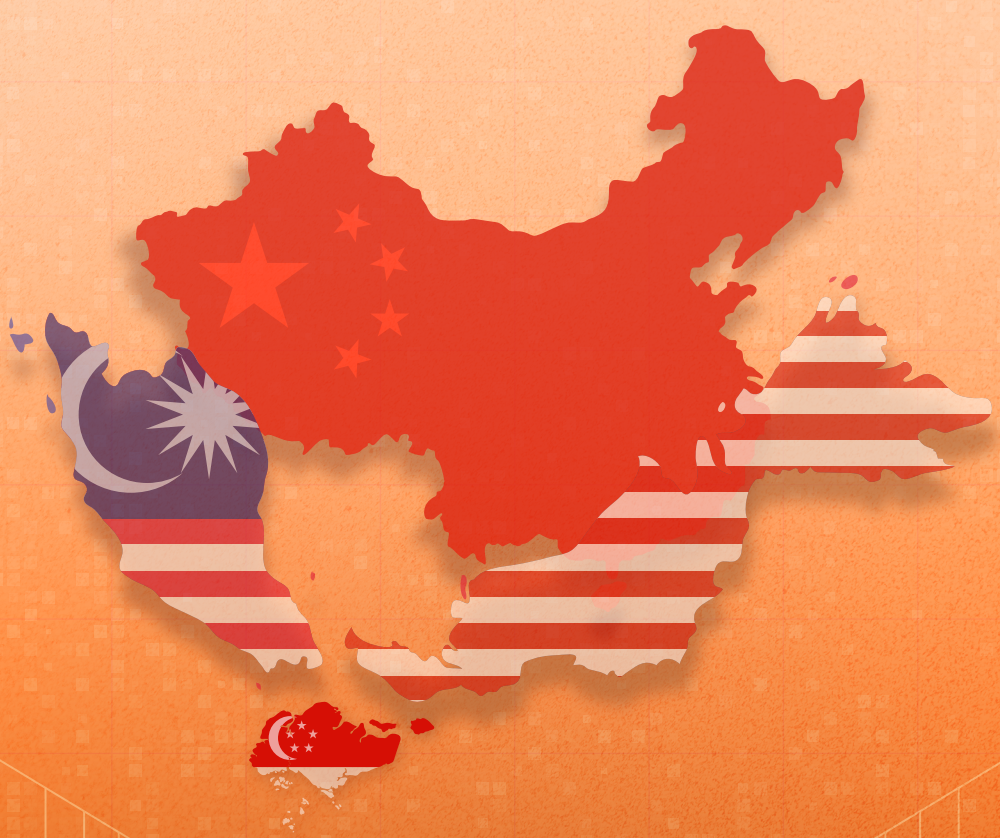
Research Institute for Democracy, Society, and Emerging Technology



A Shared Future?

Economic Security Challenges from Malaysia-China Economic Cooperation and Data Center Development

Chris Chih-Hua Tseng, Jin Chian Seer

OCT. 2025

A Shared Future?

Economic Security Challenges from Malaysia-China Economic Cooperation and Malaysia's Data Center Development

Research Institute for Democracy, Society and Emerging Technology (DSET)

Founded in October 2023 by Taiwan's National Science and Technology Council (NSTC), the Research Institute for Democracy, Society, and Emerging Technology (DSET) is Taiwan's first national think tank focused on the intersection of democracy, technology, and public policy. DSET places democratic values at the core of its mission and addresses emerging global challenges through evidence-based research and strategic analysis.

DSET's research focuses on four key areas: Economic Security, Democratic Governance, Climate Resilience and Sustainability, and National Security. It also operates a Non-Resident Fellow program that engages Taiwanese scholars and graduate students based in the United States, Europe, Japan, and other like-minded countries. Through policy research, international dialogue, and Track 1.5 diplomacy, DSET provides strategic recommendations to the public and government, strengthens Taiwan's global engagement, and promotes democratic, future-oriented approaches to technology governance.

Economic Security Research Program

The Economic Security Research Program focuses on Taiwan's economic security reforms and the emerging challenges of international multilateral cooperation. Taiwan's advanced semiconductor manufacturing capabilities form a critical foundation for maintaining order and security among techno-democracies. As global technological advancements accelerate, Taiwan's semiconductor industry remains a key driver. However, China's pursuit of technological hegemony poses comprehensive threats, making institutional reforms essential not only for Taiwan's survival but also for the broader interests of the international community.

Amid ongoing global supply chain restructuring, Taiwan faces urgent questions about its strategic positioning. How can it adapt to these shifts and work with allies to consolidate shared economic and security interests? In the era of techno-geopolitics, this research program offers policy reports and expert analysis to foster dialogue, inform decision-making, and help shape international consensus.

Disclaimer

This report was independently reviewed and published by DSET. The views expressed herein are solely those of the authors and do not represent the official position of the Government of Taiwan or the National Science and Technology Council (NSTC)

DSET Staff Authors

Economic Security Research Program

Chris Chih-Hua Tseng
Non-resident Fellow

Jin Chian Seer
Policy Analyst

The following individuals also contributed to this report:

Yun-Ting Cai
Deputy Director, Data Team

Billy Zhe-Wei Lin
Research Fellow, Data Team

Executive Summary

This report is a review of the current Malaysia-China economic cooperation and a case study of Malaysia's data center development to understand the potential Chinese influence in these projects. Our intention is to shift policymakers' attention from items, end-use, and end-users to think about economic security challenges that come from supplier-side relationships and different types of economic cooperation between China and other non-aligned emerging economies, particularly through the case of Malaysia and the data center industry. We hope that this approach can complement the existing discussion on AI leadership, AI infrastructures, and technology diversions, and stimulate policy discussions on meeting the needs of non-aligned countries that could provide comparative infrastructural advantages to the American AI capabilities.

Specifically, we examined recent trends of trade and foreign direct investment from China to Malaysia, and we highlighted several memoranda of understanding (MOUs) signed between the two countries in April 2025 that reflected core goals of Malaysia-China economic cooperation. Then, we zoomed in on the Malaysian data center case to explore various roles in the data center supply chain and the geopolitical and geoeconomic advantages of Southeast Asian countries in the data center industry. More importantly, we differentiated several models of collaborations in the data center industry, including greenfield, joint venture, colocation, and hybrid cloud. We identified the economic security risks that come along with different models, using examples of collaborations between Malaysian and Chinese firms, including the hardware-level risks (Greenfield), physical access risks (Colocation), covert equity influence (Joint Venture), and API-level leakages (Hybrid Cloud).

Lastly, we made several policy recommendations that expand the scope of the newly announced AI Action Plan and address concerns from recent incidents of diversions while strengthening the position of the U.S. and allies in building more cooperation with Southeast Asian countries. On the one hand, we suggested stronger regulations on computing power, more validating mechanisms that can be used to investigate various types of joint collaboration on data centers, and strengthening customs inspections on high-end SSDs to counter the smuggling of high-performance AI training hard drives. On the other hand, we highlighted the need for the U.S. and allies to incentivize other countries to continue working with the U.S., developing broader cooperation to strengthen their industrial bases and, in return, tapping into their comparative infrastructural advantages and countering China's ambition of dominating AI infrastructures in this key region.

Key Findings and Recommendations:

1. Chinese capital has been significantly and consistently investing in Malaysia, building the foundation for Malaysia to engage in broader economic cooperation with China, signing multiple MOUs in 2025 to collaborate on industrial transformation, digital economy, technological innovation, and advanced technology applications.

2. The complex roles between suppliers and co-development models for data centers can lead to various levels of economic security risks. Beyond greenfield and colocation, joint ventures and hybrid clouds may pose higher risks due to shareholder influences and API-level leakages.

3. Two interrelated directions should be considered in regulating data center development. First, rules for profiling and verifying data centers and access to computing power should be established, including a trusted whitelist program, a safe computing density threshold, and an expansion of extraterritorial authority on critical infrastructure protection for AI infrastructures.

4. Second, the capacity for investigating and prosecuting indirect transfers through unlisted foreign entities should be strengthened. This includes end-use and end-user declarations, chip security mechanisms, and customs inspections for high-performance SSDs.

5. Lastly, to incentivize allies and non-aligned countries to develop closer cooperation, a new partnership framework on AI infrastructure should be created. Incentives and punishments are closely related; as the U.S. deploys more tariff pressure on other countries, an AI infrastructure partnership framework can enable the U.S. to expand its AI infrastructure while encouraging trusted countries to access U.S.-licensed technologies and achieve economic upgrading, thereby countering China's tactics in the region.

Contents

List of Tables

List of Figures

Section I: Malaysia-China Economic Cooperation in the Era of U.S.-China Competition

Introduction :

1. Why Southeast Asia? Why Malaysia?

The exigency of economic security lies not only in illuminating security risks but also in a deeper understanding of the interdependent world. This report examines Malaysia-China economic cooperation, particularly through the case of data centers, to identify the main incentives for Malaysia and the risks associated with different models of cooperation.

Before we go further with the analysis, we want to first discuss the case selection logic behind focusing on Southeast Asian countries, particularly Malaysia, in this report. There are three reasons why Southeast Asian countries should receive more focus. First, many Southeast Asian countries have emerged as the largest partners for China. In 2024, ASEAN was the largest trading partner for China, with a total trade volume of USD 988.2 billion, according to China's National Bureau of Statistics. Regarding individual countries, Vietnam, Malaysia, and Indonesia are the top three trading partners among ASEAN countries. Moreover, China has also targeted many Southeast Asian countries as its major outbound investment partners. According to China's Ministry of Commerce, in 2023, Singapore is the second-largest outward direct investment (ODI) destination behind Hong Kong, while Indonesia, Vietnam, Thailand, Malaysia, Cambodia, and Laos are all among the top 15 recipients.

Second, ASEAN countries, particularly Singapore and Malaysia, have been expanding their footprint in the semiconductor industry and emerging technologies, welcoming investments from both the U.S. and China. Since the 1990s, Singapore and Malaysia have been using their regional advantage of dense industrial networks and cheap labor costs to attract foreign investment and enter the hard disk and high-tech industries. Currently, Singapore is one of the most prominent players in the semiconductor manufacturing equipment (SME) industry, while Malaysia has a strong presence in the semiconductor advanced testing and packaging (ATP) industry. In the last few years, Malaysia has attracted investment from multinational firms like Intel and Infineon, while Singapore has not only attracted manufacturers like UMC and Vanguard but also SME suppliers such as Applied Materials and Lam Research. ASEAN countries, particularly Singapore and Malaysia, have also gained prominence recently in the booming data center industry because of the density of submarine cables in the region, and studies have shown that ASEAN countries are more open to Chinese cloud providers, including Alibaba Cloud, Huawei Cloud, and Tencent, and all ASEAN countries have more than 50% of hyperscale cloud providers from China with some of them using entirely Chinese providers.[1]

Lastly, Malaysia is also politically important for ASEAN in 2025. Anwar Ibrahim, Malaysian Prime Minister, serves as the 2025 ASEAN chairman, and the country will host all the main ASEAN events, including the annual Summit and Foreign Ministers' Meeting. ASEAN has been

building bilateral talks with China and the Gulf Cooperation Council (GCC), aligning the Master Plan of ASEAN Connectivity 2025 with China's Belt and Road Initiative before, and in May 2025, ASEAN hosted its first three-way talk with both China and GCC, aiming to synergize markets and upgrade existing free trade agreements. Former Malaysian ambassador to the U.S., Mohamed Nazri bin Abdul Aziz, said in an interview regarding the three-way talk that China was "quickly filling up the vacuum" in global leadership as the U.S. has distanced itself from other countries because of tariff threats.[2] On the other hand, Malaysia also plays a crucial role in shaping the narrative and balancing acts between China and the U.S. for the region. Anwar Ibrahim has claimed that the ASEAN-GCC-China Summit still operated in ASEAN's balanced engagement, and ASEAN has made good progress in talking with the U.S. regarding their Comprehensive Strategic Partnership. In July 2025, Malaysia signed a Memorandum of Understanding (MOU) with the U.S. on strategic civil nuclear cooperation, and it also announced that it would require trade permits for AI chips of U.S. origin to move through Malaysia, making it one of the first Southeast Asian countries to align its export control policies closer with U.S. regulations.

2. Even More Strengthened Malaysia-China Cooperation

In April 2025, Chinese President Xi Jinping visited Cambodia, Malaysia, and Vietnam, and Malaysia and China signed 31 MOUs, focusing on a slew of issues from security cooperation and cross-border mobility of people and goods to cooperation on AI and emerging technologies. These MOUs expanded the existing Malaysia-China relationships in economic, financial, infrastructural, and technological cooperation, which have been established for several decades. China and Malaysia have established a comprehensive strategic relationship since 2013 with the signing of the Five-Year Program for Economic and Trade Cooperation (2013-2017), and in May 2014, Malaysia's Prime Minister Najib Razak and China's Premier Li Keqiang met in China, recognizing 2014 as the Malaysia-China Friendship Year and agreeing to achieve a bilateral trade volume of USD 160 Billion.

Besides the high-profile trip for the Chinese President, China also held its Central Conference on Work Related to Neighboring Countries (中央周邊工作會議) in April 2025, which set the scope of China's priority just days before Xi's trip. Besides Chinese President Xi, other participants included members of the Standing Committee of the Political Bureau of the Chinese Communist Party Central Committee: Li Qiang, Zhao Leji, Wang Huning, Cai Qi, Ding Xuexiang, and Li Xi, as well as Vice President Han Zheng. China last held this meeting in 2013, more than a decade ago, and the meeting this year marked China's return to its focus on neighboring countries. The conference concluded that China should extend President Xi's foreign affairs agenda, "building a community with a shared future," to its neighboring countries while deepening its ties through industrial and supply chain cooperation, security cooperation, and increased people-to-people exchanges.[3]

After these interactions between China and Southeast Asian countries, Malaysia is one prominent example of China's neighboring countries that is seen as shifting toward China

regarding international relations. One thing that we should emphasize is that, before the events of 2025, many observers noted that Malaysia had been dancing between the U.S. and China but not entirely tilting towards the latter.[4] Malaysia's Anwar Administration has been more deferential to China, praising Xi as an outstanding leader, pledging support for China's three global initiatives, and even dropping the word "peaceful" in recognizing China's One China Policy against Taiwan. However, Malaysia continued to pursue its strategies of equidistance and non-alignment to some degree with the U.S. by maintaining economic and security cooperation with the U.S. and its allies, most notably Japan and Australia, balancing visits between Chinese and U.S. officials, and hosting more multilateral military exercises with the U.S. than with any other partners.

However, in 2025, as China looked to strengthen its relationship with neighboring countries in Southeast Asia, the U.S. announced its "reciprocal" tariffs against all countries. While Malaysia was hit with a 24% tariff initially and later negotiated to 19%, tariffs have effectively drawn Malaysia closer to the Chinese circle, both narratively and economically.[5] After Xi's visit, Malaysia and China announced a joint statement that adopts China's policy agenda, endorsing China's narrative of building a community of shared future. Politically, Malaysia and China established an unprecedented "2+2" framework of Joint Foreign and Defense Dialogue mechanisms to deepen the high-level defense and strategic cooperation between the two. On the economic side, the 31 MOUs signed between the two countries are less about speculation on investment and trade but more comprehensive in terms of collaboration strategies on various fronts, from R&D to technological cooperation, expanding the scope of the 14 MOUs signed in 2024. Malaysia still maintains close ties with several U.S. allies, including Japan, Australia, and France. However, on the topic of economic security, these MOUs not only benefit the booming data center industry but also provide a broader landscape of how the strengthening of Malaysia-China ties can create challenges for the U.S. leadership. Given Malaysia's critical role in ASEAN and the Islamic finance and economy, these challenges can have implications for those areas as well.

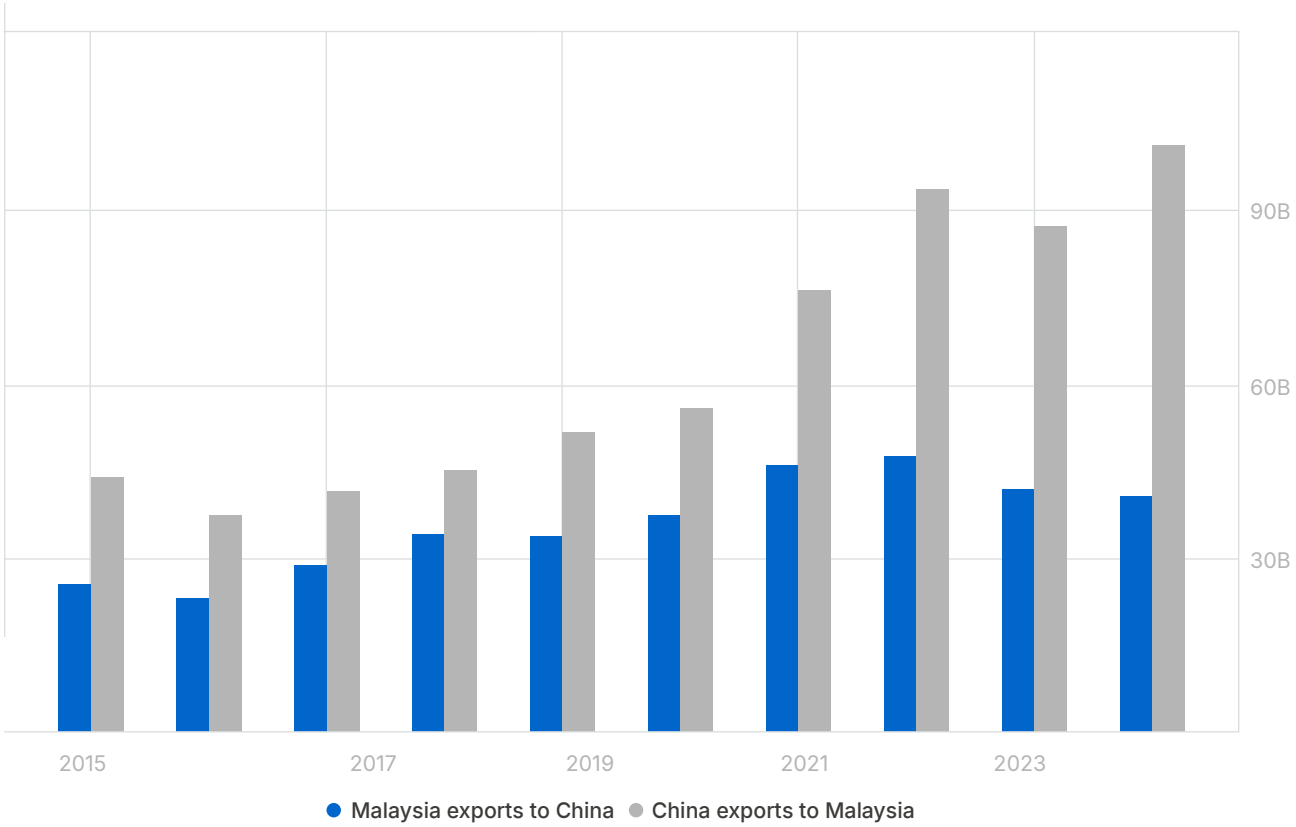
3. Background: Trade and Investment between Malaysia and China

Before we discuss the MOUs signed between the two countries, we should first elaborate on the growing economic ties between Malaysia and China. Regarding trade, China has been Malaysia's largest trading partner since 2009. According to Malaysia's Ministry of Investment, Trade, and Industry, the trade value between Malaysia and China in 2024 was USD 113.84 billion (RM 484.13 billion), representing 16.8% of Malaysia's total trade. In comparison, the total trade value between Malaysia and other ASEAN countries was USD 179.92 billion (RM 765.09 billion), with Singapore being Malaysia's second-largest trading partner. The U.S. was Malaysia's third-largest trade partner, with a trade value of USD 76.40 billion (RM 324.91 billion).

