority owned by PRC-linked entities, and then cross-checked the manual search with deep AI searches using ChatGPT-5 and Gemini 3 Pro to ensure that we did not miss potential linkages during our manual sorting. This process identified 147 power plants with an aggregate capacity of approximately 34 GW (Figure 7).

Figure 7 – China-Linked Power Plants in SE Asia vs. Datacenter Hotspots

Note: the black heatmap shading for datacenter concentration areas is based on the number of datacenters rather than their IT capacity in MW because our dataset does not yet have sufficient fidelity to be charted in a representative way. We are working to close that gap but, in the meantime, believe that the raw number of facilities in an area still provides a valid directional indicator as to its importance as a computing hub.



Source: Datacenter Map, GADM, Global Energy Monitor, Authors' Analysis.

Nearly half of this capacity is in Indonesia, with a material portion of it consisting of coal plants powering nickel smelters. Malaysia hosts much less — approximately 4 GW — none of which is in Johor but of which a bit over 80% resides in the adjacent Malacca province. Thailand did not have any PRC-owned power plants within its borders. That said, it bears noting that Thailand in some months now imports nearly a quarter of its electricity in the form of hydropower from Laos, which is generated and transmitted using a heavily China-linked power plant and grid system.[49]

The disposition of PRC-owned and invested power generation assets near Southeast Asian computing hubs versus the region's datacenter capacity growth trends creates an interesting and time sensitive geoeconomic opportunity for the United States and its partners, particularly Japan, South Korea, Germany, and France. We call it the "*Datacenters and Dynamos Package: Export Financing for Integrated Compute and Generation Assets*."

The U.S. EXIM Bank and its German, Japanese and Korean counterparts, U.S. hyperscalers, and electricity generation equipment vendors and builders from all five countries, are well-positioned to fund export packages that combine datacenter expansions with power generation investments. Such packages will likely need to restrict PRC entities' ownership. Passive minority ownership interests of vetted PRC entities could potentially be acceptable but would need to verifiably prevent access to operational data or influence over decision-making, service vendor selection, and other such important functions that could offer a malign actor access. The power plants do not necessarily have to be co-located with datacenters but having them on the same grid circuits helps alleviate local concerns about energy shortages, bolsters security of AI compute, and builds a cloud-grid ecosystem that runs on allied rails, as opposed to PRC-linked ones.

Malaysia and Thailand would be the highest priority countries given the coming growth in datacenter capacity and the fact that Chinese entities' penetration in their grids and generation bases is lower than in Indonesia. Indonesia and the Philippines would also be high strategic priorities from the perspective of facilitating energy abundance, particularly via US LNG, and advanced nuclear equipment, but with the knowledge that Chinese firms' already have a significant presence in the Indonesia generation asset base and the Filipino grid might require a different economic and political approach since immediately moving to sideline PRC actors could stimulate local opposition or trigger other destabilizing outcomes.

Pursuing an integrated "secure cloud, secure grid" strategy will require substantial diplomatic, financial, and political investment. But the alternative is to risk repeating what happened in 5G where Western refusal or inability to engage in geoeconomic campaigns to offer credible alternatives created a system that at worse runs entirely on Chinese rails in many countries or else, like Mexico, runs on hybrid rails that trade cheaper upfront capital cost for data insecurity.

China-Origin Hardware and Data Insecurity

Links to the PRC in the electricity sector merit scrutiny for several reasons. First, key power system equipment often naturally incorporates remote access capabilities so manufacturers can keep systems running from afar. This is fine under "normal" conditions but can become problematic if the manufacturer can be coerced into either turning systems off for national, rather than corporate reasons or else collecting and sharing data on power flows and customers in an unauthorized manner. These concerns arise with PRC-domiciled entities and their subsidiaries because they are subject to the PRC 2017 National Security Law, which requires them to cooperate with PRC government agencies upon demand and further, prevents them from notifying anyone else of this cooperation.

