Issue Brief
June 15, 2026

Chips, Code, and Control: Rewriting the Economics of Old Tech Wars

Abhivardhan and Jagannath Panda

Photo credit: Dancing Man / Shutterstock.com

Is the emerging global technology order still defined by a single United States–China rivalry, or has that binary narrative already become obsolete? This paper argues that contemporary techno-geopolitics is no longer a unified "tech cold war," but a fragmented competition across two distinct domains: semiconductors and artificial intelligence ecosystems. The semiconductor contest is shaped by export controls, manufacturing chokepoints, strategic denial, and industrial subsidies. By contrast, AI ecosystems remain more networked and commercially interoperable through data flows, cloud infrastructure, open-source models, and cross-border talent mobility. This paper contends that states misread technological competition when they treat chips and AI as a single geopolitical battlefield. While semiconductor nationalism may intensify hardware decoupling, algorithmic ecosystems are far harder to contain. This divergence is creating a new hierarchy of power shaped not only by fabrication capacity, but also by influence over code, standards, data governance, and platform dependency. It further argues that middle powers, including India, Japan, South Korea, and Singapore, can leverage this fragmentation to pursue technological sovereignty through diversified semiconductor partnerships and sovereign AI governance frameworks.

For nearly a decade, even in a pre-COVID world, the dominant debate in global technology politics was framed in simple terms: the United States leads innovation, China scales manufacturing, and the rest of the world must choose sides.[1] That binary framing is now increasingly outdated. The intensifying competition between Washington and Beijing over semiconductors has not produced a single, unified technological cold war.[2] As Han-Wei Liu and Ching-Fu Lin (2025)[3] posit, this shift represents a move toward "techno-geopolitics," where the international legal order is being revitalized by the logic of national security. In this environment, the global semiconductor value chain has been weaponized through specific "chokepoint" nodes. These are essential, non-

substitutable segments, such as extreme ultraviolet (EUV) lithography and advanced electronic design automation (EDA) tools, where a handful of actors hold the structural power to exclude entire nations from technological progress. This modern pursuit of technological dominance mirrors a much older historical impulse. As Ian Morris (2013) observes, the attempt to measure "war-making capacity" through assessments of relative military power is as old as conflict itself.[4] Today, however, the "algorithms" for predicting the outcome of future conflicts are no longer found in troop numbers alone, but in the relative strength of a society's digital and industrial base.

It has therefore generated diverging effects across two connected but increasingly separate domains: chips on one side, and artificial intelligence ecosystems on the other. Semiconductors remain deeply tied to industrial capacity, military modernization, and supply-chain control. AI, however, depends not only on chips but also on data flows, cloud infrastructure, research talent, open-source models, regulation, and trusted partnerships. This distinction matters because while the U.S.-China chip rivalry has become sharper and more restrictive, the global AI ecosystem[5] has become more networked, decentralized, and commercially adaptive.

"Governments across the Indo-Pacific are no longer responding to a single technological contest. They are increasingly managing two parallel geopolitical realities. One concerns strategic hardware dependency, and the other concerns software power, data governance, and access to frontier AI systems.

As a result, governments across the Indo-Pacific are no longer responding to a single technological contest. They are increasingly managing two parallel geopolitical realities. One concerns strategic hardware dependency, and the other concerns software power, data governance, and access to frontier AI systems. This shift is creating new diplomatic openings for countries such as India, Japan, South Korea,[6] Singapore, and other middle powers[7] across the Global South. The central question today is no longer whether the U.S.-China tech war will divide the world; it is whether the eventual fragmentation of chips and the globalization of AI can create space for new technological sovereignty elsewhere.

Why the Chip War Is Producing Uneven Outcomes

The semiconductor competition between the United States and China has become highly political. Export controls, entity blacklists, investment restrictions, and subsidies are now core tools of statecraft.[8] Washington seeks to slow China's access to advanced chips, lithography tools, and high-end computing power. Beijing, in turn, has doubled down on indigenous semiconductor capabilities, industrial subsidies, rare earth leverage, and domestic substitution strategies.

Yet the effects of this competition are not evenly distributed. Restrictions on advanced GPUs or chipmaking tools can slow training capacity for frontier AI models, but they do not halt innovation entirely. AI development increasingly benefits from model efficiency, distributed computing, specialized chips, open-source architectures, and smaller domain-specific systems. In other words,

denying access to the most advanced hardware may constrain scale, but it does not eliminate creativity or adoption.