If we further break down the bilateral trade between Malaysia and China, we can see that not only has the trade volume between the two increased, but China's exports to Malaysia have

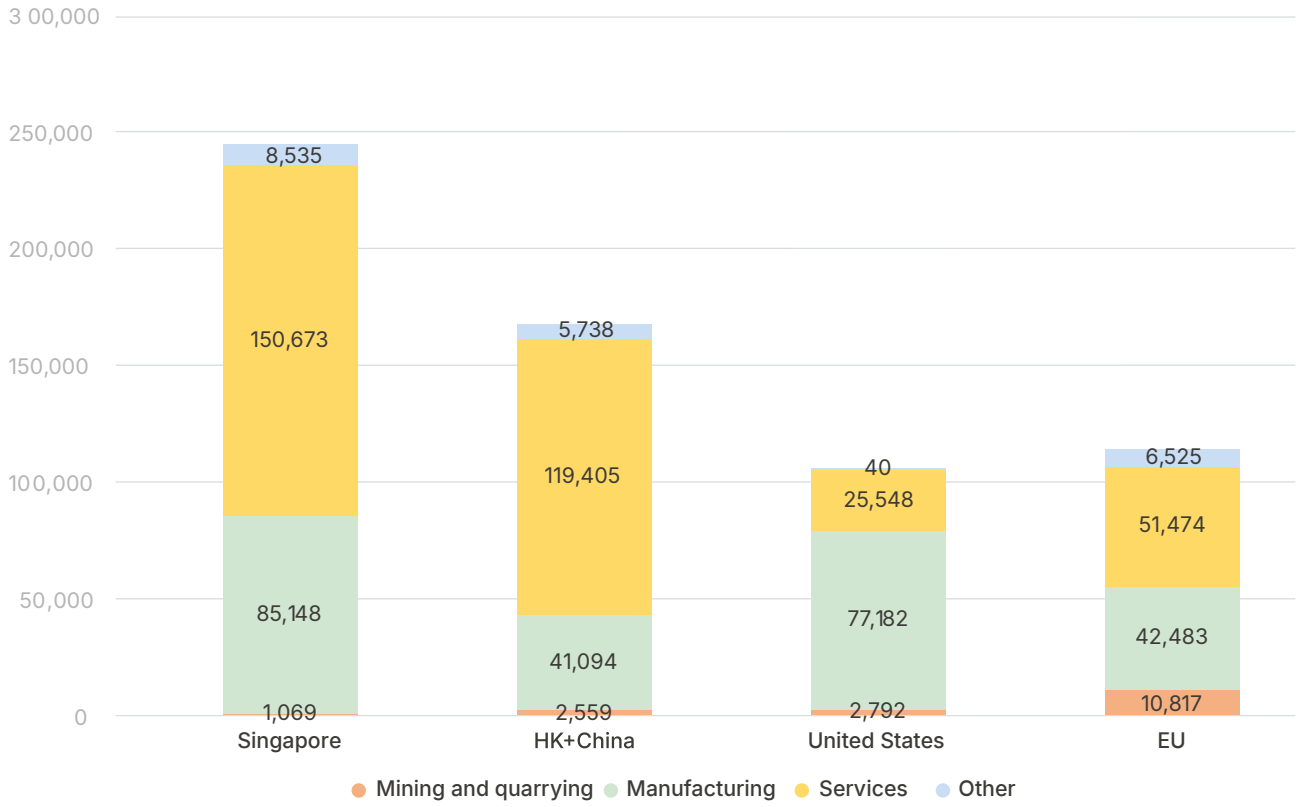
been growing in the last few years, signaling a stronger interdependence between the two and the growing Chinese economic leverage over Malaysia, according to the UN Comtrade database (See Figure 1). In 2024, the top 3 exports from Malaysia to China were electrical and electronic equipment (USD 16.16B), mineral fuels, oils, and distillation products (USD 4.49B), and plastics (USD 2.43B), while the top 3 exports from China to Malaysia, excluding unspecified commodities, were electrical and electronic equipment (USD 25.13B), machinery, nuclear reactors, boilers (USD 13.86B), and plastics (USD 4.71B), per the UN Comtrade database. Generally, Malaysia and China are more interdependent on each other, particularly in the electronics sector.

Figure 1. Malaysia-China Bilateral Trade from 2015-25



Source: UN Comtrade Database; Trading Economics

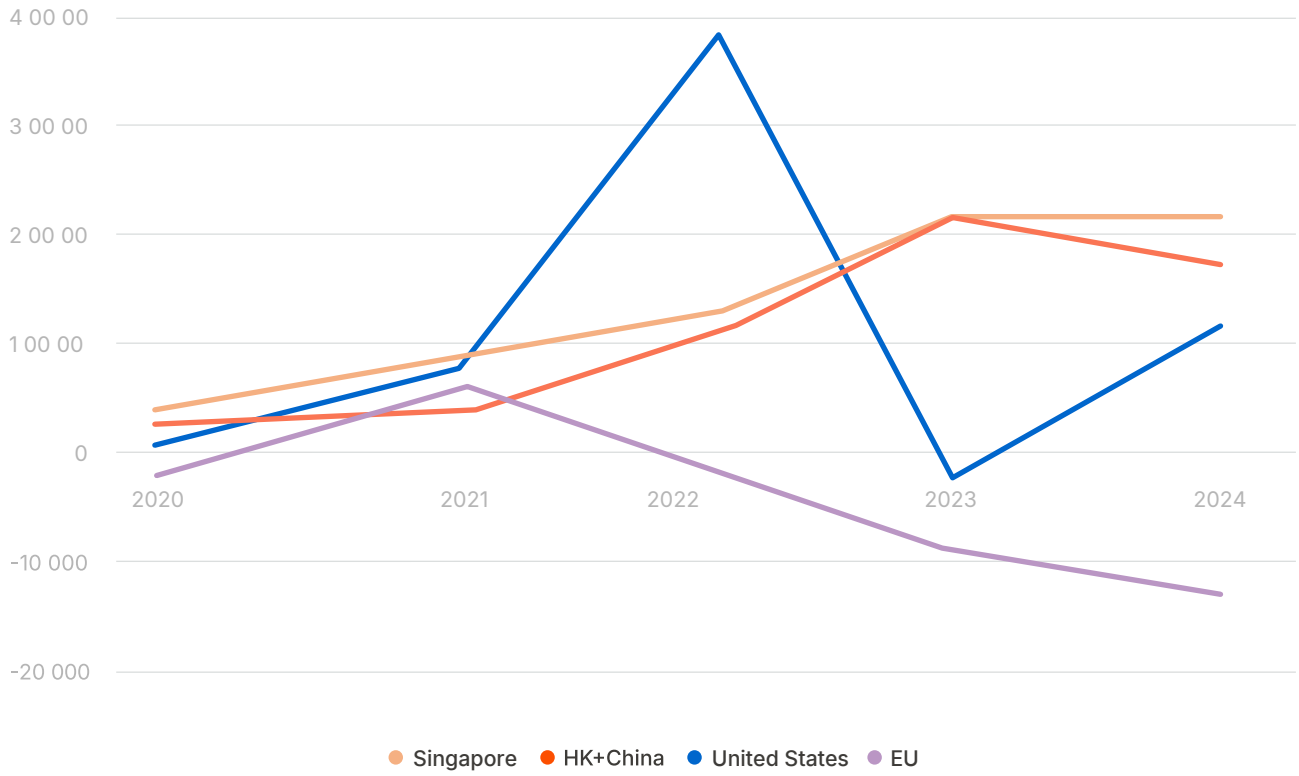
Figure 2. Malaysia's FDI Stock by Countries and Sectors in 2024 (RM Million)



Source: Department of Statistics Malaysia (DOSM).

However, bilateral trade can only tell us the interdependence between countries, and for an FDI-dependent country like Malaysia, we also need to examine investment flows to understand why Malaysia is more dependent on China in recent years and is more inclined to strengthen economic cooperation with China. Malaysia's economic development has relied on foreign direct investment (FDI) as a crucial mechanism to attract capital and drive technological innovation, and Chinese capital has become more substantial than that of other Western countries. In 2024, besides Singapore, China (including Hong Kong) is the largest source of Malaysia's FDI stock, signaling the penetration of Chinese capital in Malaysia and its lasting influence (see Figure 2). In fact, U.S. FDI stock in Malaysia has been outshone by Chinese (including Hong Kong) capital since 2016. Considering the historical legacies, the EU has a larger FDI stock in Malaysia; however, it was surpassed by Chinese capital in 2023. Although the U.S. still invests heavily in Malaysia's manufacturing sector, it is not the largest source of FDI stock in the manufacturing sector; instead, Singapore is the largest immediate source of FDI in the manufacturing sector, and considering China's massive outbound direct investment in Singapore, China may likely be the largest ultimate source of FDI in Malaysia's manufacturing sector.

Figure 3. Malaysia's Net FDI Flows by Country, 2020-24 (RM million)



Source: DOSM

Moreover, Chinese capital (including Hong Kong) has been constantly flowing into Malaysia, whereas EU and U.S. capital have been fluctuating and even declining. Figure 3 presents the net FDI flows from Singapore, China (including Hong Kong), the U.S., and the EU over the last five years. In the last five years, Hong Kong and Chinese capital have been constantly and increasingly investing in Malaysia, particularly in the manufacturing sector. Singaporean capital also flows into Malaysia in a steadily growing trend and a similar volume. Comparatively, the net FDI flows from the U.S. to Malaysia have greatly fluctuated, and the EU capital has been flowing out of Malaysia in the last three years.

This suggests that while U.S. FDI might provide a massive thrust in some years, Chinese and Singaporean capital can be more consistent in investing in Malaysia's manufacturing sector and strengthening its industrial base, which can lead to stronger export-oriented growth and more consistent economic upgrading.

In conclusion, Malaysia and China's close trade relationship is only part of the story; instead, we suggest that FDI is a crucial factor that explains Malaysia's goal to further its cooperation with China, including the signing of MOUs. China has been Malaysia's largest trading partner since 2009, but we have seen increased efforts to deepen cooperation between the two countries

in recent years. As FDI in Malaysia can lead to strong performance on GDP growth,[6] the growing importance of Chinese capital is both a signifier and a signified concept for further cooperation. On the one hand, to sustain and attract more FDI from China, particularly to invest in the manufacturing sector and achieve economic upgrading, MOUs build broader, government-to-government commitments to facilitate more cooperation between firms and universities. On the other hand, the weakening importance of U.S. investment vis-à-vis China has created less need for Malaysia to balance its economic relationship with the U.S. and become less responsive to U.S. economic security concerns unless it is pressed.

4. Malaysia-China MOUs and the Shared Future of Malaysia-China Economic Security

Here, we highlight some MOUs signed in April 2025 between Malaysia and China that can boost China's standing in emerging technologies, particularly the data center industry, and pose significant challenges to economic security.

1."Two Country, Two Parks": Since 2013, Malaysia and China have established the "Two Country, Two Parks" framework between the Malaysia-China Kuantan Industrial Park and the China-Malaysia Qinzhou Industrial Park. This framework attracted investment and enabled a growing volume of goods to flow into other countries, generating industrial opportunities, such as the steel industry in Kuantan, Malaysia, and the agricultural products processing industry in Guangxi, China.

In 2025, this new MOU upgrades the existing framework, and Malaysia and China agree to co-develop a new China-Malaysia High-Tech Eco-Industrial Park in Shenzhen.[7] This new MOU aims to foster high-tech collaboration between the two countries, investing $22 billion in building an industrial park with R&D activities in Shenzhen and manufacturing in Malaysia. The new industrial park will target key industries such as AI, new energy technologies, and advanced manufacturing equipment in its initial phase. Moreover, the new industrial park will leverage the advantages of the Shenzhen Special Economic Zone. The Shenzhen Government Procurement Association and the Shenzhen Outbound Alliance will be in charge of attracting key industrial players and developing supply chain systems.

According to the MOU, this new industrial park will be designed on three pillars. First is the vertical collaboration between China's R&D and manufacturing in Malaysia. Secondly, institutional integrations between Malaysia and China will be made, including standardization and the creation of a digital customs, where Huawei Cloud is one of the known service providers. Lastly, this project will help local Malaysian firms to enhance their capabilities and integrate into high-tech supply chains. One notable example is the collaboration between Shenzhen's Googol Technology, which specializes in semiconductor manufacturing equipment, and Malaysia's Censof, a semiconductor testing firm. Chinese officials also highlighted Chinese EV manufacturers, such as Geely and Chery, and Chinese data center firms, including GDS and Chindata Group, as crucial players in accelerating Malaysia's economic transformation.

2.**Malaysia-China Joint Laboratories on AI and Material Science:** Malaysia's Minister of Science, Technology, and Innovation (MOSTI) signed an MOU that aims to launch new joint laboratories between the two countries. This MOU aims to provide mutual support for establishing joint laboratories in emerging technologies among research institutions, higher education institutions, and enterprises. These laboratories will target areas like AI, blockchain, biotechnology, advanced material technology, renewable energy, and other mutually identified emerging technologies, and this initiative aligns with Malaysia's industrial policy and political agenda, such as the New Industrial Master Plan 2030 and the Malaysia Madani to achieve economic growth through innovation, economic and workforce upgrading for Malaysians.[8]

3.**Global Talent Cooperation:** Another MOU, signed between China and Malaysia's Minister of Higher Education, aims to create cooperation between the University of Malaya and Peking University and establish joint laboratories, primarily collaborating on AI and material technology.[9] The cooperation between Malaysia and China on cultivating global talents in AI and emerging technologies comes at a time when the U.S. is cracking down on research universities and foreign visas. These two MOUs should be understood in light of China's expansive efforts to win the global race for talent[10] and strengthen China's industrial capabilities through investing in research infrastructure.

4.**AI and Digital Economy Cooperation:** Here, we highlight two MOUs signed between China's National Development and Reform Commission (NDRC) and Malaysia's Minister of Digital, whose agency was newly established by the current Prime Minister Anwar Ibrahim. Regarding AI cooperation, Malaysia and China aim to strengthen technology exchange programs, AI infrastructures (including building datasets and data centers), collaborations on AI guidelines and applications, and jointly explore AI security risks. On the other hand, the two countries will cooperate on the digital economy through policy coordination, digital transformation, innovation, and talent development. Moreover, the Malaysia Digital Economy Cooperation (MDEC), an agency under the Ministry of Digital, will collaborate with China's Zhejiang University to further develop in the field of digital transformation, AI,and smart city applications.[11]

5.**Satellite-based Technology Applications:** The last MOU that is related to advanced technologies was signed between MOSTI and NDRC regarding China's BeiDou Global Navigation Satellite System (BDS), which is one of the leading navigation satellite systems in the world. The two countries agree to develop and apply satellite-based technology to various areas, including agriculture, logistics, finance, and manufacturing. The goal of this MOU for Malaysia is to enhance its capabilities in space technology and geospatial intelligence, encouraging co-development and upscaling satellite-based applications with Chinese firms and promoting collaborations between Chinese and Malaysian research institutions, universities, and firms.[12]

In conclusion, although we focused on MOUs that are related to semiconductors and emerging technologies, all the MOUs signed

between Malaysia and China symbolize the more comprehensive integrations between the two countries. By collaborating with China, Malaysia gains opportunities to upgrade its economy through Chinese investment, co-development, and technological innovations, which enable Malaysia to achieve greater leadership in ASEAN as Malaysia serves as the chairmanship in 2025. On the other hand, China can utilize these collaborations to tap into Malaysia's natural resources, infrastructure, and workforce to help solve China's own economic challenge of overcapacity. China can also benefit from Malaysia to build its supply chain resilience with Malaysian research institutions, universities, and firms in the face of economic uncertainties and restrictions. Moreover, with China's growing influence over Malaysia, China also gains better leverage to attract cooperation with other ASEAN countries and the Islamic economy.

5. Implications of the Malaysia-China Cooperation on the U.S. Economic Security

1.Malaysia as a Potential Loophole for Technology Diversions. Despite Malaysia's negation of direct governmental ties with Huawei-linked AI projects amid new U.S. rules on Huawei, Malaysian AI infrastructure firms, such as Skyvast, have announced their collaboration with Huawei and claim to use Ascend GPUs topower their AI servers.[13] Besides Huawei chips, as mentioned above, Huawei Cloud has also been one of the service providers for Malaysia-China industrial cooperation. Moreover, Malaysian research institutions, universities, and firms are encouraged to pursue co-development with Chinese entities, and as we will discuss below in the case study, some Malaysian firms like YTL Corporation have announced joint ventures on data center projects with leading U.S. firms such as Nvidia, while also collaborating on data centers with Chinese firms such as GDS. As a result, Malaysia has positioned itself between China and the U.S., and with Malaysia's growing integration with China through all the co-development and cooperation, Malaysian entities can become a loophole by developing ties with both sides. Although Malaysia balanced its engagement with China with the July announcement of requiring trade permits for AI chips of U.S. origins, the effectiveness of this remains to be seen.