Second (and related), software and hardware characteristics could create persistent access points for an adversary that can be very difficult to patch (software) to virtually impossible (hardware). Power plants and bulk power system equipment are potentially vulnerable to physical and cyber sabotage or interference regardless of the equipment maker's national origin.[50] But not a trivial concern are "kill switch" backdoors in Chinese manufactured technologies. In early 2025, investigators found undocumented cellular radios in China-origin solar inverters and grid batteries shipped to the U.S.[51] The discovery is important because utilities typically install firewalls to prevent China-made equipment from "phoning home" but the rogue radios/communication devices could allow the Chinese manufacturer (or China's intelligence services) to bypass the firewall and remotely manipulate the device.

Indeed, at least one assessment published by well-regarded industrial control systems experts noted that attacks based on embedded vulnerabilities are less of a concern than remotely orchestrated cyber operations.[52] Actual destructive actions carried out in controlled environments (2007 Aurora test at Idaho National Laboratory where malicious code was used to remotely destroy a diesel generator) and in the wild (2016 Win32/Industroyer attack on the Ukrainian electricity system) both affirm the dangers of malware implanted and activated remotely.[53]

But if a "backdoor" vulnerability is built and programmed into the physical system, things are far worse because an adversary can more easily covertly exploit access points, do so with a high degree of plausible deniability given the legitimate uses of remote access and updates, and because the only "fix" is a "rip and replace" that is likely to be cost-prohibitive in many cases. China-related hardware risks have been a persistent theme in the tech world.[54]

The examples to date are from general computing but they highlight similar risks that could play out for AI and power grid hardware to the extent that PRC entities are involved in supply chains. Bloomberg has now twice reported on potential tampering with computer server motherboards manufactured in China, offering detailed accounts that, while not 100% probative, suggest that hardware risks are real and significant.[55] Furthermore, a Marine Corps networking systems engineer testified under oath in a 2010 Federal court case that "*A large amount of Lenovo laptops were sold to the US military that had a chip encrypted on the motherboard that would record all the data that was being inputted into that laptop and send it back to China*."[56] Viewed together, the previous sources' plausible suggestion that nefarious actors could covertly penetrate supposedly secure hardware supply chains raise valid concerns about the integrity of power grid hardware assembled in China.

For downstream segments of the power grid, China-origin hardware components also pose clear and meaningful security challenges. Smart meters offer a useful example. More sophisticated versions can collect high fidelity measurements of electricity usage in homes and businesses. Chinese academic researchers have focused on meter-level electricity data as a social policing tool.[57]

The level of practical application and investment in research suggest that remote surveillance capabilities originally developed for use within China could be deployed to collect information from smart meters deployed outside China as well. Users should assume that in PRC-origin tech hardware, backdoors are a feature, not a bug. Indeed, Chinese original equipment manufacturers are subject to the 2017 National Intelligence Law and would be legally compelled to provide customer data to Chinese government actors such as intelligence agencies if they requested it.

PRC intelligence agencies would have strong incentives to seek such information. Granular electricity usage data would offer unique insight into life patterns that provide insights and warning regarding fluctuations in facility activity such as deployments. Now imagine if such address-specific data were integrated in an AI-enabled system with other information, such as public records, social media posts, cell phone locations, and other more easily obtainable datasets. The intelligence and warning value to PRC policymakers would be significant.

If the scenarios described above seem far-fetched, consider how China uses detailed data from smart meters in its own domestic context. Security personnel in western China's Xinjiang province have for nearly 10 years utilized a surveillance system known as the Integrated Joint Operations Platform (一体化联合作战平台) that fuses vast amounts of data to facilitate predictive policing and repression actions.[58] Detailed electricity usage data enables some of the most intrusive insights into a surveillance subject's daily life. Did your household electricity usage rise over the past week? The Public Security Bureau will likely visit your home for an "inspection." Did your smart meter data suggest that you might have used a power saw that can cut metal or an arc welder that you can build with? Expect a visit from the Public Security Bureau.