Domestic politics in both powers reinforce this divergence.[9] In the United States, bipartisan constituencies support industrial reshoring, strategic denial policies, and domestic manufacturing incentives. But there is also pressure from business groups and universities that seek continued market access, research collaboration, and talent mobility. In China, nationalist narratives support technological self-reliance, yet private-sector actors continue to prefer integration with global markets, software ecosystems, and international standards. This implies that semiconductor nationalism is politically easier to sustain than total AI decoupling. Chips can be regulated at ports, factories, and customs systems. Data, talent, code, and models move differently. They are harder to contain. Thus, the chip war continues to escalate, while AI ecosystems remain partially interoperable.

The Weakening of Traditional Technology Spillovers

Earlier phases of U.S.-China technological competition created broad spillover effects that functioned as a blunt instrument against entire industrial sectors. Restrictions in one domain, such as telecommunications hardware, semiconductor fabrication, or student visas, often cascaded through wider innovation networks to disrupt unrelated research endeavors. During this era, semiconductor sanctions could influence the depth of research collaboration, while talent restrictions slowed the growth of entire digital ecosystems, primarily because the underlying innovation infrastructure remained tethered to specific physical geographies. Trade tensions historically spilled into cloud services, standards-setting, and venture capital flows with little regard for the specific nuances of the technology involved.

“Research highlights that corporations routinely deploy generative AI to fragment and optimize their supply chains, frequently using superficial compliance metrics to deflect regulatory scrutiny. Thus, the geopolitical power of algorithmic networks operates completely independently of the physical hardware layer.

That dynamic is less relevant today as technology sectors move toward a more modular configuration. Firms now redesign supply chains to compartmentalize geopolitical risk by separating the trajectories of automation across different global markets. Multinational companies increasingly delink sensitive hardware operations from global software businesses to navigate the complex politics and governance challenges surrounding cross-border flows. This separation allows organizations to maintain a presence in competing jurisdictions. Universities diversify their partnerships, while governments construct trusted corridors for research that bypass restricted critical sectors, ensuring that scientific collaboration is guided by institutional trust rather than simple geographic proximity.

Recent research[10] highlights that corporations routinely deploy generative AI to fragment and optimize their supply chains, frequently using superficial compliance metrics to deflect regulatory

scrutiny. A multinational firm, for example, might publicly purge Chinese silicon from its hardware to satisfy Western security mandates while simultaneously deploying advanced AI software globally to capture emerging markets. Such firms often leverage performative compliance narratives to mask this dual strategy. Similarly, a sovereign state might join semiconductor security coalitions led by Washington while quietly integrating Chinese cloud infrastructure into commercial sectors to accelerate domestic economic growth. This selective engagement proves that the geopolitical power of algorithmic networks operates completely independently of the physical hardware layer.

This fragmentation has major regulatory implications that demand a new approach to governance. While semiconductor policy revolves around export control, industrial subsidies, and fabrication resilience, AI-governance issues, including privacy, safety, liability, and the norms around use of AI systems, are emerging as distinct geoeconomic and sovereignty challenges. Algorithmic systems create asymmetric operational dependencies, and foreign platforms can unilaterally alter terms of service, degrade model performance, or sever API access, effectively crippling a host nation's digital economy without ever imposing a physical embargo. Therefore, conflating these domains is misguided because governing intangible data flows and algorithmic liability requires a fundamentally different geopolitical logic from that required to secure physical industrial manufacturing supply chains. It is time for countries to recognize the necessity of building separate institutions, legal frameworks, and diplomatic strategies to manage the unique evolution of automated systems and the ethics that govern their deployment.

> ***"The global AI ecosystem operates as a decentralized network driven by private tech platforms, open-source communities, and fluid cross-border data architectures. Statecraft must essentially map its traditional tiers of human engagement onto the divergent physical and digital realities of the modern technology stack.***

Two Diplomatic Tracks: Chips Security and AI Cooperation

Historically, the architecture of global statecraft has relied on a tiered system of engagement to navigate complex international relations. The traditional framework designates Track 1 as formal, direct government-to-government negotiations; Track 2 represents entirely unofficial channels that rely on academics, industry leaders, and civil society to build consensus outside rigid policy constraints; while Track 1.5 seamlessly merges these two worlds, creating informal venues where state officials and private experts collaboratively tackle emerging geopolitical threats. The divergence between hardware security and algorithmic governance now necessitates a structural evolution of this framework. Semiconductor supply chains are physical, geographically bound, and strictly governed by zero-sum, state-led export controls, making them the natural domain of hard Track 1 negotiations. Conversely, the global AI ecosystem operates as a decentralized network driven by private tech platforms, open-source communities, and fluid cross-border data architectures. Therefore, regulating AI systems and ecosystems demands integrating the actual

commercial and academic architects of these models through robust Track 1.5 and Track 2 channels. Statecraft must essentially map its traditional tiers of human engagement onto the divergent physical and digital realities of the modern technology stack.