2.Heightening the Global Talent Competition between China and the West. Although the number of Malaysian international students in the U.S. is declining year after year (around 4,800 students), Malaysia is the 7th and 11th largest source country of international students in the UK[14] and Australia[15] in 2023-24. Nevertheless, China has rapidly emerged as a popular destination for Malaysian students, with over 10,000 Malaysian students enrolled in Chinese universities in 2023,[16] creating greater competition for talent with other Western institutions. Chinese universities and research institutions are known to attract global talent with generous scholarships, and the Malaysia-China cooperation on talent development provides us with another view on using bilateral agreements to establish not just research cooperation or talent exchanges but also investing in joint laboratories and research infrastructures.

3.China's Future Cooperation with Other ASEAN Countries and the Islamic Economy. ASEAN countries have generally adopted multilateralism and non-alignment strategies. This does not mean that they prefer neutrality; rather, they would engage in multiple ties with major powers and delicately balance their relationships to avoid entanglements with great power rivalries. For instance, ASEAN countries such as Malaysia and Singapore have expressed that they are willing to comply with U.S. export control rules, but they would not amend any of their existing regulations. Moreover, ASEAN is a multilateral regime that prioritizes its centrality, preventing individual countries from altering regional affairs without coordinating with other ASEAN countries. Thus, on the one hand, China's strengthened bilateral ties with Malaysia would propel talks between China and the ASEAN platform on future cooperation, such as the recently completed free trade deal talks,[17] and on the other hand, we can expect that U.S. trade and economic security negotiations with individual ASEAN countries would be confounded by multilateralism and ASEAN centrality. Lastly, it is also possible that Malaysia's access to the Islamic economy can generate an even broader integration between sovereign wealth funds and energy production in the Middle East, infrastructural resources and workforce in Southeast Asia, and Chinese R&D capabilities, as China and Gulf countries have been looking to deepen their political and economic ties,[18] and as will be covered in our case study, sovereign wealth funds in the Middle East have also been investing in Malaysia's data center industry.

Summary

The Malaysia-China economic cooperation should be understood as efforts from Malaysia to address challenges to its development in the high-tech sector. Malaysia, and to some extent, the broader Southeast Asia, can be trapped in economic upgrading due to two primary factors: overreliance on foreign investment that tends to maintain lower-value-added production in the country, and a low-skilled labor force comprising both domestic and migrant workers. The MOUs mentioned above highlighted Malaysia's efforts to apply advanced technology, strengthen industrial transformation and digital economy, and deepen collaboration between Malaysian and Chinese universities and laboratories in the training of skilled labor, R&D, and technological innovation. The more robust and significant FDI in Malaysia from Chinese capital over the last decade signals that China may be more willing to work with Malaysia at the government-to-government level than the U.S. or other Western countries. As a result, Malaysia-China economic cooperation may not only create loopholes in the U.S.-led economic security regime that safeguards the diffusion of emerging technologies, but it also exposes the weaknesses of the U.S. partnership framework in working with other countries and actually portrays the leadership in the global race for technologies.

Section II: Southeast Asia's Strategic Role in Technological Geopolitics

Building on the analysis in Section I, Malaysia's deepening cooperation with China demonstrates how bilateral agreements can reshape the regional economic-security landscape, while also underscoring the strategic importance of both Malaysia and Singapore in Southeast Asia's technological geopolitics. In particular, the region has gradually evolved into a critical node in the global semiconductor and AI data center supply chains, bringing it back to the forefront of international attention. Section II will further examine the roles and strategic significance of Malaysia and Singapore in the geopolitics of technology.

1. Geopolitical Leverage and Strategic Alignment: Singapore and Malaysia as Emerging AI Data Center Hubs

Within the context of modern global trade and industrial supply chains, the region surrounding the South China Sea and the Strait of Malacca has long been recognized as a critical maritime corridor. Located at the southern edge of this strategic axis, Singapore and Malaysia's coastal cities—such as Penang, Port Klang, and Johor Bahru—alongside Indonesia's Batam Island, have emerged as preferred sites for multinational corporations establishing manufacturing bases and data infrastructure.

This trend began as early as the 1970s, when U.S. semiconductor firms, confronted by rising domestic costs, global competition, and the oil crisis, started offshoring backend processes—such as packaging and testing—to lower-cost Asian countries. This shift catalyzed the emergence of the foundry model and laid the foundation for the offshore fragmentation of the global semiconductor supply chain.

Emerging Asian markets—particularly Taiwan, Japan, and South Korea—quickly rose as key semiconductor powerhouses. Malaysia, meanwhile, leveraged its robust port infrastructure and cost-effective labor to secure a central role in backend operations.[19] Intel, among other U.S. firms, established facilities in Penang as early as the 1980s, gradually transforming the region into a so-called "Silicon Valley of the East." As of 2023, Malaysia accounts for 13% of the world's outsourced semiconductor assembly and testing (OSAT) capacity, and 20% of U.S. semiconductor imports.[20]

2. Structural Logic Behind Southeast Asia's Emergence as a Global AI Data Center Node

Singapore's geographic advantages date back to the 19th-century colonial era. Situated at the southern tip of the Malay Peninsula—between the Pacific and Indian Oceans—Singapore possesses a natural deep-water harbor and a prime maritime location. British colonial administrator Stamford Raffles established a free port system on the island, transforming it into a vital hub for international trade.

Following independence, Singapore continued to develop its port infrastructure and logistics capabilities. Through efficient governance and an extensive network of trade agreements—27 free trade agreements (FTAs) signed to date—

and maritime connections to over 600 global ports, Singapore has cemented its status as one of the world's most active trade hubs.[21] The PSA Singapore currently operates 55 berths with a design throughput capacity of 43.9 million TEUs annually.[22]

Beyond geography and trade, Singapore has attracted substantial FDI through sound financial regulation, liberal investment policies, and a pragmatic foreign labor framework.[23] Its "non-discrimination toward foreign capital" principle allows overseas firms to enjoy nearly equal status with domestic counterparts, reinforced by tax incentives, transparent regulations, and streamlined administrative procedures, creating a globally competitive business environment.

Singapore has also channeled its trade and financial capital into strategic national investments, with a strong emphasis on technological innovation and high-value-added sectors. This has led global tech firms—including Google, Amazon, Meta, and Microsoft—to establish their Asia-Pacific headquarters and cloud infrastructure hubs in the city-state.

In contrast, Malaysia—while a relatively late entrant—has rapidly risen due to its proximity to Singapore and its lower costs for land and electricity. In recent years, as Singapore imposed data center development quotas due to energy and land constraints, a wave of foreign investment shifted toward Johor (Malaysia) and Batam (Indonesia), positioning Johor as a new frontier for hyperscale data center development.[24]

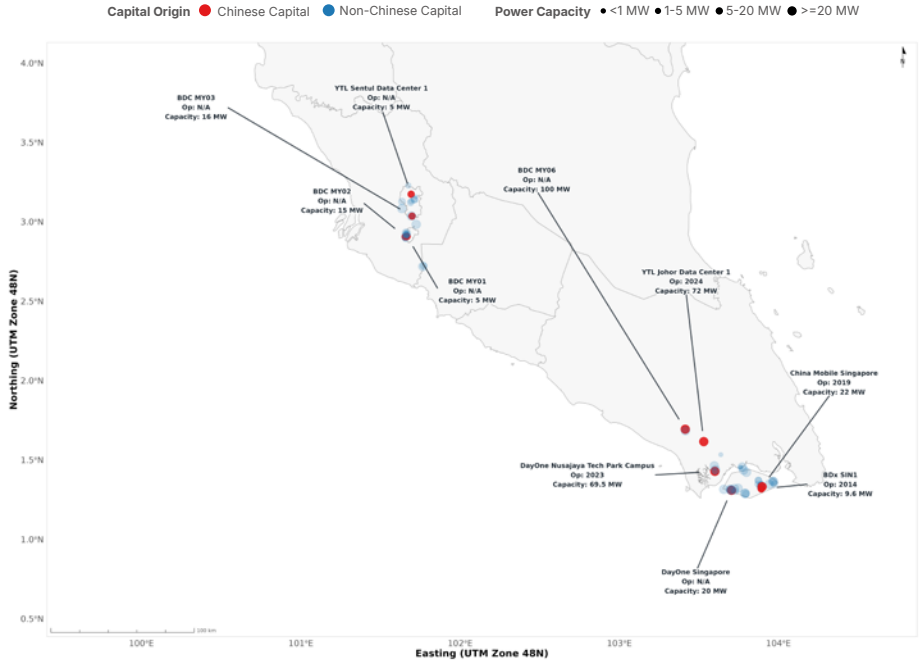
The Johor-Singapore Special Economic Zone (JS-SEZ), launched in 2025, further reduces the regulatory barriers to cross-border business.[25] [26] With expansive land, low-cost energy, and proactive policy support, Johor complements Singapore's ecosystem and connects to global data and compute flows via jointly developed submarine cable systems.[27]

3. Johor as a Geopolitical Battleground for Technology

As shown in Figure 4, Johor, Malaysia, has increasingly emerged as the primary spillover destination for Singapore's data center industry. In recent years, Singapore's moratorium on new data center licenses—driven by land scarcity and energy constraints—has pushed multinational operators to seek alternative sites across the border. Three main clusters in Johor have become focal points: Nusajaya Tech Park, Kulai, and Sedenak Tech Park.

According to data compiled by DSET, Johor has attracted not only Western operators relocating from Singapore but also significant expansion linked to the People's Republic of China (PRC). Notable projects include DayOne (the overseas brand of GDS Holdings), Bridge Data Centres' MY06 facility under ChinData, and the joint venture between GDS and YTL to develop a large-scale data center campus. Based on DSET's statistical compilation and compute-capacity conversion, as of August 2025, Johor accounts for the majority share of Malaysia's newly added data center capacity. Compared to other regions, Johor has already surpassed the historically dominant Klang Valley (Selangor and Kuala Lumpur), underscoring its role as the most important growth hub for regional AI infrastructure, as illustrated in Figure 5.

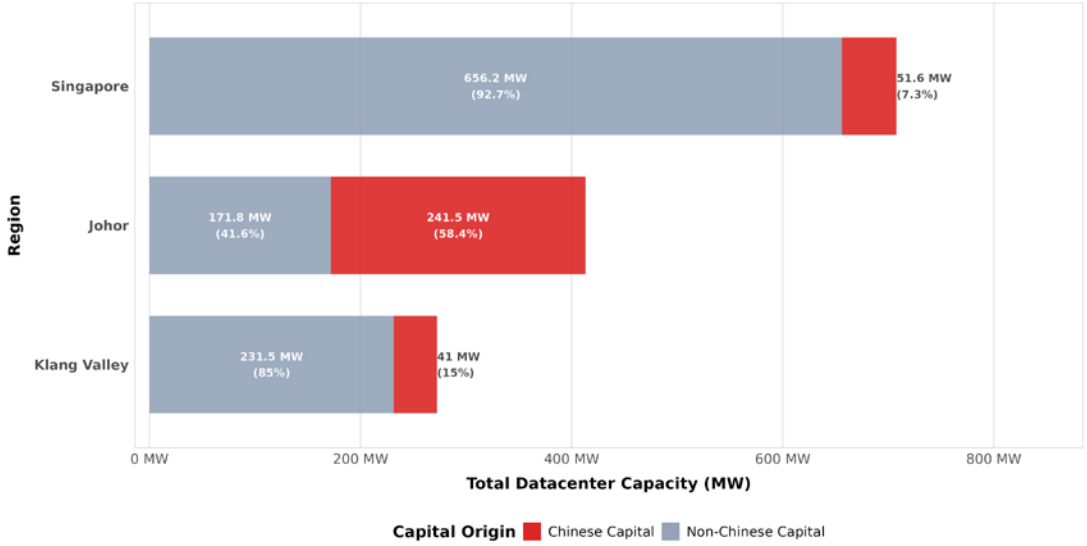
Figure 4: Mapping Data Center Capacity in Malaysia and Singapore: Chinese vs. Non-Chinese Capital Investments



Data:Enhanced datacenter estimates with Chiese capital classification
Red=Chinese Capital, Blue= Non-Chinese Capital
Labels show: Full Name | Operational Year | Capacity (Chinese capital facilities only)

Source: Data compiled by DSET from Datacenter Map;[28]
analysis of Chinese capital infrastructural participation and visualization conducted by the author.

Figure 5: Regional Datacenter Capacity in Malaysia and Singapore: Chinese vs. Non-Chinese Capital Investment Shares



Data:Enhanced datacenter estimates with Chiese capital classification
Red bars highlight Chinese Capital investment concentration
Values show capacity in MW and percentage of regional total

Source: Data compiled by DSET from Datacenter Map;[29]
analysis of Chinese capital infrastructural participation and visualization conducted by the author.

In addition, this report differentiates, on the infrastructural level, between PRC- and non-PRC-backed data center projects in Johor. The findings (see Figure 5) indicate that PRC-linked data centers account for a total of 242MW, compared to 172MW for non-PRC data centers, representing 58.4% of Johor's expansion.

Taken together, Johor has become the single largest concentration of PRC-linked infrastructural investment in Malaysia's national data center landscape, accounting for much of the region's recent surge in compute capacity. Beyond projects already operational or under construction, many additional facilities—announced via press releases but yet to break ground—are also expected in this area. In other words, Johor has rapidly evolved into a strategic frontier where Western hyperscalers and PRC firms compete side by side, turning it into a geopolitical battleground for control over next-generation compute power. While capacity shares will continue to shift as new facilities are completed, China's footprint in Johor already demonstrates an early and deliberate strategic positioning in the regional compute race.

4. China's Strategic Positioning in Southeast Asia

Over the past three decades, China has systematically advanced its "Go Out" strategy, deepening economic and supply chain cooperation with Southeast Asian nations.[30] Singapore and Malaysia have served as regional footholds for a broad range of industrial and infrastructure initiatives.

Singapore's partnership with China began with the launch of the China-Singapore Suzhou Industrial Park[31] in 1994, which later expanded to include the Sino-Singapore Tianjin Eco-city,[32] the Chongqing Connectivity Initiative,[33] and the China-Singapore Guangzhou Knowledge City,[34] focusing on domains such as urban governance, green transition, and the digital economy.

Malaysia, for its part, has become a critical node in the Belt and Road Initiative (BRI) since 2013.[35] Chinese capital and technology have supported a wide range of projects in manufacturing, infrastructure, and digital transformation—such as the East Coast Rail Link (ECRL) and the Melaka Gateway—strengthening Beijing's strategic footprint along the Strait of Malacca.[36] [37]

Beginning in 2024, the two countries signed a five-year China–Malaysia Economic Cooperation Framework (2024–2028), aimed at strengthening joint supply chain development and technology collaboration in semiconductors, AI, and digital infrastructure.[38]

In April 2025, the Trump administration imposed "Liberation Day Tariffs" on major manufacturing economies—34% on China and 24% on Malaysia (renegotiated to 19% in August).[39] In response, Beijing launched high-level diplomatic visits to Vietnam, Malaysia, and Cambodia, signing multiple memoranda focused on AI, manufacturing, and infrastructure cooperation.[40]

The Two Countries, Twin Parks Initiative exemplifies China's deepening engagement,

linking Malaysia's Kuantan Industrial Park with China's Qinzhou Free Trade Zone to create an integrated trade and industrial corridor, solidifying China's strategic influence in the Southeast Asian supply chain.[41] [42]

China's long-term cultivation of influence in the region is becoming increasingly visible. While both Singapore and Malaysia maintain strategic ambiguity in their foreign and technology policies, recent developments underscore the reach of Chinese engagement. In 2023, a spike in exports of high-end NVIDIA GPUs to Singapore raised suspicions of transshipment to China.[43] Malaysia's government also briefly announced plans to adopt Huawei's Ascend GPU for national AI infrastructure—a decision later rescinded following U.S. pressure, but nonetheless indicative of China's entrenched influence.[44]

At the same time, both Singapore and Malaysia are strategically leveraging this geopolitical moment to advance their national interests. By positioning themselves as neutral hubs and transshipment platforms in the reconfiguration of global value chains, these states illustrate how the tech war has evolved beyond a bilateral U.S.-China standoff into a multidimensional contest involving multilateral statecraft and alliance calculus.

Consequently, for the United States to implement an effective containment strategy targeting China's AI and semiconductor ambitions, unilateral sanctions or coercive restrictions on third countries will be insufficient. Instead, Washington and its democratic allies must cultivate inclusive partnerships with the Global South and non-aligned nations, building a trusted, values-aligned technological alliance that is not only defensive but also generative in its appeal.

5. Southeast Asia's Enduring Ethnic and Commercial Linkages with China

While China's formal state initiatives have reshaped Southeast Asia's strategic landscape, an equally consequential—but less visible—dimension lies in the region's ethnic Chinese business and trust networks.

Understanding China's influence thus requires examining not only government-led strategies, but also the historical and structural linkages rooted in diaspora communities, informal capital flows, and cultural affinity.

Since October 2022, the U.S. Department of Commerce implemented an interim final rule under the Export Administration Regulations (EAR) to restrict China's access to advanced semiconductor manufacturing equipment and high-performance GPUs. The measure marked a pivotal turn in U.S. export control policy, aiming to constrain China's capacity to train large-scale AI models and advance foundational chip technologies. In response, Chinese entities have pursued increasingly sophisticated circumvention strategies—many of which have been systematically analyzed in prior DSET studies (Uncovering Huawei's *Shadow Network*,[45] *The Great Siege*,[46] *The Remote Poaching Model*).[47] This intensifying confrontation has not only reshaped the global semiconductor supply chain but also creatednew pathways for industrial

reconfiguration and geopolitical competition.

Amid this global realignment, Singapore and Malaysia have emerged as strategic nodes in China's regional engagement, not only through formal diplomacy and economic initiatives, but also via less visible networks rooted in shared ethnicity and trust. One of the most consequential and yet often overlooked dimensions is the Bamboo Network: an informal but highly influential web of business and kinship ties among ethnic Chinese communities across Southeast Asia.[48]

Emerging from colonial-era migration patterns, this network is anchored in common ancestry, language, and cultural traditions. It continues to shape business practices, capital flows, and informal governance structures in the region. For many Malaysian and Singaporean Chinese business elites, these ties often carry greater operational significance than formal ownership or regulatory compliance. In recent years, the Chinese government has demonstrated increasing sophistication in leveraging these relationships to expand its strategic foothold in sectors such as AI infrastructure, enabling indirect channels of influence that may elude conventional oversight.