Global AI and the Electrons Powering It Should Run on Non-China Rails

Hyperscale-artificial intelligence infrastructure fundamentally depends on the electricity systems that power it. No matter how advanced U.S. or allied semiconductors, software, and model architectures become, datacenters' operational value hinges on the integrity of the grids and power plants feeding them. Recent revelations of ostensibly Chinese operations to compromise U.S. electricity producers and distributers, both great and small, provide ample warning that cyber defenses are seriously lacking in the sector. Unfortunately, where the buck stops for deployment of adequate defenses remains ambiguous at best.[59]

A PRC-owned generation asset able to curtail output at strategically opportune moments, or power-electronics equipment whose firmware can be manipulated remotely creates structural vulnerabilities that can take billions of dollars of investment in high performance computing offline or else render it uncompetitive because of unreliability concerns. Accordingly, electricity grids, high-voltage transformers, inverters, substation automation gear, and grid-scale storage are now arguably as integral to informational dominance as fabs or model-training pipelines. Adversaries that can penetrate, influence, or selectively degrade these assets gain coercive power over the consumers and countries that rely on them.

The United States and its allies lead in advanced logic chips, GPU architecture, foundational models, and hyperscale cloud. China, by contrast, commands global shares in high-voltage transformers, power-electronics inverters, and certain grid-automation equipment, backed by state financing and vertically integrated industrial capacity. These asymmetries mean that the contest over AI infrastructure will not play out solely in compute supply chains, but across the full stack of electrical hardware that determines compute reliability.

Given that the emerging competition is global, a rational U.S. and allied strategy must geographically prioritize to prevent dispersed efforts from diluting national objectives. Not every grid, data-center market, or host country matters equally for global AI security. Policymakers should identify the jurisdictions where future AI training and inference capacity is most likely to concentrate, assess the degree of PRC hardware penetration in those electricity systems, and then deploy resources accordingly — development finance, supply-chain security measures, alternative equipment subsidies, investment screening, and joint energy-infrastructure projects.

This paper offers a starting blueprint for managing and winning the multi-decade global AI and electricity competition now underway: defining the compute–power nexus as a unified security domain; mapping risk channels created by foreign control, equipment dependence, and cyber-physical access; and outlining criteria for selecting priority theaters for competition.

Notes

[1] Gabriel Collins is the Water-Energy Thrust Leader at Rice University's Water Institute and holds a membership interest in Cactus Water Services, LLC. This relationship is covered by a Rice University conflict of interest management and monitoring plan. He is the Baker Botts Fellow in Energy & Environmental Regulatory Affairs at the Center for Energy Studies, Rice University's Baker Institute for Public Policy. He heads the CES Program on Energy & Geopolitics in Eurasia and is also an Energy-Water Thrust Leader at Rice University's Water Institute.
[2] Christopher Bronk is a cyber expert who is a Professor at the University of Houston's Hobby School of Public Affairs and a Non-Resident Scholar at the Baker Institute.
[3] Gilding, Simeon. "5G Choices: A Pivotal Moment in World Affairs." The Strategist (Australian Strategic Policy Institute), January 29, 2020. https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/.
[4] Bronk, Chris. "Information Power!: Tracking Computing's Collision with Global Politics." Communications of the ACM 68, no. 11 (November 2025). https://doi.org/10.1145/3771377.
[5] See, for instance: U.S. Senate Select Committee on Intelligence. Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media, with Additional Views. 116th Congress, 1st Session, Senate Report 116-XX. Washington, D.C.: U.S. Government Publishing, 2019. https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf.
[6] Cox, Joseph. "Amazon Shuts Down NSO Group Infrastructure." Vice, July 19, 2021. https://www.vice.com/en/article/amazon-aws-shuts-down-nso-group-infrastructure/
[7] Lee, Doowan, and Shannon Brandao. "Huawei Is Still Too Big to Fail — and That's a Major Risk to the World." Foreign Policy, April 30, 2021. https://foreignpolicy.com/2021/04/30/huawei-china-business-risk/.
[8] D'Sola Alvarado, Parsifal. Huawei's Expansion in Latin America and the Caribbean: Views from the Region. Special Report No. 529, April 2024. Washington, DC: United States Institute of Peace. https://www.usip.org/sites/default/files/2024-04/sr-529_huaweis-expansion-latin-america-caribbean-views-region.pdf.
[9] Ghalia Kadir and Joan Tilouine, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin," Le Monde, January 26, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.
[10] Ibid.
[11] Leonard, Jenny, Julian Deutsch, and Kamil Kowalcze. "Germany Mulls Paying Deutsche Telekom to Replace Huawei Gear." Bloomberg. Republished on MSN Money. Accessed October 30, 2025. https://www.msn.com/en-us/money/companies/germany-weighs-paying-deutsche-telekom-to-replace-huawei-gear/ar-AA1PvMdl.
[12] Haag, Alex. "The State of AI Competition in Advanced Economies." FEDS Notes. Board of Governors of the Federal Reserve System, October 06, 2025. https://www.federalreserve.gov/econres/notes/feds-notes/the-state-of-ai-competition-in-advanced-economies-20251006.html.