Consequently, the first diplomatic track must directly govern the physical layer of the semiconductor industry. This domain involves forging trusted manufacturing partnerships and navigating critical physical chokepoints such as lithography, electronic design automation, and access to rare earths. The geopolitics of hardware are inherently exclusionary because dominant powers closely guard the physical stack to constrain participation across the supply chain. Countries like Japan, Taiwan, and South Korea remain central to this landscape as they manage fabrication incentives and security-screened technology alliances.[11]

Conversely, the second track operates as a fluid, multi-stakeholder arena focused entirely on the evolutionary trajectories of different kinds of automation and the governance of algorithmic infrastructure. Nations must pursue independent technology diplomacy tracks that remain deliberately disaggregated from traditional economic negotiations. This shift demands rigorous negotiation over data portability and the applied ethics of cross-border information flows. States lacking semiconductor fabrication strength can still exert massive geopolitical power through the implementation of a dedicated Technology–Foreign Affairs–Defense–Industry (2+2+T) ministerial framework. Such a framework elevates technological sovereignty as a permanent fourth pillar alongside foreign, industrial and defense policy, ensuring that agreed-upon algorithmic principles govern the flow of information rather than simple geographic proximity. To operationalize this framework,

> ***"Diplomatic agreements must include legally binding commitments for shared capability building. Participating states would co-fund regional high-performance computing clusters and collaborate on curating cross-border datasets specifically reflecting unique Indo-Pacific contexts.***

the "T" (Technology) must function as a distinct geopolitical lever. Integrating this technology pillar alongside foreign and defense policy requires four specific structural adaptations:

- **Synchronizing Controls on Algorithmic Intangibles:** While traditional defense tracks manage hardware export regimes (like the Wassenaar Arrangement), the technology pillar must govern the non-physical chokepoints of the AI era. Nations would use this forum to align regulatory restrictions on the cross-border transfer of foundational model weights, proprietary synthetic datasets, and advanced algorithmic architectures, preventing adversaries from bypassing silicon sanctions through software acquisition.

- **Aligning Algorithmic Governance with Hard Security:** The framework must dictate the precise terms of AI integration into joint military operations. Allies would use these forums to establish definitive red lines for autonomous weapons systems and forge secure, shared protocols for pooling sensitive defense data.

- **Architecting Federated Interoperability Corridors:** Rather than passively relying on the API gateways of dominant global tech monopolies, the technology track must establish direct, state-sanctioned technical bridges. This involves negotiating the exact cryptographic standards that allow sovereign AI ecosystems across the Indo-Pacific to securely communicate and execute joint inferences without ever surrendering data to a third-party cloud provider.

- **Mandating Compute Pooling and Joint R&D:** Diplomatic agreements must include legally binding commitments for shared capability building. Participating states would co-fund regional high-performance computing clusters and collaborate on curating cross-border datasets specifically reflecting unique Indo-Pacific contexts.

Emerging corporate partnerships signal a fractured world order where sovereignty is shared between nation-states and massive technology platforms.[12] Therefore, Indo-Pacific economies must actively secure strategic leverage within this new reality. Negotiating robust data rights and enforcing the operational ethics of digital infrastructure remain strategic imperatives.

> ***India holds a distinct strategic advantage. The country's digital public infrastructure has already proven that sovereign, state-backed protocols can successfully shape market behavior and prevent foreign capture of civic technology.***

India and the Indo-Pacific Digital Opportunity

While Indo-Pacific governments frequently publish ambitious AI strategies, their continued fixation on hardware procurement leaves their economies vulnerable to these operational chokepoints.[13] India, however, holds a distinct strategic advantage in neutralizing this exact vulnerability. The country's digital public infrastructure has already proven that sovereign, state-backed protocols can successfully shape market behavior and prevent foreign capture of civic technology. Translating that precedent into the AI epoch requires moving beyond basic capacity building and asserting greater architectural agency, encouraging domestic frameworks and market standards to govern the region's digital dependencies.