This dynamic is especially evident in the behavior of Malaysian Chinese conglomerates, many of which have repositioned themselves to lead the AI infrastructure wave through strategic transformation.[49] For example, the Kuok Group—via its subsidiary K2 Data Centres—has invested in self-built data center facilities in Johor, while YTL has utilized its existing in energy and construction to co-develop hyperscale data centers with China's GDS. These firms, rooted in traditional business models and bolstered by transnational commercial ties, are now channeling those capabilities into the AI domain. As a result, their investment origins, technology partners, and data flow configurations must be included in any robust risk assessment framework adopted by the United States and its democratic allies.

Section III: The Case of Malaysia's Data Center Industry

Part 1: From Land to Compute– Mapping the AI Data Center Supply Chain in Singapore and Malaysia

Following the preceding review of Singapore and Malaysia's geopolitical positioning and China's regional economic footprint, this section turns to the physical dimension of AI data center development in both countries. No longer merely data transit hubs, Singapore and Malaysia are rapidly emerging as strategic nodes in the global AI compute infrastructure map. As demand for generative AI and high-performance computing continues to surge, AI data center architecture and operational models have become focal points in the geopolitical contest for technological primacy.

This section provides a structured overview of the AI data center supply chain—from land acquisition and energy provisioning to construction, system integration, and operational management. It identifies key stakeholders and their roles across seven interconnected segments, establishing the analytical foundation for the next part's examination of Chinese infiltration risks and competing infrastructure models.

1. Land and Energy Providers

Both Singapore and Malaysia utilize state-backed mechanisms to allocate land and energy for AI data center development. Malaysia, in particular, leverages its abundant land reserves and natural gas resources to offer competitively priced, scalable infrastructure—especially in Johor. Key players include:

- **YTL** – Active in integrated energy and land development;
- **Keppel Corporation** – Operating across utilities, urban development, and data center infrastructure;
- **Sime Darby Property** – A leading developer involved in large-scale data center projects, including partnerships with Google;[50]
- **Kuok Group (via K2 Strategic)** – Planning multi-billion-dollar investments in AI data centers;
- **Tenaga Nasional Berhad (TNB)** – Malaysia's national power utility and a key provider of grid capacity and green energy solutions;
- Royal land authorities – Holders of strategic land banks, particularly in Johor.

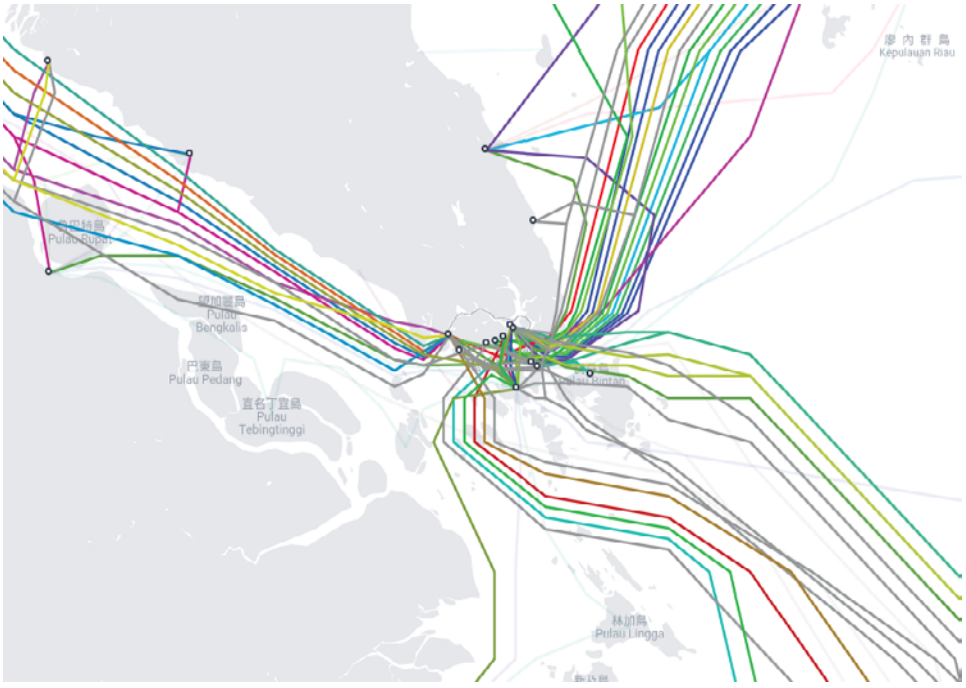
In Singapore, Jurong Town Corporation (JTC) oversees industrial land zoning, including data center-specific parks, while SP Group manages the national power grid and energy delivery systems.

The map in Figure 6 highlights the locations of publicly known AI data center clusters that are rapidly developing in Johor, Malaysia—including Sedenak Tech Park, Nusajaya Tech Park, and the YTL (Kulai)—as well as their proximity to major border checkpoints. The clustering of these AI infrastructure sites underscores the region's strategic significance as a cross-border data hub and a key node for managing geopolitical risks in the global technology supply chain.

Figure 6. Distribution of Publicly Known AI Data Center Clusters in Singapore and Johor, Malaysia

Source: Financial Times [51]

Figure 7. Distribution of Submarine Communication Cables Passing Through Singapore



Source: submarinecablemap

The map in Figure 7 illustrates the 41 submarine communication cables—existing, planned, and under construction—that pass through Singapore. The dense concentration of these cables highlights Singapore's critical role as a global hub for internet data transmission. Its strategic location makes Singapore the most interconnected node in Southeast Asia, underpinning the region's cloud computing, AI data centers, and international data sovereignty.

2. Construction and Engineering Contractors

This segment includes civil works, structural design, and the installation of power and cooling systems. Given the unique demands of hyperscale AI workloads, high-density compute environments require specialized engineering. Key contractors include:

- **YTL Construction** – Experienced in large-scale infrastructure delivery;
- Gamuda Berhad – Recently secured a hyperscale data center contract with a Google subsidiary;[52]
- Lendlease,[53] **Samsung C&T**, and other Japanese/Korean firms – possess niche expertise in thermal management and modular data center engineering for regional projects.

3. Hardware Suppliers

The compute core of AI infrastructure is built on a global supply chain of advanced hardware. Major vendors include:

- **NVIDIA** – Dominant in AI training GPUs;
- **AMD** – CPUs and GPU accelerators;
- **Intel** – CPUs and AI-specialized chips;
- **Dell Technologies, Lenovo, and Gigabyte**– Providers of full-stack server and storage infrastructure;
- **Hewlett-Packard Enterprise (HPE)** and **Supermicro** – Key suppliers of enterprise-grade and AI-optimized server platforms.

These firms have extensive market penetration in both Singapore and Malaysia.

4. Systems Integrators and Managed Service Providers

This layer bridges hardware, software, and security. Core responsibilities include systems configuration, cloud orchestration, and cyber risk mitigation. Leading providers include:

- **NTT DATA (formerly Dimension Data)** – Offers integrated managed services and enterprise IT infrastructure;
- **Accenture, TCS, and Infosys** – Provide AI infrastructure transformation, hybrid cloud integration, and workload optimization;
- Regional and local firms also play roles in specialized or regulated sectors.

5. Data Center Operators

Operators ensure long-term uptime, physical and virtual provisioning, and tenant services. Prominent players include:

- **Equinix, Digital Realty** – Global colocation and interconnection providers with major campuses in Singapore and expansion plans in Malaysia;
- **ST Telemedia Global Data Centres (STT GDC)** – Singapore-based with a strong presence across Southeast Asia;
- **Keppel Data Centres, YTL Data Centre Holdings, and Time dotcom/AIMS** – Active local operators;
- **Telekom Malaysia (TM)** – National telecom with significant data infrastructure;
- **Princeton Digital Group (PDG) and Vantage Data Centers** – Newer entrants investing aggressively in hyperscale AI facilities.

6. Cloud and AI Platform Providers

Cloud hyperscalers and AI service platforms form the software-access layer for users of compute services:

- **Amazon Web Services (AWS)** – Recently announced a new AWS Region in Malaysia;
- **Microsoft Azure, Google Cloud and Oracle Cloud Infrastructure (OCI)** – Expanding regional availability zones and AI-native compute regions;
- **Alibaba Cloud, Huawei Cloud, Tencent Cloud**– Maintain or are expanding service footprints in the region.

These firms deliver Compute-as-a-Service (CaaS) and Platform-as-a-Service (PaaS), lowering entry barriers for AI users and enabling scalable AI model deployment without on-prem infrastructure.

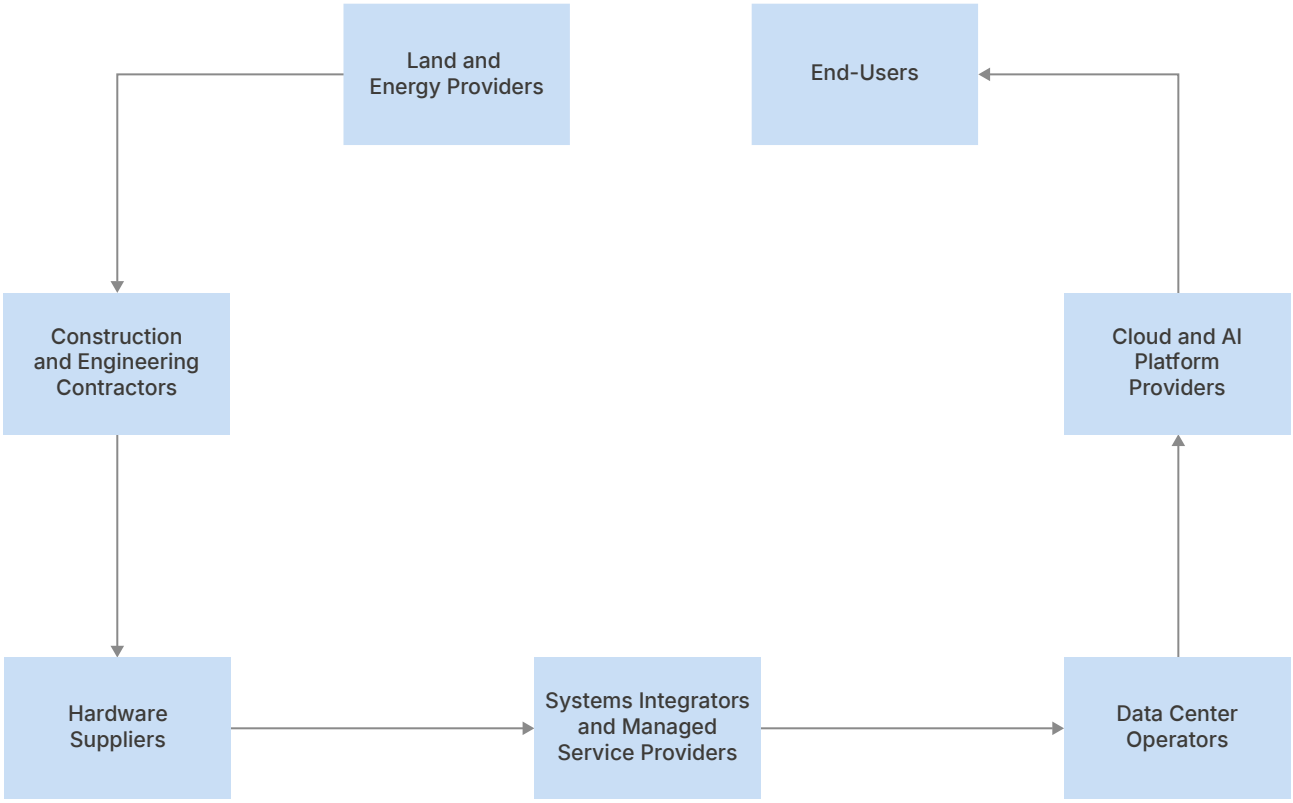
7. End-Users

The downstream beneficiaries of AI infrastructure include:

- **Semiconductor design firms** – Rely on high-throughput computing for simulation and verification;
- **AI startups** – Innovating in large language models, computer vision, and robotics;
- **Multinational corporations** – Leveraging AI across supply chains, automation, and enterprise analytics;
- **Government agencies** – Especially in defense, intelligence, and public health analytics;
- **Biomedical institutions** – Applying AI in genomics, diagnostics, and drug discovery.

The diverse composition of this user base illustrates the AI data center's foundational role in supporting national innovation systems and digital transformation agendas.

Figure 8: From Land to Compute: Sequential Roles in AI Data Center Supply Chain



Source: Author's illustration.

Conclusion

Taken together, these interconnected segments form a vertically integrated and globally entangled AI infrastructure ecosystem. Singapore and Malaysia have become indispensable strategic nodes in the global buildout of AI compute capability, occupying a frontline role in the geopolitical contest over technological infrastructure and data sovereignty. Figure 8 provides a visual representation of the seven sequential roles in this ecosystem.

Part 2: Infrastructure Models and Pathways of Chinese Infiltration in Singapore and Malaysia's AI Data Centers

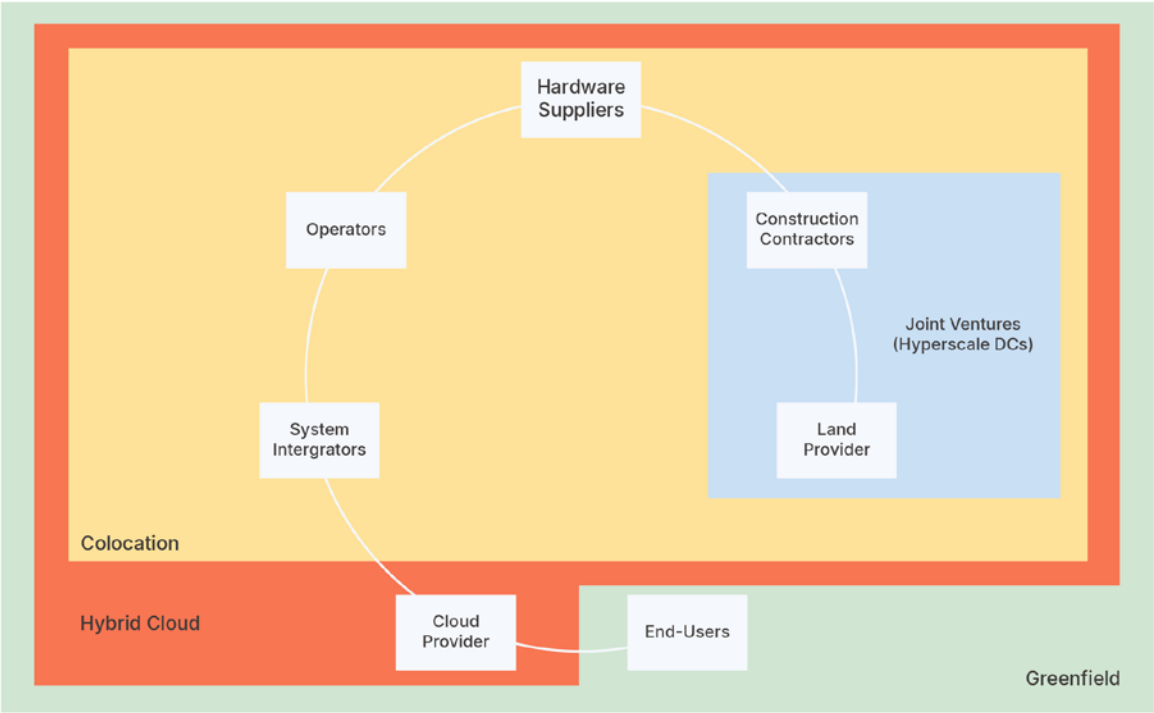
As AI infrastructure scales rapidly across Singapore and Malaysia, data center construction and operational models have become increasingly diversified. While both governments actively promote FDI as part of their national digital transformation agendas, their open investment environments—combined with strategic ambiguity in their diplomatic positioning—have inadvertently created pathways for Chinese firms to circumvent export controls and embed themselves in high-performance computing (HPC) infrastructure.

While a significant share of these facilities is led by companies aligned with democratic allies, the broader "non-alignment" posture in Southeast Asia has allowed Chinese or Chinese-linked firms to engage via diverse ownership structures and indirect channels.[54] [55] This section outlines four prevalent infrastructure models in the region—Greenfield (fully owned), Joint Venture/Partnership, Colocation, and Hybrid Cloud—and analyzes each model's associated risks, infiltration vectors, and challenges to auditability.

The following section defines these four deployment models and analyzes how each model's adoption shapes the industrial advantages of data center service providers in the Singapore–Malaysia region, as well as the associated security risks arising from varying levels of supply chain control. Figure 9 illustrates how operators exercise differing degrees of control across the seven key segments of the data center supply chain under each deployment model. Table 1 categorizes the four models according to their operational logic and representative firms. While each model lists specific exemplars, the accelerating demand for AI compute has compelled many providers to adopt multiple models simultaneously in order to achieve rapid market expansion.

This section will further discuss China's past deployments in this region and the potential strategies it employs to circumvent U.S. export controls, highlighting risks and loopholes in the current regulatory framework. For each model, concrete case studies are provided to illustrate how, in the context of the global AI boom, widespread investment in data center infrastructure may create possible pathways for China to acquire advanced computing power.

Figure 9. Illustration of Data Center Deployment Models and Supplier Relationships



Source: Author's illustration

Table 1. AI Infrastructure Deployment Models and Representative Companies

Model Type	Description	Representative Companies
Greenfield (Fully-Owned Deployment)	Data centers fully funded and built by parent firms; complete control from land to operations.	Microsoft, AWS, Google, Alibaba Cloud, GDS (Global Data Solutions), Mubadala Investment Company, Kuok Group (K2 Data Centres)
Joint Venture / Partnership	International and local firms co-invest, share operations, and combine land, power, and technical resources.	YTL/GDS, TM One/Singtel,[56] AIMS/ DigitalBridge(Strategic Partnership)[57]
Colocation (Rack Leasing)	Providers lease rack/cabinet space, power, and cooling; tenants bring their own servers.	Equinix, Yondr Group, Princeton Digital Group (PDG), Keppel Data Centres, NTT, Bridge Data Centres, AIMS(TIME dotCom)
Hybrid Cloud (On-Premise + Public Cloud Integration)	Mix of local/self-built infrastructure with public cloud platforms	Microsoft, AWS Outposts, Alibaba Cloud, Tencent Cloud, Huawei Cloud

Source: Author's illustration

Model 1: Greenfield (Fully-Owned Infrastructure)[58]

a. Deployment Logic and Definition

The Greenfield (fully-owned infrastructure) model refers to enterprises independently developing and operating new data centers (from land acquisition, design, construction, equipment procurement, to subsequent operations and maintenance), all under the complete control of the investor. This approach offers full customization, allowing organizations to design and build data centers to their exact specifications (including IT infrastructure and systems), unconstrained by existing layouts or locations. While it provides unparalleled control and optimization potential for specific AI workloads, it typically requires substantial capital investment and longer development cycles. For the investor, this model enables the highest level of operational autonomy, cybersecurity, and data sovereignty, making it particularly suitable for industries with extremely high data sensitivity requirements (such as finance, defense, and semiconductors), albeit with the highest capital requirements.