[13] Malay Mail. “Chinese Companies Fuel Malaysia’s Data Centre Boom amid Rising AI Demand.” Malay Mail, April 3, 2025. https://www.malaymail.com/news/money/2025/04/03/chinese-companies-fuel-malaysias-data-centre-boom-amid-rising-ai-demand/171748.
[14] The White House. “FACT SHEET: Ensuring U.S. Security and Economic Strength in the Age of Artificial Intelligence.” January 13, 2025. Archived January 15, 2025. Internet Archive. https://web.archive.org/web/20250115010947/https://www.whitehouse.gov/briefing-room/statements-releases/2025/01/13/fact-sheet-ensuring-u-s-security-and-economic-strength-in-the-age-of-artificial-intelligence/. Original: https://www.whitehouse.gov/briefing-room/statements-releases/2025/01/13/fact-sheet-ensuring-u-s-security-and-economic-strength-in-the-age-of-artificial-intelligence/. Accessed October 15, 2025.
[15] Benj Edwards, “Biden Administration Puts Quotas on Global AI Chip Sales,” Ars Technica, January 13, 2025, https://arstechnica.com/ai/2025/01/biden-administration-puts-quotas-on-global-ai-chip-sales/ (accessed October 15, 2025).; Federal Register, “Framework for Artificial Intelligence Diffusion,” January 15, 2025, FR Doc. 2025–00636, https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion (accessed October 15, 2025).
[16] Tom Barrett and Johanna Lim, “The US AI Diffusion Rule: What Is It, Why Did the United States Rescind It, and Implications for Australia,” United States Studies Centre (Explainer), July 21, 2025, https://www.ussc.edu.au/the-us-ai-diffusion-rule.
[17] Gabriel Collins, “Could the Permian Basin Become America’s Next AI Data Hub?” Rice University’s Baker Institute for Public Policy, August 15, 2025, https://doi.org/10.25613/CDF1-4006.
[18] Ibid.
[19] Gabriel Collins and Michelle Michot Foss, “Critical Minerals and Materials Geoeconomics: Lessons and Ideas From Past Wars and Strategic Competitions,” Rice University’s Baker Institute for Public Policy, March 19, 2025, https://doi.org/10.25613/084W-XS50.
[20] https://history.state.gov/historicaldocuments/frus1941v06/d422.
[21] https://history.state.gov/historicaldocuments/frus1941v06/d421.
[22] Mark Cotta Vaz and John H. Hill, “Pan Am at War: How the Airline Secretly Helped America Fight World War II,” (85).
[23] Intelligence Online. “Abu Dhabi’s Spymaster Fashions Local Palantir 2.0 with Chinese Help.” Intelligence Online, January 27, 2021. https://www.intelligenceonline.com/government-intelligence/2021/01/27/abu-dhabi-s-spymaster-fashions-local-palantir-20-with-chinese-help,109638008-eve.
[24] Huawei Cloud, “Saudi Arabia Class C License,” Huawei Cloud Compliance Center, accessed October 15, 2025, https://www.huaweicloud.com/intl/en-us/securecenter/compliance/compliance-center/ksa-classc.html.
[25] Google Cloud. “Google Cloud and PIF Advance AI Hub in Saudi Arabia.” Press release, May 13, 2025. https://www.googlecloudpresscorner.com/2025-05-13-Google-Cloud-and-PIF-Advance-AI-Hub-in-Saudi-Arabia.
[26] OpenAI. “Introducing Stargate UAE.” News release, May 22 2025. https://openai.com/index/introducing-stargate-uae/.

