

ANALYSIS | ATHENALAB

Geopolitics, AI and Chile's Strategic Autonomy

Alejandro Amigo

Senior Researcher AthenaLab

September 28, 2026



ATHENALAB

International relations • Security • Defense
CHILE

1. INTRODUCTION

The central historical question of geopolitics is who controls space. Strategic passages, sea lanes and natural resources are some of the elements that define the distribution of power and the freedom of action of States. The current level of progress in artificial intelligence (AI) adds a new variable to that equation. Therefore, it is now important to know which state actors control the data centers, semiconductors, models and standards on which other States depend.

The leading powers in AI development, the United States and China, compete in this field with different emphases. To some extent, each replicate in this new dimension the type of power it already exercises over geographic space. In sum, Washington seeks to control the critical points of the technology chain, while Beijing expands through diffusion and mass adoption.

This article argues that AI extends the geography of power into a new space of competition, in which data, models, compute, standards and user networks become sources of influence. For countries such as Chile, this could affect their strategic autonomy, since seemingly technical decisions may end up conditioning their national security. It also presents opportunities, because the new geography still requires energy, minerals, territory and routes; areas in which Chile holds relevant assets.

This analysis first describes the layers of the AI ecosystem; then, the approaches of China and the U.S. in this field; next, our country's vulnerabilities; and, finally, Chile's options in this new area of geopolitics.

2. THE LAYERS OF THE NEW VARIABLE OF POWER

The AI ecosystem can be understood as a set of overlapping layers, each made up of nodes that represent sources of influence. At the base are the energy, water and critical minerals that sustain digital infrastructure. Above them sits a second layer, made up of data centers; transmission media, such as submarine cables, and semiconductors; and computing capacity. In this layer, influence derives from who produces and operates that infrastructure and, in the case of advanced chips, from who controls their export.

The third layer is data, where influence derives from the jurisdiction under which data are stored and from the access that other States may claim over them. Next come the models, closed or open, which create dependence on the provider and its updates. Further up are standards and regulations, where influence is exercised by whoever sets the rules of the game. The final layer comprises users and applications, where network effects raise the cost of switching providers or platforms.

This reading shows that power in the field of AI is exercised from specific nodes within these layers and that no single state actor controls all of them. It also demonstrates that geography still matters, since data centers need territory, energy and water, and submarine cables follow concrete routes. Therefore, States that lack the capabilities to compete at the technological frontier can occupy relevant positions in the lower layers, a point developed for Chile further on.

3. TWO APPROACHES TO AI

The approaches of the United States and China to AI carry over into this dimension the ways in which both powers already exercise their power in the classic geographic sphere; an imperfect but useful analogy for understanding how each of these actors approaches the ecosystem described above.

THE UNITED STATES: CONTROL OF CRITICAL POINTS

The United States sustains its global power through a network of alliances and bases located in regions of importance to the aims of its strategy. With respect to AI, it replicates that logic by dominating the chokepoints of the technology chain. Its companies concentrate the design of advanced chips, the main cloud platforms and frontier models. In addition, since 2022 Washington has used export controls to prevent China from accessing the most advanced semiconductors and equipment. The AI Action Plan of July 2025 formalized this approach in three pillars, which seek to accelerate innovation, build infrastructure and lead in AI diplomacy. The plan also seeks to prevent adversaries from accessing compute, as this is a matter of geostrategic competition and national security.¹

This U.S. containment policy also has an expansion dimension, aimed at getting partners to adopt American technology rather than Chinese technology. The aforementioned plan states that the United States must meet global demand by exporting its full technology stack. In this regard, the executive order of July 2025 that created the American AI Exports Program offers partners packages of hardware, data, models, cybersecurity and applications.²

This expansion also relies on selective alliances around the semiconductor supply chain, which reproduce on the technological plane the logic of the U.S. network of security alliances. The Pax Silica declaration, signed by Japan, South Korea, Singapore, the Netherlands, Israel, the United Arab Emirates, the United Kingdom and Australia, among other States, seeks to secure the supply chains of the chips used in artificial intelligence models.³

This initiative, which Chile recently joined, establishes a hierarchy between allies integrated into U.S. technological infrastructure and clients that only have market access.

Access to U.S. technology thus operates as a bargaining instrument, in the same way as the security guarantees it grants its allies under certain conditions. The risk of this approach is that the conditional use of access to that technology may erode the trust of its partners, since they may perceive in U.S. policy a transactional logic rather than a stable commitment.