In terms of supply chain segmentation, the Greenfield model covers all seven major segments (1-7), granting the data center operator absolute control across the entire supply chain from land to end-user services.

b. Deployment Logic and Definition

Due to its vertical integration, the Greenfield model provides a secure foundation for constructing a trusted and auditable compute environment. Its operating principle is based on establishing a top-down Chain of Trust, where every hardware component, power module, and network element can be independently sourced and configured—excluding vendors from high-risk geopolitical backgrounds (e.g., China).

Building on this logic, the Greenfield model offers operators unparalleled visibility and control across all seven supply chain segments—from land acquisition to cloud services—ensuring a verifiable and sovereign infrastructure. To safeguard system integrity and data sovereignty, such facilities typically deploy servers equipped with Trusted Platform Modules (TPMs), complemented by internal audits and source code review procedures to prevent malicious firmware tampering or backdoor insertion.

Despite its design for security, the model remains vulnerable at the operational interface. External contractors, unvetted personnel, and diagnostic tool providers may introduce latent risks—making zero-trust operational policies and forensic readiness essential.

A representative example is Amazon Web Services (AWS), which operates its Singapore Region as a fully managed infrastructure comprising three independent Availability Zones. While it does not carry Uptime Institute Tier IV certification, its design meets or exceeds Tier III standards for redundancy and reliability. AWS also holds the highest-level MTCS (Multi-Tier Cloud Security)[59] Level 3 certification from the Singapore government, demonstrating robust governance in isolation, compliance, and risk management.

Another example is ST Telemedia Global Data Centres (STT GDC), which operates proprietary facilities across Singapore and other Southeast Asian countries. These centers are engineered for high availability and auditability, catering to clients in the semiconductor, biomedical, public, and cloud service sectors. Their architectures prioritize complete operational traceability and end-to-end physical and digital security.

c. PRC Circumvention Tactics and Export Control Challenges

Despite offering the highest degree of control over the supply chain, the Greenfield model's very strength in autonomy and verifiability has made it a prime target for Chinese firms seeking to bypass export controls. To circumvent U.S. restrictions on advanced GPUs (e.g., NVIDIA A100/H100, AMD Instinct), Chinese companies often establish proxy entities in jurisdictions such as Hong Kong or the Cayman Islands. These shell entities, disguised as neutral foreign investors, are used to gain access to Singapore and Malaysia—economies heavily reliant on FDI—for deploying "shadow Greenfield" operations that remain effectively controlled by Chinese parent firms (see Figure 10 for a schematic illustration of this model).

These facilities appear to be developed by third parties but are in fact operated under full Chinese control. They often avoid investment screening mechanisms, import restricted chips through transshipment hubs (e.g., Hong Kong, the UAE, or Southeast Asia), and connect back to China via encrypted channels (VPN or SD-WAN), forming a transnational "shadow compute cluster." These clusters are built to enable offshore AI model training and data processing, directly undermining the effectiveness of U.S.-led export control regimes.

Because such facilities are designed for internal use rather than public service, they do not issue press releases or list their clients—making them far harder to detect than the other three deployment models. Privately held or non-listed companies have no obligation to disclose ownership or clientele, while even publicly listed firms are generally not required to name their end users. Additionally, since these deployments do not involve cabinet rentals or public cloud services, they remain off the industry radar.

Furthermore, because the Greenfield model allows complete control over end-user relationships, Chinese firms or even local entities can collaborate discreetly with China-based tech companies under export restrictions, offering outsourced compute services or customized infrastructure deployment. Such arrangements—often undisclosed to the public—enable Chinese companies to access high-performance computing resources offshore while avoiding regulatory scrutiny. Multiple reports have indicated large volumes of NVIDIA GPUs being rerouted to Singapore and Malaysia, suggesting that these shadow Greenfield deployments may already be operating at scale across the region.[60] [61]

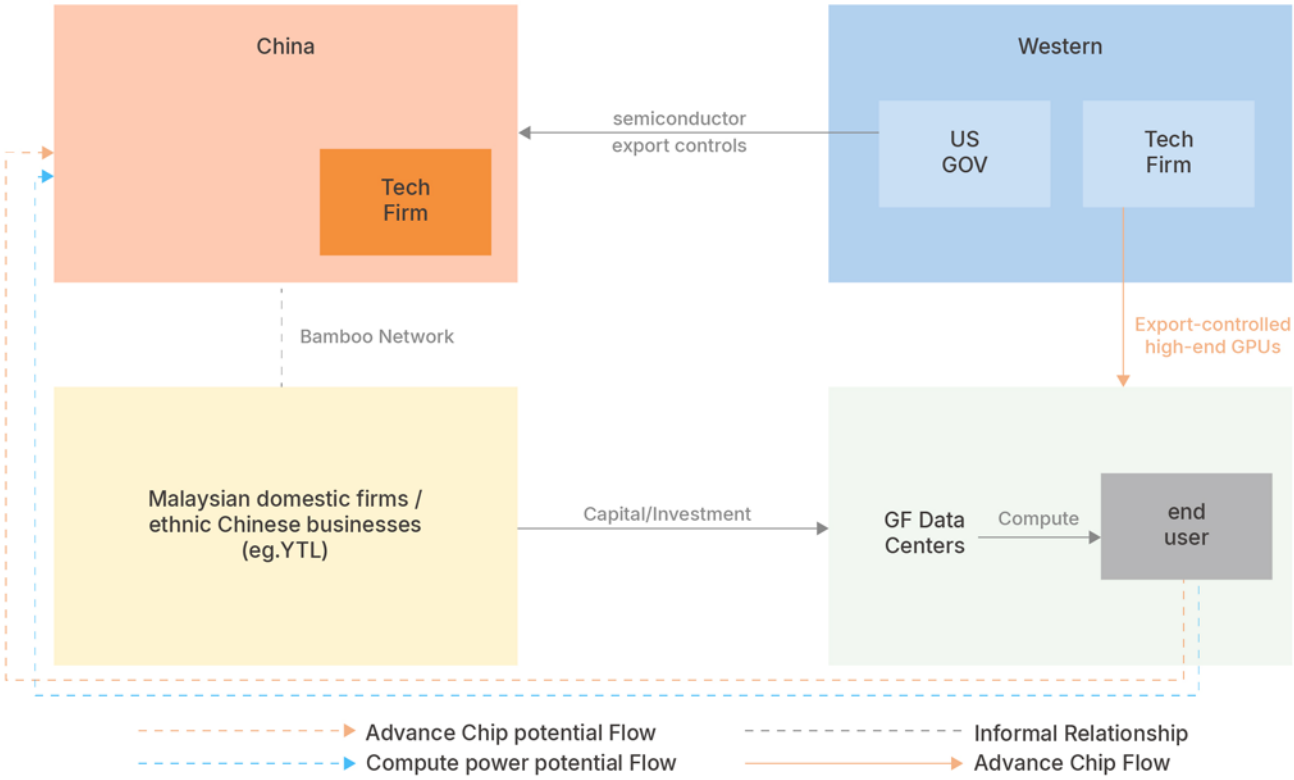
d. Case Example and Strategic Implications

In Malaysia, K2 Strategic Infrastructure (a wholly owned subsidiary of the Kuok Group) is constructing AI data centers via the Greenfield model.[62] Its clientele remains obscured from public view. Although there is no conclusive evidence linking K2 directly with Chinese tech firms, the Kuok Group has maintained longstanding and deep commercial ties with China. Its businesses—including Shangri-La Hotels, trading operations, and logistics ventures—operate extensively within mainland China. Ethnic Chinese business families such as the Kuoks have historically played pivotal roles in China's reform era, maintaining close connections with political and economic elites in Beijing. These families are often regarded as strategic commercial partners in China's engagement with Southeast Asia.[63]

Moreover, the Kuok family's prominence within the broader Bamboo Network—the transnational economic web of ethnic Chinese business elites across East and Southeast Asia—suggests an underlying framework of trust and social proximity with PRC-related actors.

As K2 operates privately and is not publicly listed, and as it does not offer colocated compute services, its user base and operational purpose remain largely invisible. In the absence of transparency mechanisms or beneficial ownership disclosure, such independently owned Greenfield facilities could be leveraged to bypass export controls and form "shadow compute clusters." Although there is no concrete evidence of misuse, these structural vulnerabilities warrant serious consideration in policy risk assessments.

Figure 10: Operational Logic of the Greenfield Model and Potential Flows of Chips and Compute Power to Circumvent Export Controls



Source: Author's illustration

Model 2: Joint Venture / Partnership[64]

a. Deployment Logic and Definition

The Joint Venture or Partnership model involves two or more entities—typically combining international cloud providers, AI infrastructure vendors, or hardware suppliers with local real estate developers, utility providers, or sovereign funds—to co-invest in, build, and operate data centers. Ownership, governance, and operational responsibilities are divided based on equity stakes or contractual agreements. This arrangement facilitates rapid market entry, cost-sharing, and localization of compliance and regulatory engagement.

While international partners bring technical know-how, proprietary technologies, and operational expertise, local partners contribute access to land, electricity, licenses, and political connections. However, because control is distributed, transparency and cybersecurity oversight may be uneven—particularly when one of the partners originates from a jurisdiction subject to export controls or cybersecurity concerns.

In terms of supply chain roles, the local partner often handles upstream components such as

land acquisition and construction (Segments 1–2), while the foreign partner controls mid- to downstream operations (Segments 3–6: hardware suppliers, systems integration, operator, and cloud services). Both parties may jointly coordinate end-user interactions and customer-facing services (Segment 7).

b. Operational and Security Risks under this Model

The primary advantage of the joint venture model lies in its regulatory agility and the ability to pool complementary resources. However, this benefit comes at the cost of fragmented operational control. When responsibilities are divided across entities, especially between international and local partners, decision-making over security-critical domains (such as hardware procurement, system architecture, and access management) can become misaligned or contested. This fragmentation limits visibility and assurance, complicating government oversight of compliance with export controls or national security mandates.

These risks are further amplified when one of the participating entities is linked to the PRC. PRC-affiliated firms may introduce remote diagnostics systems, backend access privileges, or firmware update channels into the data center architecture—potentially enabling unauthorized data access, AI model parameter exfiltration, or covert compute leasing. In certain instances, these embedded access vectors may persist without the knowledge of the local or foreign partner, particularly when infrastructure is co-managed without a centralized audit authority.

Furthermore, many joint ventures lack a unified security governance framework. Disparities in transparency levels, ambiguous contractual terms regarding data jurisdiction, access rights, and audit scope can create structural blind spots—undermining user trust and limiting effective state oversight.

Amid growing demand for AI infrastructure and an increasingly constrained global supply of high-performance compute, the joint venture model has become a favored approach for rapid deployment. To gain first-mover advantage, many hyperscale data center operators have formed partnerships with local firms to accelerate buildout. These arrangements allow international cloud providers and AI platform vendors to swiftly secure land, electricity, and regulatory clearances—streamlining deployment and reducing barriers to entry.

Representative examples include Singtel's joint venture with Malaysia's TM (Nxera) to develop a next-generation AI data center campus in Johor, integrating subsea cable and backbone network resources;[65] the 168MW AI data center park in Johor jointly developed by YTL Power International and China's GDS Holdings; and Time dotcom's partnerships with foreign vendors for AI infrastructure. In Singapore, ByteDance has also reportedly participated in data center development via third-party collaborations.[66] [67]

These cases illustrate how the joint venture model is increasingly adopted as a strategic response to urgent infrastructure needs amid the global AI compute race.

c. PRC Circumvention Tactics and Export Control Challenges

Amid ongoing geopolitical realignment and escalating export controls on advanced chips, Singapore and Malaysia—particularly Johor—have emerged as key nodes in the global redistribution of AI infrastructure. For U.S. companies, the region offers advantages such as lower land and electricity costs and a relatively facilitative regulatory environment, enabling expansion of cloud and AI services. For Chinese firms, facing increasing restrictions on accessing high-end GPUs within the mainland, Southeast Asia presents an attractive alternative deployment hub to sustain offshore AI development (see Figure 11 for a schematic illustration of this model).[68]

In this context, joint ventures and technical cooperation between local companies and PRC-linked firms have become mutually beneficial arrangements. Local partners typically provide access to land, power, and government channels, while Chinese firms contribute capital, technical expertise, and systems integration capabilities. These collaborations accelerate data center deployment and allow domestic firms to participate in the global AI supply chain, even without full control over critical technologies. At the same time, they offer Chinese entities a channel to maintain overseas deployment capabilities.

However, this model also carries significant structural risks. Despite legal ownership of infrastructure or procurement licenses resting with the local partner, critical technical control—including hardware sourcing, system architecture, cloud platform deployment, and backend operations—often remains with the Chinese side, either through internal technical teams or outsourced service providers. This creates structural asymmetry in the control of compute infrastructure, which (despite formal legal ownership) can in practice undermine local operational sovereignty and compliance assurance mechanisms. Furthermore, opaque contractual terms and equity structures often favor the Chinese partner, leaving local firms with limited oversight over core decision-making.

These arrangements also open potential backdoors for export control circumvention. While local firms may legally acquire advanced GPUs, the technical operation and maintenance are frequently handled by Chinese entities via remote access or outsourced compute-as-a-service models. In some instances, Chinese firms may indirectly gain access to restricted compute power, undermining the enforcement of U.S. export control policies. More alarmingly, there is growing concern that PRC-linked entities may exploit these partnerships to procure large volumes of GPUs through local intermediaries and reroute them back to China via smuggling or grey-market logistics.

For governments and end users concerned with cybersecurity and data sovereignty, such joint venture structures are particularly problematic. They enable Chinese firms to obtain legally acquired GPUs through joint venture partners and offer remote AI model training and inference services—effectively operating under a "Training-as-a-Service" model that bypasses export restrictions. In doing so, these structures challenge the effectiveness of the current international technology control regime and introduce vectors for illicit GPU acquisition by China through ostensibly compliant local entities.

d. Case Example and Strategic Implications

A clear illustration of the strategic and security implications of JV-based AI infrastructure is the collaboration between Malaysia's YTL Power International and China's GDS Holdings to develop a high-performance AI data center campus in Kulai, Johor, with a combined capacity of 168MW.[69] In this structure, YTL contributes local assets—land, energy, and regulatory facilitation—while GDS contributes operational and technical capabilities. Parallelly, YTL has entered into a partnership with NVIDIA (2023–2025) to deploy next-generation GPU architectures, including Blackwell Ultra, potentially becoming one of the first AI cloud services providers in Southeast Asia to do so.[70] [71]

SEA Group (the parent of Shopee) is reported as an anchor tenant, and given its historical early-stage funding from Tencent, this adds another layer of indirect PRC linkage to the consortium.[72] [73] This illustrates how, even where GPU procurement is legally executed by local entities, operational control—including deployment, maintenance, and AI workload orchestration—can effectively remain under PRC influence, enabling a 'soft infiltration' of compute capability.

This case underscores a loophole in U.S. export control enforcement: through JV structures, PRC-affiliated companies can access high-end compute infrastructure indirectly, bypassing controls centered on end-user identification and use restrictions. With key operational authority residing on the Chinese side and limited transparency in agreements, control of compute capacity may disproportionately favor PRC firms, posing grave national security and data sovereignty concerns.[74]

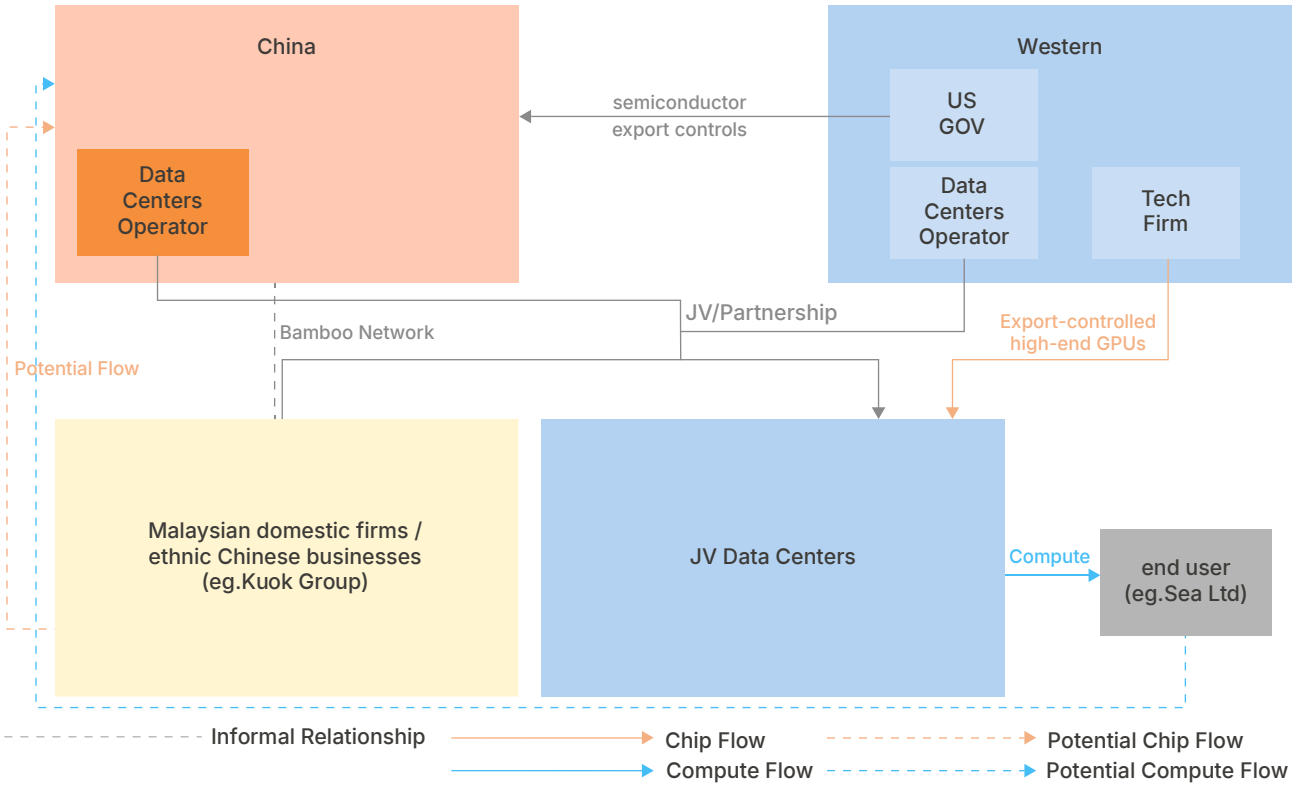
Model 3: Colocation[75]

a. Deployment Logic and Definition

For data center operators, the colocation model involves providing customers with secure, reliable rack space, power, cooling, and network connectivity, while maintaining control over the entire physical infrastructure and site operations. Customers are responsible for supplying and maintaining their own servers and IT equipment. This model allows service providers to diversify their client base and maximize facility utilization, while also developing value-added services such as cross-connects, real-time technical support, and compliance consulting. While the operator manages physical risks, information security and regulatory compliance are shared responsibilities with the customer.