For instance, a less discussed but increasingly obvious impact of the Brussels Effect[14] is that, while European regulators successfully developed sophisticated rules governing data, platforms and AI, the resulting interoperability and compliance challenges generated substantial costs that favored large technology platforms with significant regulatory resources, particularly those in the United States. Moreover, while the Brussels Effect did influence American regulatory mechanisms around data, platforms and AI, it did not necessarily empower start-ups and legacy tech players within the EU. This suggests that India has a meaningful opportunity to pursue cognitive independence and digital individual sovereignty by championing cooperation through interoperable standards.

In fact, physical geography further amplifies sovereignty. Major infrastructure projects, such as coastal data center initiatives in Andhra Pradesh, serve as modern strategic ports. These high-capacity hubs offer surrounding nations a neutral and reliable alternative to dominant global

technology platforms. In addition, cognitive independence relies heavily on cultivating a thriving research-industrial nexus. The Anusandhan National Research Foundation, for instance, has the potential to act as the primary catalyst for this shift.[15] The focus must pivot toward bridging the crucial gap between academic research and industrial application. Targeted investments in edge computing and proprietary models can forge independent, specialized technological architectures. India can then leverage these homegrown innovations by exporting them across the Global South as sovereign digital public goods, thereby helping establish a resilient, alternative technological bloc.

Why Data Governance Matters More than Ever

Physical infrastructure and computing clusters establish the foundation of the modern digital economy. Legal frameworks, however, dictate how that structural power is wielded and who captures the resulting value. As such, the importance of data governance has expanded exponentially.

Industry practice increasingly demonstrates that AI governance functions as a direct subset of data governance. The operational integrity of any foundational model depends heavily on strict controls over data provenance, training quality, and rigorous lifecycle testing. Across the Indo-Pacific, robust data legislation has consequently evolved into a primary instrument of modern digital statecraft. These frameworks preempt extractive practices in which foreign platforms leverage behavioral data to train proprietary systems without adequate local accountability. They enforce a reciprocal dynamic, guaranteeing that domestic datasets generate an equitable return for the local economy while simultaneously dictating the parameters within which AI systems operate inside sovereign jurisdictions. Building on the reality that algorithmic integrity relies on effective data control, two strategic pillars underpin this vision of legal architecture:

> ***"Building on the reality that algorithmic integrity relies on effective data control, the two strategic pillars—fiduciary data obligations, and tiered sovereignty and algorithmic independence—underpin legal architecture across the Indo-Pacific.***

- **Fiduciary Data Obligations:** Meaningful accountability requires global platforms that extract behavioral insights to contribute directly to the ecosystems from which these insights are derived. Modern legislation should enforce fiduciary duties alongside standard privacy rights. Entities processing domestic data must commit to concrete ecosystem reinvestments, including funding local research initiatives, curating high-quality datasets for model training, and subsidizing the shared digital infrastructure required for rigorous algorithmic auditing.

- **Tiered Sovereignty and Algorithmic Independence:** A nuanced approach to data residency can protect vital national interests without isolating domestic markets. Strategic datasets involving defense, public health, and government operations may demand absolute domestic retention to minimize external vulnerabilities. At the same time, standard commercial data can circulate freely across trusted regional corridors governed by

interoperable Indo-Pacific standards. Because AI governance inherently relies on data access, meaningful algorithmic independence mandates that foundational models trained on the domestic population should be open to localized scrutiny, auditing and adaptation. This will help local developers and regulators to conduct fine-tune and technical auditing, ensuring the underlying intelligence layer remains accountable to domestic legal and regulatory frameworks.

The fusion of these proactive frameworks with expanding physical connectivity offers a compelling pathway forward for Indo-Pacific nations. Within this model, robust sovereign safeguards and active participation in global markets can reinforce rather than undermine one another.

Summing Up

Viewing global technological advancement strictly as a binary superpower rivalry is increasingly inadequate. The international system has evolved into a more complex and layered geopolitical reality. This fragmentation creates a significant strategic opportunity for India and the broader Indo-Pacific region. Securing long-term prosperity does not require dependence on any single technological ecosystem. Instead, durable strategic influence will depend on the seamless fusion of independent digital infrastructure and visionary data governance. Moving forward, the ultimate measure of resilience in the AI era will extend far beyond control of semiconductor supply chains to encompass the institutions, standards, and governance frameworks that shape how technology serves society.