[27] Ibid.
[28] OpenAI. "Introducing OpenAI for Countries." News release, May 7, 2025. https://openai.com/global-affairs/openai-for-countries/.
[29] Carola Hoyos, "The Evolution of the Seven Sisters," Financial Times, March 11, 2007. https://www.ft.com/content/2103f4da-cd8e-11db-839d-000b5df1062.
[30] Ibid.
[31] Carey, Jane Perry Clark. "Iran and Control of Its Oil Resources." *Political Science Quarterly* (1974): 147-174.
[32] Gabriel Collins and Andrew S. Erickson, "Could China Take Over Taiwan's Semiconductor Industry without Invading?" (Houston: Rice University's Baker Institute for Public Policy, September 27, 2023), https://doi.org/10.25613/D4ER-0D37; Andrew S. Erickson, Gabriel B. Collins, and Matt Pottinger, "The Taiwan Catastrophe: What America — and the World — Would Lose If China Took the Island," Foreign Affairs, 16 February 2024. https://www.foreignaffairs.com/united-states/taiwan-catastrophe.
[33] Collins, Gabriel. "America Should Lead the Fight Against Global Energy Poverty." Foreign Policy, March 20, 2025. https://foreignpolicy.com/2025/03/20/america-energy-poverty-china-power/.
[34] Ringler, Claudia, Abdulaziz M. Alqarawy, William Brent, Gabriel Collins, Paul Orengoh, Bridget Scanlon, and Lama Yaseen. 2020. Enhanced Water Security and Energy Access: Key Investments for Sub-Saharan Africa. T20 Saudi Arabia Policy Brief (Task Force 10: Sustainable Energy, Water, and Food Systems). https://www.global-solutions-initiative.org/wp-content/uploads/2025/03/T20_TF10_PB14.pdf.
[35] Twidale, Susanna, and Nina Chestney. "Explainer: What Caused the Iberian Power Outage and What Happens Next?" Reuters, June 18, 2025. https://www.reuters.com/business/energy/what-caused-iberian-power-outage-what-happens-next-2025-06-18/.
[36] Mendelson, James. "When the Lights Go Out: Lessons from the April 2025 Iberian Blackout." LinkedIn, May 6, 2025. https://www.linkedin.com/pulse/when-lights-go-out-lessons-from-april-2025-iberian-james-ln5ue.
[37] George, A. Shaji, T. Baskar, and P. Balaji Srikaanth. "Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors." *Partners Universal International Innovation Journal* 2, no. 1 (2024): 51-75.
[38] Kiryakova, Elena, Olena Borodyna, Rebecca Nadin, Lorraine Howe, and Yue Cao. *China's evolving role in Africa's energy transition: Overseas trade and investment in Kenya, Mozambique and South Africa*. ODI Global Report, 2025.
[39] Boston University Global Development Policy Center. 2025. China's Global Power Database. Retrieved from https://www.bu.edu/cgp/.
[40] "JSHP Transformer: News." JSHP Transformer. Accessed October 14, 2025. https://www.jshp.com/news.html; Craig Singleton, Beijing's Power Play: Safeguarding U.S. National Security in the Electric Vehicle and Battery Industries (October 23, 2023), Foundation for the Defense of Democracies, accessed October 14, 2025, https://www.fdd.org/wp-content/uploads/2023/10/fdd-memo-beijings-power-play.pdf.
[41]

http://www.stategrid.com.cn/html/sgiden/gb/CoreBusiness/OurInvestments/index.shtml#here.
[42] https://stategrid.com.br/en/home/actives/.