In terms of supply chain roles, colocation operators' degree of control depends on their operating model (greenfield or joint venture), but typically covers segments 1-5 (land, construction, hardware, integration, operations). The IT/application layers (6-7: operations, cloud) are managed by customers themselves or via third-party cloud services.

Figure 11: Operational Logic of the Joint Venture Model and Potential Flows of Chips and Compute Power to Circumvent Export Controls



Source: Author's illustration

b. Operational and Security Risks under this Model

The colocation model offers a cost-efficient and scalable pathway for AI workloads, making it particularly attractive to small and medium-sized enterprises (SMEs), early-stage AI startups, and research institutions that lack the resources to construct dedicated facilities. It is also widely adopted for rapid deployment, prototyping, and hybrid cloud integration. While customers retain operational authority over their own equipment and compute resources, they remain dependent on the colocation provider for critical infrastructure services, including power distribution, cooling systems, physical access controls, building management systems (BMS), and network infrastructure.

Depending on the ownership structure of the facility—whether a fully-owned greenfield deployment or a joint venture—the colocation provider typically controls all infrastructure layers except for customer-owned servers and their associated cloud services. Since colocation services generally do not directly supply compute capacity, they pose a comparatively lower risk of high-end chip diversion under export control frameworks than greenfield or joint venture models. However,

insufficient due diligence on client onboarding can create opportunities for PRC-linked end users to colocate servers acquired through illicit channels, indirectly leveraging the provider's infrastructure to operate restricted compute workloads.

The more direct security concern arises when the provider is affiliated with PRC-linked entities or integrates Chinese-manufactured components—such as remote diagnostics tools, network switches, or firmware—into its core infrastructure.[76] In such cases, the risks of unauthorized remote access, embedded surveillance, or hardware-level compromise increase substantially. Without robust encryption, network segmentation, and inter-domain verification, misconfigured switches or software-defined networking (SDN) overlays could be exploited to intercept data flows, exfiltrate AI model parameters, or covertly replicate workload behavior.

In Singapore and Malaysia, leading colocation operators, including Equinix, Digital Realty, ST Telemedia Global Data Centres (STT GDC), Princeton Digital Group (PDG), and Vantage Data Centers, hold certifications such as ISO 27001, SOC 2, and MTCS. However, the depth of their supply chain security governance varies, making provider-specific provenance audits and risk assessments essential for customers with high data sovereignty and cybersecurity requirements.

c. PRC Circumvention Tactics and Export Control Challenges

Although the colocation model primarily involves leasing physical infrastructure—such as rack space, power, cooling, and network connectivity—without directly supplying compute resources, the risk of high-end chip diversion under export control frameworks is comparatively lower than in greenfield or joint venture models. However, PRC-affiliated firms often exploit the division of responsibilities in colocation ecosystems to reduce detection risk. This is achieved through layered cooperation among colocation operators, cloud service providers, and end customers, effectively masking the acquisition and use of advanced compute capacity (see Figure 12 for a schematic illustration of this model).

U.S. export controls on AI GPUs are designed to constrain or delay Chinese technology companies from enhancing military or other national-security-related capabilities through AI model training. Under the colocation model, PRC-linked operators can dilute these controls by separating hardware operations from infrastructure ownership. Furthermore, regulatory environments in Singapore and Malaysia do not restrict local end users from consuming cloud services offered by Western providers such as AWS, Oracle, or Microsoft, enabling Chinese technology firms to legally access AI-capable infrastructure and services via local hosting or cloud platforms.

In practice, PRC technology firms such as SenseTime and ByteDance may lease racks in colocation facilities through Southeast Asia-based subsidiaries or intermediaries, using

sites operated by international providers like Equinix, Digital Realty or DayOne (formerly the international business of GDS Holdings).[77] [78] Even when these clients manage their own hardware, supply chain vulnerabilities persist if the facility incorporates China-sourced components for power, cooling, or remote diagnostics, or if it lacks proper network segmentation and strict access controls—creating potential for dual-layer infiltration at both the physical and network levels.

d. Case Example and Strategic Implications

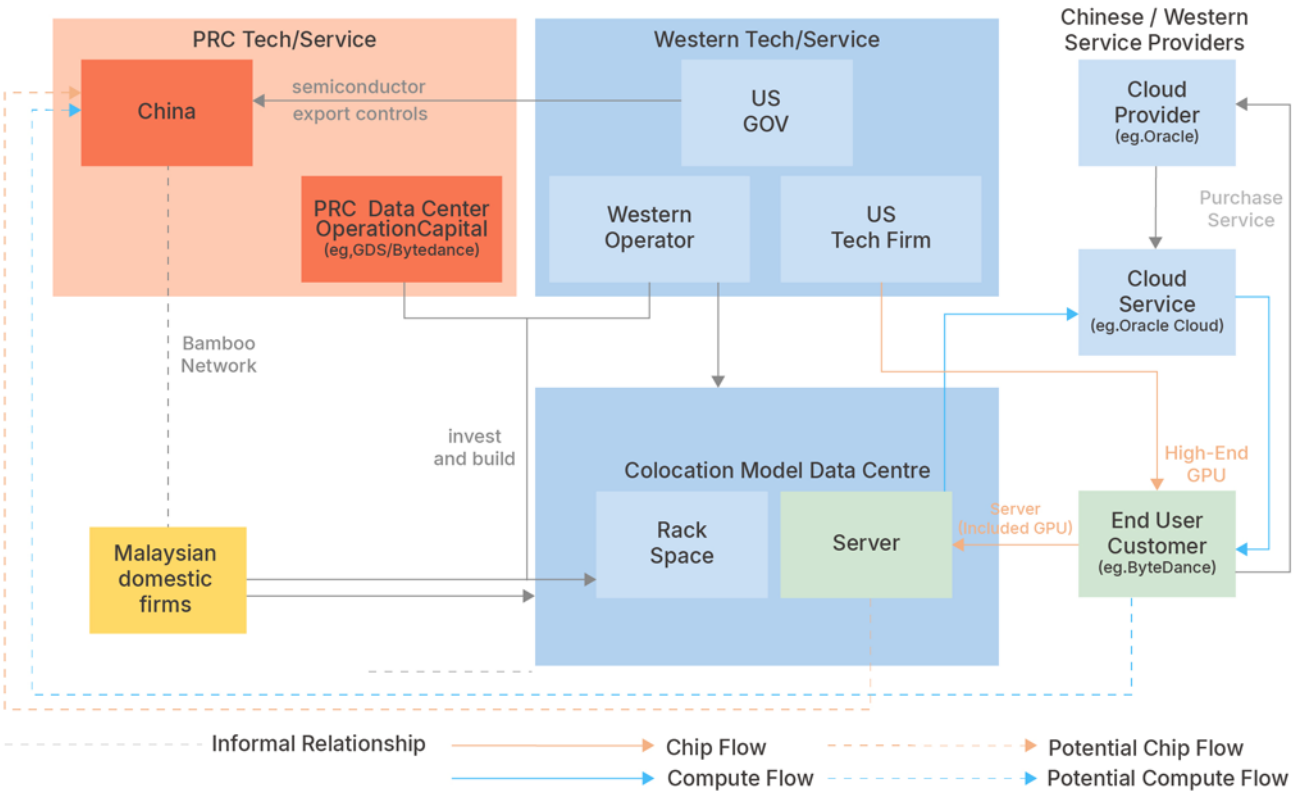
In a practical example of the colocation model, ByteDance has deployed compute infrastructure in Malaysia through both Day One Data Center and Bridge Data Centres, leveraging cloud services provided by Oracle. Bridge Data Centres, a subsidiary of Chindata Group, launched the first phase of its 110 MW hyperscale facility (MY06) in Johor's Sedenak Tech Park in 2022, with ByteDance serving as an anchor tenant.[79] GDS has since rebranded as DayOne and established a strategic partnership with Oracle, making Oracle its second-largest customer and positioning Johor and Batam as emerging hubs for AI cloud computing.[80] [81] In parallel, Malaysia's Minister of Investment, Trade, and Industry announced ByteDance's plan to invest approximately RM 10 billion (US $2.13 billion) to develop an AI hub in the country.[82]

Notably, ByteDance has also entered into a joint venture with Australian hyperscale provider AirTrunk to establish a data center in Singapore, and multiple reports have documented its attempts to acquire U.S.-restricted high-performance GPUs outside mainland China.[83] [84] This pattern illustrates how Chinese technology firms actively pursue diversified strategies—including cross-border partnerships and colocation arrangements—to circumvent export controls and secure AI compute resources.

From the perspective of U.S. export control policy, the primary challenge in the colocation model is that operators have limited visibility into the type and origin of GPUs installed within tenant-owned servers. Even if racks are leased to ostensibly compliant customers, there remains the possibility that they are controlled by PRC-affiliated entities or are indirectly providing compute power for Chinese technology firms. When the colocation operator itself is PRC-linked, or when its supply chain incorporates China-manufactured infrastructure components, the potential for exploitation increases—creating dual-layer infiltration risks spanning both the physical and network domains.

This case underscores that, amid the accelerating global AI infrastructure race, existing export control frameworks are insufficient to address scenarios in which restricted compute power is indirectly obtained via the colocation model. Without targeted policy interventions—such as mandatory disclosure of GPU inventories for colocation tenants, enhanced supply chain provenance checks, and tighter scrutiny of PRC-linked operators—this model may remain a primary channel through which Chinese technology firms secure advanced AI compute, undermining the strategic intent of U.S. technology containment policies.

Figure 12: Operational Logic of the Colocation Model and Potential Flows of Chips and Compute Power to Circumvent Export Controls



Source: Author's illustration

Model 4: Hybrid Cloud[85] (Focus on Cloud Service Provider)[86]

a. Deployment Logic and Definition

In the hybrid cloud model, data center operations are primarily viewed from the perspective of cloud service providers (such as AWS, Google Cloud, Microsoft Azure, and Oracle Cloud), who own and operate globally distributed data centers, either greenfield or joint ventures. The provider maintains control over all hardware, networks, cybersecurity, and operations. Customers simply connect remotely to the cloud platform via the internet, accessing computing, storage, and AI services in any global region as needed. Typical client use cases include pure cloud deployments (where all IT workloads are run entirely on the cloud), or hybrid integrations (where local or colocated resources are maintained and securely connected to the cloud for collaborative computing, backup, or AI training).

From the perspective of supply chain roles, cloud service providers in the hybrid cloud model exercise high levels of control over segments 1-6 (from land to cloud), achieving a globally standardized operating model. Customers retain control only over their own data, applications, and workload configurations, while fully relying on the provider for the security and integrity of the underlying infrastructure.

b. Operational and Security Risks under this Model

Hybrid cloud architectures integrate locally deployed compute resources—whether self-built or leased—with public cloud infrastructure through a unified management interface. This setup enables organizations to retain sensitive data and mission-critical AI workloads within local or sovereign environments, while leveraging the scalability and elasticity of public cloud platforms for less-sensitive or high-volume tasks.

Operationally, this model depends on layered isolation and elastic scaling. Platforms such as AWS Outposts, Azure Arc, and Google Anthos allow standardized APIs and consistent governance policies across hybrid environments. Software-defined networking (SDN) and end-to-end encryption are typically used to secure cross-domain data transfers and synchronization. This approach is widely adopted in sectors that require both security and scalability, such as public services, healthcare research, advanced manufacturing, and financial technology.

However, precisely because this model balances security and scalability, the cloud service provider itself becomes a potential risk vector. The security implications differ significantly between Western-capital-backed and PRC-linked providers. Public cloud services draw on computing resources deployed in data centers worldwide; if the provider has PRC ownership (such as Alibaba Cloud, Huawei Cloud, or Tencent Cloud) or operates data centers within China, it becomes subject to China's Data Security Law, under which such providers could be compelled to transfer foreign user data to Chinese authorities.[87]

c. PRC Circumvention Tactics and Export Control Challenges

In the hybrid cloud model, PRC circumvention of export controls primarily follows two pathways.

First, PRC-linked cloud service providers operating in Singapore and Malaysia can deliver local hosting or infrastructure services where data is nominally stored domestically, yet core cloud platforms remain under PRC control. This allows China to potentially access critical datasets for AI model training through these providers, even when the underlying infrastructure is locally sited or operated via greenfield or joint venture facilities (see Figure 13 for a schematic illustration of this model).

Second, because GPU export controls are largely enforced based on end delivery within China, PRC technology firms requiring significant training compute can instead deploy infrastructure abroad and openly consume Western cloud services to conduct high-performance AI model training. These two routes demonstrate that current control regimes—focused solely on the final sale location of advanced chips—are increasingly ineffective in constraining PRC access to AI compute.

In practice, PRC firms may lease public cloud compute resources from AWS, Microsoft Azure, or Google Cloud via Singapore- or Malaysia-registered subsidiaries, integrating them with private nodes based on Anthos, Azure Arc, or OpenStack to form hybrid deployments.

Deployments on PRC-affiliated platforms (e.g., Alibaba Cloud, Huawei Cloud, Tencent Cloud) may introduce risks such as parameter synchronization, telemetry sent to China-based management consoles, or automatic backups to PRC servers.[88] [89] Under China's Data Security Law and related compliance mandates, such processes could erode effective data sovereignty and undermine the intended impact of export controls—often without the customer's explicit awareness.

d. Case Example and Strategic Implications

In a practical example of the hybrid cloud model, PRC cloud service providers such as Alibaba Cloud and Tencent Cloud have expanded aggressively overseas under China's "Digital Silk Road" strategy, embedding themselves into foreign AI ecosystems while meeting local regulatory requirements.[90] In the Gulf region, these providers have partnered with local stakeholders to develop "sovereign cloud" infrastructure that complies with data localization mandates, yet remains under PRC operational control. According to the Carnegie Endowment, this localized integration into the host country's political and economic environment allows PRC cloud platforms to reduce regulatory scrutiny abroad while sidestepping export control restrictions targeting China's AI sector.

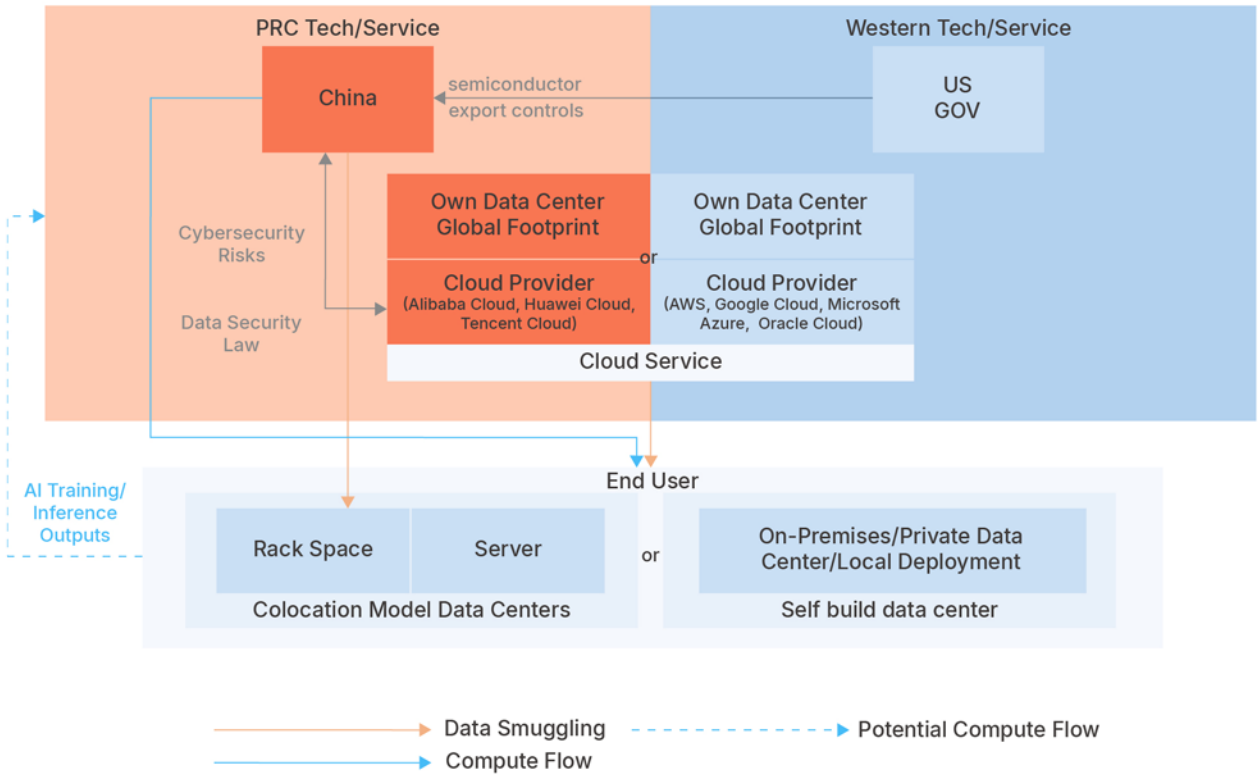
In Southeast Asia, similar dynamics emerge. PRC cloud providers have established or partnered in data centers in Singapore and Malaysia, marketing AI cloud services that appeal to both local enterprises and regional government agencies. The strategic risk lies in the fact that—even when infrastructure is

physically located outside China—these platforms may still be subject to China's Data Security Law if they are PRC-owned or operate facilities within Chinese jurisdiction, enabling potential remote access, parameter synchronization, or data transfers to PRC-based systems.