Authors –

Abhivardhan *is an AI Strategy & Governance Specialist. He is the President of the Indian Society of Artificial Intelligence and Law, and leads an AI Governance research firm, Indic Pacific. His interests and expertise span Indo-Pacific studies, AI governance, digital competition and AI & intellectual property strategies.*

Dr Jagannath Panda *is the Head of Stockholm Center for South Asian and Indo-Pacific Affairs (SCSA-IPA) at the Institute for Security and Development Policy. He is also the Editor for ISDP.*

About ISDP

The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.

www.isdp.eu

Endnotes

1 Carla Hobbs (ed.), *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry* (London: European Council on Foreign Relations, July 30, 2020), https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/; Kandy Wong, "Why this China analyst thinks full decoupling is unlikely and what gets missed in talk of reforms," *South China Morning Post*, July 11, 2024, https://www.scmp.com/economy/china-economy/article/3270078/why-china-analyst-thinks-full-decoupling-unlikely-and-what-gets-missed-talk-reforms.

2 Mohammed Soliman, "AI, the Gulf, and the US: A Primer," *Middle East Institute*, February 26, 2026, https://mei.edu/report/ai-the-gulf-and-the-us-a-primer/

3 Han-Wei Liu and Ching-Fu Lin, "Techno-Geopolitics and Semiconductor Chokepoints: Beyond the US-China WTO Dispute," *The Journal of World Investment & Trade* 26, no. 4 (2025): 749–791, https://doi.org/10.1163/22119000-12340372.

4 Ian Morris, *The Measure of Civilization: How Social Development Decides the Fate of Nations* (Princeton: Princeton University Press, 2013).

5 Abhivardhan and Arunima Jha, "India's AI Opportunity Lies In What It Chooses To Not Do," *Swarajya*, February 1, 2026, https://swarajyamag.com/technology/indias-ai-opportunity-lies-in-what-it-chooses-to-not-do.

6 Pratnashree Basu and Abhishek Sharma, "The Indo-Pacific frontline: Japan and South Korea respond to Russian threats," Observer Research Foundation, Expert Speak (Raisina Debates), February 10, 2025, https://www.orfonline.org/expert-speak/the-indo-pacific-frontline-japan-and-south-korea-respond-to-russian-threats.

7 Francisco Javier Varela Sandoval, Isabella Wilkinson, Alex Krasodomski, and Rowan Wilkinson, "How middle powers can weather US and Chinese AI dominance: The case for 'sovereign AI' strategies," Chatham House, February 16, 2026, https://www.chathamhouse.org/2026/02/how-middle-powers-can-weather-us-and-chinese-ai-dominance/.

8 Han-Wei Liu and Ching-Fu Lin, "Techno-Geopolitics and Semiconductor Chokepoints: Beyond the US-China WTO Dispute," *The Journal of World Investment & Trade* 26, no. 4 (2025): 749–791, https://doi.org/10.1163/22119000-12340372.

9 Georgios Dimitropoulos, "Digital Plurilateralism in International Economic Law: Towards Unilateral Multilateralism?" *The Journal of World Investment & Trade* 26, nos. 1-2 (2025): 116–155, https://doi.org/10.1163/22119000-12340354.

10 Zhe Sun, Lei Liu, Liang Zhao, Hind Alofaysan, and Bhumika Gupta, "Generative AI and ESG opportunism in supply chains: A utilitarian perspective on unintended consequences for sustainability," *Technological Forecasting and Social Change* 224 (2026): 124498, https://doi.org/10.1016/j.techfore.2025.124498.

11 Jagannath Panda, "The great danger of allowing China to co-manage global order," Institute for Security and Development Policy *(ISDP)*, June 2026 (first published in *The Washington Examiner*, March 21, 2026), https://www.isdp.eu/publication/the-great-danger-of-allowing-china-to-co-manage-global-order/.

12 Daryl Copeland, "Heteropolarity, Globalization and the New Threat Set," Guerilla Diplomacy - Rethinking International relations, February 14, 2012, https://www.guerrilladiplomacy.com/2012/02/heteropolarity-globalization-and-the-new-threat-set/#.

13 Siwei Huang, "Strategic Choices and Tradeoffs for Asia-Pacific Middle Powers in the AI Age," CAPRI Foundation, January 27, 2026, https://caprifoundation.org/securing-agency-and-managing-trade-offs-in-the-age-of-ai-strategic-choices-for-asia-pacific-middle-powers/.

14 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020).

15 Arpan Tulsyan, "The Innovation Imperative: ANRF and India's Research Vision," Observer Research Foundation, October 17, 2025, https://www.orfonline.org/expert-speak/the-innovation-imperative-anrf-and-india-s-research-vision.