CHINA: EXPANSION THROUGH DIFFUSION

In recent decades, China has projected its influence through trade and infrastructure, with the Belt and Road Initiative as its most visible expression. In AI it follows a similar path, as it seeks to expand through mass adoption. In July 2025 it presented its Global AI Governance Action Plan, directed at the Global South through digital infrastructure, technology transfer and participation in international standards.⁴ Likewise, in July 2026 it launched the World Artificial Intelligence Cooperation Organization in Shanghai, with 29 founding countries.⁵

The central instrument of the Chinese approach is open models that any company or government can download, adapt and deploy without restrictive licenses. The results are visible: in 2025, Chinese models overtook U.S. models in downloads on Hugging Face, with 41% of the total, and Alibaba's family of models has accumulated more than 113,000 derivative models.⁶ Added to this is a loop in the manufacturing sphere, since open models make it possible to deploy AI at low cost in factories, logistics and robotics, whose operational data feed back into the models. This physical loop largely escapes U.S. export controls, which focus on access to chips for training.⁷

The dependence created by Chinese open models is different from that created by closed services. An open-weight model running on one's own infrastructure cannot be switched off from Beijing, which reduces the risk of denial of access.

Its effect is more indirect, since whoever builds on Chinese models adopts their updates, tools and the technical ecosystem that develops around them. In this way, China gains influence through use, without States needing to sign agreements.

The limit of this approach is trust, because China's influence depends on governments, companies and developers being willing to integrate into their systems models designed according to Beijing's interests. For example, Chinese models incorporate the content restrictions required by Beijing's regulations, which translates into censored or biased answers on topics sensitive to the Communist Party. For this reason, in 2025 several governments restricted the use of applications such as DeepSeek on official devices, which slows Chinese penetration precisely in state and sensitive uses.⁸

4. CHILE'S EXPOSURE

Faced with the competition between both powers, middle powers such as Chile face a dilemma between achieving a degree of technological sovereignty and the dependence that results from integrating into external ecosystems. Developing their own capabilities offers greater autonomy but requires resources, scale and time that cannot be sustained, while adopting external technologies accelerates digital transformation in exchange for new forms of dependence. Therefore, decisions regarding AI models, cloud services or infrastructure providers must weigh certain aspects that could affect our strategic autonomy, which can be identified in at least four areas. It can be argued that Chile already faces each of these risks, which could materialize in contexts of crisis or tension between powers, when reversing the decision would be costly.

- **Alignment Risk**

This refers to the risk that the choice of technology providers becomes a condition of the bilateral relationship, so that a technical or commercial decision ends up affecting areas such as security cooperation, trade or access to technology. In Chile, this risk already materialized in February 2026, when the United States revoked the visas of three Chilean officials over their role in China Mobile's Chile-China Express cable, whose concession had been approved and then revoked in January.⁹

- **Control of Critical Infrastructure**

States that build or operate cables and data centers gain surveillance or disruption capabilities over essential flows. In June 2026, the Humboldt cable was approved, which will connect Chile with Australia from 2027 through a joint venture in which Desarrollo País and Google each hold 50%.¹⁰ The project strengthens Chile's position as a hub toward the Asia-Pacific, but it also concentrates half of the control of a strategic infrastructure in a U.S. company. Likewise, had Chile opted for the Chile-China Express cable, that infrastructure would have been owned by China Mobile, a state-owned company subject to China's National Intelligence Law, which obliges organizations to cooperate with that country's intelligence services.

- **Sovereignty over Sensitive Information**

Critical state data hosted by foreign providers fall within reach of extraterritorial laws and intelligence services. Chile addresses this risk only from a privacy perspective, through Law 21,719, which regulates international transfers of personal data and whose entry into force is still pending. However, there is no explicit national security criterion for state and defense data hosted in foreign clouds.

- **Supply Chain**

A state actor can suspend the supply of, or restrict, chips, compute, updates or cloud services, and do so precisely when they are most needed. Latam-GPT, the regional model promoted by CENIA and presented in February 2026, illustrates this exposure across several layers at once. It was built on Llama 3.1, an open-weight model from the U.S. company Meta, and its first version was trained on the AWS cloud.¹¹ Moreover, the supercomputer planned at the University of Tarapacá depends on chips whose export is controlled by the United States. Thus, the main regional effort to reduce external dependencies rests on technology from a single country.

CONCLUSION: CHILE'S OPTIONS

The question of who controls space remains valid; however, it has now broadened and coexists with another one, namely, who controls the layers of the AI ecosystem on which other actors depend. Chile is exposed in the upper layers but holds relevant assets in the lower ones, which depend on geology, climate and geography. Our country is the world's largest producer of copper and the second-largest producer of lithium, and its northern region records some of the highest levels of solar radiation in the world, allowing it to offer clean, low-cost energy to an industry whose electricity consumption is growing rapidly. These advantages are already translating into more than USD 7.5 billion in committed data center investments by AWS, Microsoft and Google.¹² In addition, the Humboldt cable could make the country the first direct digital link between South America and the Asia-Pacific.

However, these opportunities will only become bargaining power if our State uses them with strategic judgment.