Conversely, PRC technology firms can also exploit the hybrid cloud model by deploying infrastructure abroad and consuming Western-capital-backed cloud services for AI model training. Recent reports have suggested that Chinese engineers may have physically transported storage media into Malaysia to bypass export controls, with investigations still ongoing into whether such practices were used to leverage locally hosted Nvidia-based compute resources for high-performance AI workloads.[91] As illustrated in the figure, the orange line depicts the suspected pathway of illicit data transfer. While such providers maintain rigorous supply chain security and compliance, they often lack granular vetting of end-user affiliations—allowing ostensibly legitimate customers to channel compute power toward PRC-linked AI development.

From the perspective of U.S. export control policy, the hybrid cloud model presents dual risk pathways: PRC-owned platforms using "localization" as a regulatory shield while retaining technical capabilities for backend data access, and PRC firms exploiting foreign cloud infrastructure beyond the geographic reach of current controls. Without targeted measures—such as cross-border audit frameworks, mandatory logging and transparency for cloud operations, and enhanced vetting of foreign tenants—these pathways will remain viable routes for PRC access to advanced AI compute, undermining the strategic objectives of technology containment.

Figure 13: Operational Logic of the Hybrid Cloud Model and Potential Flows Compute Power to Circumvent Export Controls



Source: Author's illustration

Summary

Table 2 compares the characteristics of each model. Greenfield provides the highest level of operational control, technological autonomy, and data sovereignty. However, as discussed earlier, local business ties with Chinese companies (such as through the bamboo network) may create "shadow Greenfield" risks, leading to leakage of restricted chips or compute power. Joint Ventures enable rapid market entry but involve governance ambiguities over operational control, and may be influenced by PRC equity stakes or backend technical access. Colocation offers cost efficiency and flexibility, but since tenants manage their own servers and cloudservices, it creates enforcement risks regarding chip and compute controls. Hybrid Cloud carries the highest exposure, as reliance on PRC cloud service platforms and cross-border data transfers may undermine sovereignty, while PRC firms have also smuggled hard drives abroad to exploit local hybrid cloud environments, effectively bypassing export restrictions.

Table 3 further contrasts the advantages of each model with its associated risks of advanced GPU and compute leakage. Greenfield ensures maximum sovereignty when using trusted hardware suppliers. Joint Ventures face elevated risks due to asymmetric control structures. Colocation, while suitable for inference workloads by offering hosting space for tenant servers, is highly vulnerable to hidden backdoors, third-party access, and blurred responsibility for client usage oversight. Hybrid Cloud provides elastic compute integration, but when PRC cloud platforms are involved, workloads are subject to China's Data Security Law and cross-border compliance mandates, which extend Chinese jurisdiction to training and inference data.

Overall, this study demonstrates that across all four models, Chinese firms retain concrete pathways to circumvent U.S. export controls on advanced GPUs, including:

- Establishing "shadow Greenfield" sites via offshore shell companies to directly import restricted chips;
- Using Joint Ventures to gain indirect access to legally procured GPUs and deliver compute-as-a-service to PRC entities;
- Exploiting Colocation by embedding PRC tenants or hardware in multi-tenant facilities, masking GPU usage behind international operators;
- Leveraging Hybrid Cloud, both through PRC cloud platforms compelled by Chinese data laws and through offshore subsidiaries openly renting Western cloud services for AI training.

In short, while each model provides distinct operational benefits, their structural vulnerabilities collectively give Beijing multiple avenues to sustain offshore AI development, thereby undermining the effectiveness of U.S.-led semiconductor export controls. This conclusion sets the foundation for the next chapter's policy recommendations, which will propose actionable measures to mitigate these infiltration risks.

The following table summarizes the comparative features of the four models:

Table 2. Comparative Features of Four Deployment Models

Deployment Model	Operational Control	Data Sovereignty	Technological Autonomy	Linkage to PRC Supply Chain	Primary Risk Vectors	Overall Risk Level
Greenfield (Fully-Owned)	High	High	High	Low (but shadow operations via bamboo network possible)	Insider threats, proxy shell firms	Low to High
Joint Venture / Partnership	Medium	Medium	Medium	Medium to High (depending on partner)	PRC equity/ technical influence	Medium to High
Colocation (Rack Leasing)	Low to Medium	Low to Medium	Low to Medium	Variable	Tenant misuse, hidden supply chain	Medium
Hybrid Cloud (On-Prem + Public Cloud)	Medium to High (local only)	Medium to Low (cross-border transfers)	Low to Medium (public cloud dependency)	Low to High (PRC cloud platforms, DSR compliance)	Data law exposure, drive smuggling, API leakage	High

Source: Author's compilation

Table 3. Comparative Strengths and Leakage Risks

Deployment Model	Advantages	Risks of Advanced GPU / Compute Leakage
Greenfield	• Full sovereignty & control • Suitable for sensitive workloads	• Shadow facilities via shell firms • Insider O&M risks
Joint Venture	• Fast market entry • Easier land/power access	• Asymmetric control favoring PRC • Backend access, covert GPU redirection
Colocation	• Lower CAPEX • Quick scaling • Flexible for SMEs	• PRC tenants masking usage • Backdoors & third-party access risks
Hybrid Cloud	• Easier land/power access • Integrates local + cloud resources	• PRC cloud providers under Data Security Law • Cross-border leakage • Drive smuggling cases

Source: Author's compilation

Section IV: Policy Recommendations– Enhancing AI Infrastructure Trust and Supplier-side Supply Chain Integrity

Recent policy reports[92] and governmental announcements[93] on American AI capabilities have all recommended more investments and policy coordination in AI infrastructures (including other broad-based infrastructures like energy supplies) and AI innovations. Moreover, the AI Action Plan has also established a pillar on strengthening AI diplomacy and security through tariffs, export controls, and standardization. These recommendations were built on strengthening U.S. domestic capabilities and less on countering China's global strategies, which include acquiring advanced computing power, accessing global data flows from particularly Southeast Asian countries,[94] and meeting the needs of other non-aligned countries. We recommend policies to address the policy goal of expanding U.S. global leadership, and we offer more insights on constructing AI diplomacy and security with non-aligned countries in practical and meaningful ways.

To address scenarios where Chinese entities may exploit Southeast Asian AI infrastructure to bypass export controls, access high-end compute, or transfer sensitive capabilities, democratic nations and their technology partners must reinforce their regulatory, audit, and investment frameworks, building a verifiable AI infrastructure network with trusted global suppliers. Below, we suggest three policy areas that would require more overhaul:

1. Establishing Rules for Verifying Data Centers and Determining Their Access to GPUs and Computing Power

The source of risks from our case study is from the complex ways of collaboration between U.S., Malaysian, and Chinese firms. These collaborations are necessary for Malaysian firms to ensure upstream suppliers in the supply chain, but Chinese firms can possibly leverage their Malaysian partners to access restricted chips and computing power. As a result, this creates different levels of risks far beyond the traditional view that concerns buyers and end-users and their access to computing power.

Malaysian firms, such as YTL, can pursue joint ventures with leading U.S. firms and Chinese firms at the same time, highlighting the need for broader verification mechanisms. We also see that using the model weight and source code as the subject for export controls can ironically lead to China's leading role in open-source models.

We suggest that U.S. policymakers should lean more into U.S. leadership on advanced GPUs and design new verifying mechanisms to ensure the transparency of data centers beyond their users and disclose the ownership structure, hardware supply chains, compute density, and others.

a. Establish a "Trusted AI Infrastructure Whitelist Program"

Modeled on the U.S. BIS OSAT whitelist system (2025), this program would establish a certification process for AI data center operators, evaluating ownership structures, hardware supply chains, personnel vetting, and data sovereignty protocols.

b. Define a "Safe Compute Density Threshold (CDI)"

A "Compute Density Index" (CDI) should be introduced to quantify the available high-performance GPU density per unit time. Deployments below a defined threshold may be exempt from controls; those above must report end-use declarations and architectural disclosures.

c. Expand Critical Infrastructure Protection (CIP) to Overseas Data Centers with U.S. Involvement

The U.S. has the extraterritorial authority to access data stored in foreign countries via the CLOUD Act, and it has also designated data centers as critical infrastructures via the Executive Order 14117; however, they tend to focus on data security rather than the protection of the infrastructure as a whole.[95] On the other hand, Malaysia has established its Cyber Security Act in 2024, which creates more protection of national critical information infrastructures (NCII) that are either wholly or partially in Malaysia through licensing processes.[96] We suggest that the U.S. should also expand its CIP policy to establish extraterritorial authority over overseas data centers with U.S. involvement over a certain de minimis level in the supply chain as a legal basis for interventions.

2. Strengthening the Capacity for Investigating and Prosecuting Indirect Transfers through Unlisted Foreign Entities.

As AI infrastructure development becomes more complex, we also call for the need to strengthen investigation, auditing, and prosecution against indirect transfers. Aforementioned examples of the whitelist program and CDI can serve as the baseline to include unlisted foreign entities under the scope of regulations, and once data centers and AI firms exceed those baselines, more mechanisms are required to enforce the rules. These mechanisms can help illuminate the operations of data centers, including the declarations for end-use and end-users, temporary general authorization codes, and chip tagging. Organizationally, besides increasing BIS's capacity, we also suggest that the Justice Department should play a more significant role, including its National Security Division, and the redirection of the newly announced corporate enforcement framework.

Besides relying on U.S. export controls and the FDPR rules, various Asian countries have taken different measures toward investigating AI chip control breaches and prosecuting invalid buyers.[97] For example, Taiwan has largely followed U.S. export control regulations,

including the Commerce Control List and Entity List. Taiwan's Ministry of Justice Investigation Bureau (MJIB) has conducted hundreds of investigations, searched and prosecuted Chinese shell companies that illegally poached the Taiwanese semiconductor industry.[98] Previously, DSET reports have demonstrated various poaching strategies, including setting up shell companies that posed as foreign firms or through management consulting firms, and hiring Taiwanese engineers to manufacture chips without relocation.[99] In response, Taiwanese MJIB has expanded its scope to target these known Chinese poaching strategies.[100]

The Singaporean government, on the other hand, has not adopted export controls that are more aligned with the U.S., but it has investigated several chip smugglers using fraudulent and false representations as well as issued a new advisory on encouraging firms' internal compliance and legal expertise.[101] The Malaysian government announced in July that it will require export licenses for advanced AI chips of U.S. origin and will work with other countries to block illegal flows of AI chips. Since this report focuses on policies that can be adopted by the U.S. and allies, we recommend policies that can be either imposed by the U.S. unilaterally or through bilateral or multilateral agreements.

a. Require "High-Performance Compute Use Declarations (HPC-UD)"

Deployments exceeding CDI thresholds should be required to file end-use declarations specifying workload type (inference/training), end-user sector, and sensitive domain involvement (e.g., defense, chip design). Temporary General Authorization Codes (TGAC) may be granted based on risk tiering.

b. Expand "Verifiable Compute Chip Tagging (VCCT)"

Building on FDPR and EAR §734.9, each advanced GPU should carry a unique CHIP ID, paired with cloud-based verification servers to enable periodic synchronization and global traceability of compute flows. This also aligns with the current proposal of the Chips Security Act that aims to add "chip security mechanisms" to all export-controlled chips.[102] CHIP ID can deter foreign adversaries from buying the advanced chips[103] while allowing better security checks on foreign data centers and critical information infrastructures.

c. Strengthening Customs to Synergize Inspections on High-end SSDs

To counter the recent waves of Chinese engineers physically bringing in hard drives and data storage devices to data centers with access to advanced chips,[104] more efforts are needed to synergize customs inspections. One possible and practical solution is to require the U.S. and Southeast Asian customs to have more stringent inspections on high-end SSDs.

Although HDDs are common, the growing HDD capacity combined with the stagnation of throughput means that the performance of HDDs is decreasing, resulting in more data centers shifting to SSDs, particularly high-end multilayer SSDs for their large capacity and performance.[105] More data centers and AI infrastructures would use triple-level (TLC) or quad-level cell (QLC) SSDs, and we recommend that customs inspections prioritize these high-end data storage devices to capture the training of large-scale models.

3. Launch the "AI Infrastructure Partnership Framework 2.0"

Following the operational challenges and diplomatic backlash associated with the now-withdrawn AI Diffusion Rule (ADR)—which risked isolating the United States from key regional partners—a renewed cooperative framework is needed to advance aligned interests. We suggest that the U.S. should lead a new **AI Infrastructure Partnership Framework 2.0**, designed to **re-engage allies and non-aligned actors** and construct a **democracy-aligned AI supply chain ecosystem** through strategic technology coordination and geopolitical trust-building.

In the last few years, the U.S. has been less successful in building closer economic ties with allies and non-aligned countries. The U.S. has employed more unilateral controls over the last five years, while also achieving some multilateral controls with key allies. Additionally, it has attracted key firms to invest in the U.S. reindustrialization efforts; however, other multilateral economic frameworks have faced greater challenges. For example, the Indo-Pacific Economic Framework (IPEF) aims to foster economic cooperation with allies and non-aligned countries in the Indo-Pacific region, departing from the traditional model of free trade agreements. However, IPEF faces challenges in delivering substantive benefits to participating countries in terms of labor, resilience, or economic transformation. Regarding Southeast Asia, the case of IPEF shows that the U.S. has not yet come to a coordinated strategy to engage with Southeast Asian countries and counter China's growing influence, primarily due to the varying goals of different countries.[106]

The AI Infrastructure Partnership Framework 2.0 will focus on a specific industry and a targeted set of participants. Although the U.S. holds advantages in the AI industry due to its advanced chips and computing power,[107] it needs to engage with other countries and effectively leverage their strengths. Southeast Asian countries and their strength in AI infrastructures, combined with advanced chips and supply chains in the U.S. and allies, will be a better model of global leadership.

With the aforementioned validation mechanisms in place, the AI Infrastructure Partnership Framework 2.0 should build on several collaborative mechanisms and encourage deeper cooperation. Trusted Southeast Asian countries that follow U.S. regulations, such as the Executive Order of **Promoting the Export of the American AI Technology Stack**, can **receive more U.S.-licensed technologies, engage in more meaningful global talent exchanges with the U.S. and allies, and enjoy opportunities for technological applications, economic**

upgrading, and industrial transformation through collaborating with U.S. standards. Strategically, this framework will also synergize the U.S., Indo-Pacific allies, and Southeast Asian countries in countering China's tactics in the region, providing the economic basis for political will and resilience.[108]

This framework aims to:

• Encourage trusted partners in Southeast Asia, the Indo-Pacific, and Europe to adopt U.S.-licensed technologies as the foundation for their AI data center ecosystems;

• Promote cross-border interoperability standards, cloud KYC protocols, and compute registration mechanisms;

• Isolate PRC-linked compute infrastructure by creating a trusted infrastructure club, in which access to advanced AI capabilities is conditional on transparent and secure infrastructure participation.

The Trump Administration has forcefully used unilateral tariffs to return to the negotiation table, including traditional U.S. allies and other non-aligned actors. We suggest that a new framework on AI and AI infrastructure can be the carrot that hangs in front of the stick or all the aforementioned mechanisms, effectively using U.S. leadership on advanced GPUs to ensure the upgrading of other non-traditional allies and non-aligned actors, luring them into buying into U.S. regulations. Rather than mandating compliance, this framework operates through positive incentives and conditional integration—a blend of technological carrots and strategic sticks—to attract undecided nations and counter PRC influence through value-aligned infrastructure development.

Summary

The outlined policy tools form a layered strategy to secure the integrity of global AI infrastructure in the face of regulatory blind spots and geopolitical exploitation. By combining technical safeguards (VCCT, CDI, HPC-UD, high-end SSD inspections) with governance mechanisms (whitelist certification, cross-border standards, extraterritorial authority on critical infrastructure protection), and embedding them within an inclusive yet exclusive multilateral framework (AI Infrastructure Partnership Framework 2.0), democratic nations can create not only resilient supply chains but also a values-based alliance for next-generation compute governance. This approach strengthens trust, reduces the strategic ambiguity exploited by authoritarian regimes, and restores agency to nations seeking secure digital development pathways.