[43] https://www.luzdelsur.com.pe/uploads/shares/PDF/Memoria-Anual/2023/LdS_Memoria_anual_2022___1_.pdf.
[44] https://www.sempra.com/sempra-energy-announces-planned-sale-businesses-peru-and-chile.
[45] https://www.rfa.org/english/news/laos/grid-03162021152622.html.
[46] Holley. 2023. "Single Phase Electricity Smart Meter." Holley Metering. Accessed October 14, 2025. https://www.holleymetering.com/single-phase-electricity-smart-meter-product/.
[47] With or without CCP cells, PRC firms are universally subject to Article 7 of the 2017 PRC National Intelligence Law, which states in relevant part that "Any organization or citizen shall support, assist, and cooperate with state intelligence work in accordance with the law, and maintain the secrecy of all knowledge of state intelligence work." Remarks of NCSC Director William Evanina to International Legal Technology Association (ILTA) LegalSEC Summit 2019, 4 June 2019, https://www.dni.gov/files/NCSC/documents/news/20190606-NCSC-Remarks-ILTA-Summit_2019.pdf.
[48] Sara Loo, 2025/43 "Data Centres, Energy Demand and Sustainability: Can Malaysia Strike the Right Balance?" (ISEAS–Yusof Ishak Institute, June 3, 2025), https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2025-43-data-centres-energy-demand-and-sustainability-can-malaysia-strike-the-right-balance-by-sara-loo/.
[49] Energy Policy and Planning Office (EPPO), Ministry of Energy, Thailand, Electricity Statistic, accessed December 8, 2025, https://www.eppo.go.th/index.php/en/en-energystatistics/electricity-statistic.
[50] Bronk, Chris, Gabriel Collins, and Dan S. Wallach. "The Ukrainian Information and Cyber War." The Cyber Defense Review 8, no. 3 (2023): 33–50. https://www.jstor.org/stable/48755360.
[51] Sarah McFarlane, "Rogue Communication Devices Found in Chinese Solar Power Inverters," Reuters, May 14, 2025, https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/.
[52] Conway, Tim, Robert M. Lee, and Jeff Shearer. 2020. ICS Defense Use Case #7: Analysis of the Recent Report of Supply Chain Attacks on U.S. Electric Infrastructure. SANS. June 12, 2020. Accessed October 14, 2025. https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt12a556a8dbe7446c/607f2358b35a7a3c69a371c3/SANS_ICS_DUC_7_supply_chain_attacks_on_US_electric_infrastructure.pdf.
[53] Andy Greenberg, "How 30 Lines of Code Blew Up a 27-Ton Generator," Wired, October 23, 2020, https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/, Anton Cherepanov and Robert Lipovsky, "Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet," WeLiveSecurity (blog), ESET, June 12, 2017, https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.
[54] Golden, Christopher M. "Thesis: Huawei's 5G Networks and the Threat to America's National Security." U.S. Command and General Staff College (2020).

[55] Jordan Robertson and Michael Riley, "The Long Hack: How China Exploited a U.S. Tech Supplier," Bloomberg, February 12, 2021, https://www.bloomberg.com/features/2021-supermicro/.
[56] United States District Court, Southern District of Texas, Houston Division. United States of America v. Ehab Ashoor. Case No. H-09-CR-307. Excerpt of Transcript of Proceedings Before the Honorable David Hittner and a Jury, Testimony of Warren Jay Widner, Lee Chieffalo, Dewan Cureston Britwon, and Daniel Nugent. January 11, 2010. Document 89, filed January 19, 2010. Page 71, https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/r9dKMMM0Gi5I/v0.
[57] Zhang Wei, Gu Hongjian, Ao Naixiang, Wang Deyong, and Li Hua. "A Method for Social Security Risk Early Warning Based on Abnormal Electricity Consumption Behavior Identification." Journal of the China Academy of Electronics and Information Technology 11, no. 6 (2017). Quoted and summarized in "Academic: A Method for Social Security Risk Early Warning Based on Abnormal Electricity Consumption Behavior Identification," KKNews, March 27, 2017. https://kknews.cc/zh-hk/tech/k8ylx9q.html (張威、顧洪健、敖乃翔、王德勇、李華。《基於異常用電行為識別的社會治安風險預警方法》。〈中國電子科學研究院學報〉第11卷第6期，2017年。轉載並摘錄於〈學術：基於異常用電行為識別的社會治安風險預警方法〉，《每日頭條》，2017年3月27日).
[58] "China: Big Data Fuels Crackdown in Minority Region," Human Rights Watch, February 27, 2018, https://www.hrw.org/news/2018/02/27/china-big-data-fuels-crackdown-minority-region.
[59] Bronk, Chris, and Wm Arthur Conklin. "Who's in charge and how does it work? US cybersecurity of critical infrastructure." *Journal of Cyber Policy* 7, no. 2 (2022): 155-174.

Baker Institute for Public Policy