Today, decisions appear to be made in a fragmented manner, project by project, and the result is a drift toward the U.S. ecosystem, reinforced by Chile's recent accession to Pax Silica, with clouds, cables and chips of that origin, in a country whose main trading partner is China. To turn this position into strategic autonomy, four lines of action are proposed, each aimed at mitigating one of the exposure mechanisms described.

- The first line of action responds to alignment pressure and consists of creating a body that jointly assesses digital infrastructure decisions. This task could be assigned to a National Security Council that would make it possible to permanently integrate the technological, diplomatic and defense dimensions. Within that framework, a critical technologies committee, with the participation of the Ministries of Science, Foreign Affairs, Defense, Public Security and Finance, as well as the National Cybersecurity Agency (ANCI), could apply national security criteria to those decisions before the next crisis arises and bring coherence to the country's position.
- To reduce the risk of control of critical infrastructure, the proposed committee should apply a prior and transparent security review procedure to submarine cables, data centers and cloud services serving the State, with known criteria of ownership, jurisdiction and access. This would have allowed the Chinese cable case to be resolved under clear rules, rather than amid sanctions.
- Regarding the exposure of sensitive information, the State needs a national security criterion for its own data, complementing the privacy approach of Law 21,719. This entails classifying public data according to their level of sensitivity and requiring that defense, intelligence and critical infrastructure data be hosted on infrastructure under Chilean jurisdiction or with verifiable contractual guarantees.

- Finally, to reduce the risk of denial of access, Chile must diversify its providers and, at the same time, use its position to obtain better conditions. In public procurement, this means requiring portability and multi-cloud architectures, and preferring, for sensitive uses, models that can be deployed on the country's own infrastructure. In parallel, the country can link incentives for data centers, such as access to energy and faster permitting, to counterparts such as computing capacity reserved for national research and state organizations.

NOTES

¹ The White House, Winning the Race. America's AI Action Plan, July 2025. <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>

² The White House, Promoting the Export of the American AI Technology Stack, July 2025. <https://www.whitehouse.gov/presidential-actions/2025/07/promoting-the-export-of-the-american-ai-technology-stack/>

³ Elcano Royal Institute, Pax Silica. Alliances, frontier and markets in the geopolitics of the chip. <https://www.realinstitutoelcano.org/en/analyses/pax-silica-alliances-frontier-and-markets-in-the-geopolitics-of-the-chip/>

⁴ ANSI, China Announces Action Plan for Global AI Governance, August 2025. <https://www.ansi.org/standards-news/all-news/8-1-25-china-announces-action-plan-for-global-ai-governance>

⁵ Government of the People's Republic of China, Xi calls for equitable global AI governance, unveils new cooperation body, July 2026. https://english.www.gov.cn/news/202607/18/content_WS6a5c27e1c6d00ca5f9a0c4d8.html

⁶ Hugging Face, State of Open Source on Hugging Face. Spring 2026, 2026. <https://huggingface.co/blog/huggingface/state-of-os-hf-spring-2026>

⁷ Ngor Luong, USCC, Two Loops. How China's Open AI Strategy Reinforces Its Industrial Dominance, March 2026. https://www.uscc.gov/sites/default/files/2026-03/Two_Loops--How_Chinas_Open_AI_Strategy_Reinforces_Its_Industrial_Dominance.pdf

⁸ Al Jazeera, Which countries have banned DeepSeek and why?, February 6, 2025. <https://www.aljazeera.com/news/2025/2/6/which-countries-have-banned-deepseek-and-why>

⁹ UPI, Chinese cable project causes rift before Chile presidential transition, March 2026. https://www.upi.com/Top_News/World-News/2026/03/03/latam-chile-kast-boric-transition-dispute/5301772565134/

¹⁰ Ex-Ante, Cómo avanza el cable submarino de Google con el Estado [How Google's submarine cable with the State is progressing], June 2026. <https://www.ex-ante.cl/como-avanza-el-cable-submarino-de-google-con-el-estado-luego-de-que-el-gobierno-dejara-el-proyecto-chino-en-el-congelador/>

¹¹ CENIA, Latam-GPT: la primera IA regional abierta creada con datos latinoamericanos [Latam-GPT: the first open regional AI created with Latin American data], February 10, 2026. <https://cenia.cl/2026/02/10/latam-gpt-la-primera-ia-regional-abierta-creada-con-datos-latinoamericanos/>

¹² CNN Chile, Amazon, Microsoft y Google entre ellos. Chile suma más de US\$ 7.500 millones en inversiones comprometidas en data centers [Amazon, Microsoft and Google among them: Chile tops USD 7.5 billion in committed data center investments], 2026. <https://www.cnnchile.com/negocios/amazon-microsoft-google-chile-suma-mas-us7500-millones-inversiones-comprometidas-data-centers/>