References

1. Lehdonvirta, V., Wú, B., & Hawkins, Z. (2025). Weaponised interdependence in a bipolar world: how economic forces and security interests shape the global reach of US and Chinese cloud data centres. *Review of International Political Economy*, 1–26. https://doi.org/10.1080/09692290.2025.2489077

2. Chew, A. (2025, May 28). Gulf states, China take centre stage at summit of Southeast Asian nations. *Al Jazeera.* https://archive.ph/HLpEp

3. Xinhua. (2025, April 9). Xi calls for building community with shared future with neighboring countries. *Xinhua.* https://archive.ph/JZdtq

4. Kuik, C.-C. (2024, July 8). Tilting toward Beijing? Malaysia's relations with China after Li Qiang's visit. *Carnegie China.* https://carnegieendowment.org/research/2024/08/tilting-toward-beijing-malaysias-relations-with-china-after-li-qiangs-visit?lang=en&center=china

5. Carnegie China. (2025, April 23). 2025 Carnegie global dialogue: China and Southeast Asia. *Carnegie Endowment for International Peace.* https://carnegieendowment.org/events/2025/04/2025-carnegie-global-dialogue-china-and-southeast-asia?lang=en&center=china

6. Chowdhury, A., & Mavrotas, G. (2006). FDI and growth: What causes what? *The World Economy, 29*(1), 9–19. https://doi.org/10.1111/j.1467-9701.2006.00755.x

7. Al Mayadeen English. (2025, April 17). China-Malaysia $22bln tech park deal boosts industrial cooperation. *Al Mayadeen* English. https://archive.ph/MCsHk

8. Malay Mail. (2025, April 17). What's in the Malaysia-China MOUs on emerging tech, satellite navigation. https://archive.ph/20jN4

9. Malay Mail. (2025, April 17). From AI to satellites: What's in the 31 Malaysia-China MOUs inked during Xi Jinping's visit. *Malay Mail.* https://archive.ph/skU84

10. Mallapaty, S. (2025, June 9). How China is vying to attract the world's top scientific talent. *Nature*. https://archive.ph/mzidw

11. Ministry of Digital. (2025, April 17). Malaysia ties up with China's National Development and Reform Commission to strengthen AI, digital economy [Press release]. https://archive.ph/nf5Te

12. Sharon, A. (2025, April 17). Driving digital growth: Malaysia's partnership with China. *OpenGov Asia.* https://archive.ph/MqrXv

13. Wong, Y. X. (2025, May 21). Malaysia says Huawei-linked AI project not government-backed. *MarketWatch.* https://www.marketwatch.com/story/malaysia-says-huawei-linked-ai-project-not-government-backed-af58c1ad

14. ICEF Monitor. (2025, March 27). Full-year data highlights decline in foreign enrolment in UK universities in 2023/24. *ICEF Monitor*. https://archive.ph/hpzdX

15. Australian Government Department of Education. (2025, June 15). International student numbers by country, by state and *territory. Australian Government Department of Education.* https://archive.ph/OLtUn

16. Hassan, H. (2024, September 1). More Malaysians flocking to China's universities, drawn by affordability and growing prestige. *The Straits Times.* https://archive.ph/VMDAE

17. Reuters. (2025, May 21). China, ASEAN complete negotiations on upgraded free trade deal. *Reuters.* https://archive.ph/xdfII

18. Chen, A. (2025, April 21). China's CNOOC agrees LNG deal with UAE's Adnoc amid tariff war with US. Reuters. https://archive.ph/MGkjV

19. Saw, R. (2023, October 19). Intel Malaysia: From a muddy paddy field to a manufacturing powerhouse. *SoyaCincau.* https://archive.ph/dJznX

20. Lim, B., & Stoiber, H. (n.d.). Silicon Malaysia. *IEEE Semiconductors*. https://archive.ph/VEAQt

21. InCorp Content Team. (2025, July 7). Beyond borders: Looking at the Singapore free trade agreements. *InCorp Asia.* https://archive.ph/GAmIG

22. PSA Singapore. (n.d.). *Our story.* https://archive.ph/BcN1u

23. Nguyen, M. (2023, June 22). Vietnam can draw upon Singapore's successful foreign investment attraction policies as a reference for experience and potential solutions. HMLF Law Firm. https://archive.ph/cu5eX

24. Zhang, Y. (2023, September 6). Due to land constraints, environmental and energy considerations in Singapore, Malaysia has become a new target for foreign investment in data centers [由於新加坡土地限制、環境及能源考量等因素，馬來西亞成為外資投資資料中心之新目標]. *Bureau of Foreign Trade, Ministry of Economic Affairs.* https://archive.ph/MbIkW

25. Chin, S. F. (2025, January 7). S'pore, Malaysia sign agreement on Johor-S'pore Special Economic Zone; 20,000 jobs to be created. *The Straits Times.* https://archive.ph/Ro8I4

26. Walker, O. (2025, January 21). Malaysia ties fortunes to Singapore as US-China tensions mount. *Financial Times.* https://archive.ph/xzg7f

27. TeleGeography. (n.d.). *Singapore: Submarine cable map. SubmarineCableMap.com.* https://archive.ph/tEhIL

28. Datacenter Map. (n.d.). *Datacenter Map.* Retrieved August 29, 2025, from https://www.datacentermap.com/

29. Datacenter Map. (n.d.). *Datacenter Map.* Retrieved August 29, 2025, from https://www.datacentermap.com/

30. General Office of the State Council. (2006, March 15). Better implementation of the "Going Out" strategy [更好地實施「走出去」戰略]. *The Central People's Government of the People's Republic of China.* https://archive.ph/9ryd

31. Suzhou Industrial Park Administrative Committee. (2025, March 19). *Introduction to the park.* Suzhou Industrial Park Tech Pioneers. https://archive.ph/AMOw5

32. People's Daily Online. (2022, November 25). Livable, business-friendly, and tourist-friendly: China–Singapore Tianjin Eco-city [宜居宜業宜游 中新天津生態城]. *People's Daily Online.* https://archive.ph/v8282

33. Chongqing Municipal Commission of Commerce. (n.d.). Key project information [重點項目資訊]. https://archive.ph/YzR21

34. Huangpu Media. (2024, December 17). Sino-Singapore Guangzhou Knowledge City: Advancing with innovation and openness. *Guangzhou Municipal Government.* https://archive.ph/PLBCo

35. Sukumaran, T. (2020, November 17). Did a Belt and Road project in Malaysia just crash and burn? *South China Morning Post.* https://archive.ph/iUJc1

36. Liu, H., & Guan, K. (2025, April 16). China and Malaysia jointly build a high-quality Belt and Road flagship project [中馬打造高質量共建「一帶一路」旗艦項目]. *CPC News Online.* https://archive.ph/sNhT2

37. Tham, S. Y. (2024, February 15). The return of Melaka Gateway: Scaled-down ambitions. *Fulcrum.* ISEAS – Yusof Ishak Institute. https://archive.ph/BqtKH

38. Zhang, Y. (2024, June 24). Chinese Premier Li Qiang begins a three-day official visit to Malaysia on June 18, 2024 [中國總理李強於 2024 年 6 月 18 日對馬來西亞展開為期 3 天工作訪問]. *Bureau of Foreign Trade, Ministry of Economic Affairs.* https://archive.ph/0J8VQ

39. *Highlights: Trump imposes vast global tariffs. (2025, April 2).* https://archive.is/IgTds#selection-4379.0-4379.45

40. De, C. (2025, April 14). As U.S.–China rivalry intensifies, Xi Jinping visits three Southeast Asian countries [中美博弈加劇之際習近平出訪東南亞三國] [Republished from Deutsche Welle (Chinese)]. https://archive.ph/GA5bd

41. Yang, Y., Liu, H., & Li, X. (2025, April 14). A new chapter in China–Malaysia "Two Countries, Twin Parks" cooperation [中馬「兩國雙園」合作譜新篇]. CPC News Online [Republished from *People's Daily Online*]. https://archive.ph/2wRDM

42. People's Daily (People's Daily Online). (2025, April 18). Joint statement between the People's Republic of China and Malaysia on building a high-level strategic China–Malaysia community with a shared future [中華人民共和國和馬來西亞關於構建高水平戰略性中馬命運共同體的聯合聲明]. CPC News Online. https://archive.ph/rZWMp

43. Walker, O., & Russell, A. (2025, March 24). Malaysia to crack down on Nvidia chip flows under US pressure. *Financial Times.* https://archive.ph/XSSgm

44. Chen, W. (2025, May 22). Tech war: Malaysia walks back from AI project with Huawei as tech giant denies chip exports. *MyNews.* https://archive.ph/L61ul

45. Wang, T.-Y., & Chiang, M.-Y. (2024, December 18). *Uncovering Huawei's shadow network: Shenzhen Major Industry Investment Group and Taiwanese suppliers in China's semiconductor strategy.* Research Institute for Democracy, Society and Emerging Technology. https://dset.tw/en/research/uncovering-huaweis-shadow-network/

46. Chang, J. C.-C., Lin, H.-T., Wang, T.-Y., Chiang, M.-Y., Cheung, S., Wei, C.-A., Chou, Y. N., Hung, J., & Wu, C. (2025, April 1). *The great siege: The PRC's comprehensive strategy to dominate foundational chips.* Research Institute for Democracy, Society and Emerging Technology. https://dset.tw/en/research/the-great-siege/

47. Chiang, M.-Y. (2024, August 27). *The remote poaching model: How China's Bitmain acquired Taiwan's edge AI chip technology and its implications for economic security.* Research Institute for Democracy, Society and Emerging Technology. https://dset.tw/en/research/00039/

48. Weidenbaum, M., & Hughes, S. (1996). *The bamboo network: How expatriate Chinese entrepreneurs are creating a new economic superpower in Asia* (pp. 23–60). The Free Press.

49. Burgos, J. (2025, April 16). Billionaire Robert Kuok, Malaysian tycoons seek profit from data center boom. *Forbes Asia.* https://archive.ph/ONG6U

50. IDCNova. (2025, April 21). Sime Darby Property aims to build more data centers in Malaysia; 2 Google data centers under its belt. *IDCNova.* https://archive.ph/vAgvB

51. Ruehl, M. (2024, July 19). From palm oil data: Malaysia builds AI hub on Singapore's doorstep. *Financial Times.* *https://archive.ph/1zSBb*

52. Anand, R., & Melin, A. (2025, May 5). Google unit awards data centre contract to Malaysia's Gamuda. *The Edge Singapore, published via Yahoo News.* https://archive.ph/XNO5J

53. Ee, E. (2019, June 29). Lendlease announces US$1 billion data centre partnership [Press release]. *Lendlease.* https://archive.ph/2Lp7Y

54. Woo, S. (2024, October 7). One of the biggest AI boomtowns is rising in a tech-industry backwater. *The Wall Street Journal.* https://archive.ph/6D9A1

55. Walker, O. (2025, January 12). Malaysia expects surge of Chinese investment, economy minister says. *Financial Times.* https://archive.ph/8OPPo

56. Telekom Malaysia. (2024, June 18). TM and Singtel's Nxera form joint venture to develop next-generation data centres [Press release]. *TM.* https://archive.ph/1eIoO

57. DigitalBridge. (2022, November 21). DigitalBridge announces formation of edge data center platform in Asia and acquisition of a stake in AIMS Group [Press release]. *DigitalBridge.* https://archive.ph/fs1sg

58. Wodehouse, C. (2025, March 11). Greenfield vs. brownfield data centers: Key differences and considerations. *Pure Storage Blog.* https://archive.ph/p6ab5

59. Amazon Web Services. (2025, June 17). Multi-tier cloud security standard (MTCS) compliance. *AWS.* https://archive.ph/wC5Rv

60. Morales, J. (2025, February 18). DeepSeek GPU smuggling probe shows Nvidia's Singapore GPU sales are 28 percent of its revenue—but only 1 percent are delivered to the country: Report. *Tom's Hardware.* https://archive.ph/jAhZJ

61. Uncle US Stock. (2025, May 13). Malaysia's monthly imports of NVIDIA GPUs reach nearly USD 3 billion, hitting a record high [馬來西亞單月進口 NVIDIA GPU 近 30 億美元創歷史新高]. *Cnyes.com.* https://archive.ph/5ZWhW#selection-629.0-641.0

62. WargaBiz. (2025, July 9). This 3rd-gen Kuok is transforming the family empire with a $10B AI bet. *WargaBiz.* https://archive.ph/XezAf

63. The Economist. (2020, May 28). South-East Asian tycoons' high-wire act. *The Economist.* https://archive.ph/YVcmg

64. Global Data Center Hub. (2025, May 23). Strategic partnerships in data centers: Joint ventures, leasing, and management contracts. *Global Data Center Hub.* https://archive.ph/xiNLW

65. Telecomdrive Bureau. (2024, June 19). TM, Singtel's Nxera form JV to develop next-gen data centres. *TelecomDrive.* https://archive.ph/F3Yqv

66. Chia, J. (2024, June 10). Singapore picks AirTrunk, Equinix, GDS and Microsoft in data centre pilot programme. *Mingtiandi.* https://archive.ph/qx5TB

67. Guandian Net. (2024, June 11). ByteDance plans to invest an additional USD 2.4 billion in Malaysia to expand data centers and AI hub [字節跳動拟在馬來西亞追加投資 24 億美元擴建數據中心和 AI 中心]. *Guandian Net.* https://archive.ph/6eMSf

68. Walker, O. (2024, May 19). Malaysia expects surge of Chinese investment, economy minister says. *Financial Times.* https://archive.ph/8OPPo

69. GDS Holdings Limited. (2022, April 27). YTL and GDS to partner on 168MW data center development at the visionary YTL Green Data Center Park in Johor, Malaysia [Press release]. *Globe Newswire.* https://archive.ph/KIjDT

70. Butler, G. (2025, July 29). YTL Power and Nvidia to invest $2.3bn in AI infrastructure in Malaysia. *Data Center Dynamics.* https://archive.ph/F4Hf2

71. Astro Awani. (2025, March 19). YTL early adopter of NVIDIA Blackwell Ultra, the next evolution of the NVIDIA Blackwell AI factory platform [Media statement]. *Astro Awani International.* https://archive.ph/zvZ7w

72. Malaysian Investment Development Authority. (2023, July 7). YTL data centers and Sea break ground with the RM1.5bil first phase of the 500MW YTL Green Data Center Park in Johor [Press release]. *MIDA*. https://archive.ph/wFeCh

73. Li, J. (2022, March 3). Amid regulatory crackdowns, Tencent takes a tactical approach to its investments. *KrASIA*. https://kr-asia.com/amid-regulatory-crackdowns-tencent-takes-a-tactical-approach-to-its-investments

74. Patel, D., Chen, K., Nishball, D., Chiam, I., & Knuhtsen, R. (2025, March 26). The GPU cloud ClusterMAX™ rating system: How to rent GPUs—90%+ coverage by rental GPU value, GPU cloud evaluation guidelines, GPU pricing updates, GPU bubble burst, CoreWeave IPO, hyperscalers, AI neocloud economics, neocloud IRR. *SemiAnalysis*. https://archive.ph/8B70P

75. Equinix. (n.d.). What is colocation? *Equinix*. https://archive.ph/zW7ne

76. Perrigo, B. (2025, April 22). Exclusive: Every AI datacenter is vulnerable to Chinese espionage, report says. *TIME*. https://archive.ph/3hBpK

77. SenseTime. (2021, July 19). SenseTime establishes Singapore International AI Innovation Center: "Original AI" shines again in the Lion City [商湯科技成立新加坡國際 AI 創新中心，「原創 AI」再綻獅城] [Press release]. *SenseTime*. https://archive.ph/a1Xq7

78. Guandian Net. (2024, June 11). ByteDance plans to invest an additional USD 2.4 billion in Malaysia to expand data centers and AI hub [字節跳動拟在馬來西亞追加投資 24 億美元擴建數據中心和 AI 中心]. *Guandian Net*. https://archive.ph/6eMSf

79. Malaysian Investment Development Authority. (2022, November 9). Bridge Data Centres and ByteDance celebrate grand opening of the first phase hyperscale data centre (MY06) in Johor, Malaysia [Press release]. *MIDA*. https://archive.ph/xcvVy

80. Ontiveros, J. E., Patel, D., & Nishball, D. (2025, June 30). How Oracle is winning the AI compute market: Stargate, OpenAI, ByteDance, unique datacenter strategy, investment grade neocloud, revenue and EBIT forecast. *SemiAnalysis*. https://archive.ph/ZCoNj

81. Mokhtar, F., & Hawkins, M. (2025, July 10). Oracle said to move ahead with cloud services plan in Indonesia. *Bloomberg*. https://archive.ph/SfVPF

82. Gooding, M. (2024, June 10). TikTok owner ByteDance to expand Malaysia data center footprint in $2.1bn AI deal: Minister hails boost for Malaysia's digital economy. *DataCenterDynamics*. https://archive.ph/i2sDP

83. Trueman, C. (2025, January 2). ByteDance could spend $7bn to access Nvidia Blackwell chips outside China – report: Would make TikTok's parent company one of Nvidia's biggest customers. *DataCenterDynamics*. https://archive.ph/jHNgA

84. Tech in Asia. (2025, April 29). Tencent, Alibaba buy Nvidia GPUs from ByteDance. *Tech in Asia*. https://archive.ph/gbRzv

85. Center for Internet Security. (n.d.). What you need to know about hybrid cloud environments. *CIS*. https://archive.ph/nFyD5

86. Oracle. (n.d.). Hybrid cloud. *Oracle*. https://archive.ph/DCcSQ

87. General Office of the State Council. (2021, June 11). Data Security Law of the People's Republic of China [中華人民共和國數據安全法]. *The Central People's Government of the People's Republic of China*. https://archive.ph/HFe8b

88. Sutter, K. M. (2021, October 21). China's recent trade measures and countermeasures: Issues for Congress (CRS Report No. R46915). *Congressional Research Service*. https://archive.ph/5XYHT

89. BBloombergQuint. (2021, June 14). China's new data law gives Xi the power to shut down tech firms. *BloombergQuint*. https://archive.ph/adFPB

90. Lu, B., Zhang, Q., & Chen, D. (2025, July 16). The digital silk road in the Gulf: Navigating risks amid China–US rivalry. *The Diplomat*. https://archive.ph/ARk10

91. Huang, R., & Lin, L. (2025, June 12). Chinese AI companies dodge U.S. chip curbs by flying suitcases of hard drives abroad. *The Wall Street Journal.* https://archive.ph/8syqZ#selection-2535.0-2727.0

92. Anthropic. (2025, July 21). Build AI in America. *Anthropic.* https://archive.ph/oPZqu

93. The White House. (2025, July 23). White House unveils America's AI action plan. *The White House.* https://archive.ph/wgs4L

94. Institute for International Governance of Artificial Intelligence, Tsinghua University. (2025, March 28). Why can't China's AI development bypass "overseas computing power"? Understanding national AI through "submarine cables" [中国 AI 发展为何绕不开 '海外算力'？从 '海底光缆' 看国家 AI]. *Zhiyuan Community.* https://archive.ph/4Bfy8

95. Martin, E. E., Hounfodji, C. N., & Plotinsky, D. (2025, July 2). Key cybersecurity, privacy, and national security considerations for data centers in 2025. *Morgan Lewis.* https://archive.ph/xtA88

96. Kennedy, G., Haylock, A., & Lai, J. W. J. (2024, December 19). Malaysia's new Cyber Security Act 2024 – A summary and brief comparative analysis. *Mayer Brown.* https://www.mayerbrown.com/en/insights/publications/2024/12/malaysias-new-cyber-security-act-2024-a-summary-and-brief-comparative-analysis

97. Allen, G. C., & Goldston, I. (2025). Understanding US allies' current legal authority to implement AI and semiconductor export controls. *Center for Strategic and International Studies.* https://archive.ph/9DeYu

98. One example can be seen in the news coverage from Hsiao, P.-W. (2022, March 9). Preventing China from poaching high-tech talent: Bureau of Investigation mobilizes 100 agents to probe 8 illegal PRC firms [阻中國挖角高科技人才 調查局動員百人偵辦 8 家違法陸企]. *Central News Agency.* https://archive.ph/SyYRB

99. Chiang, M.-Y. (2024, August 27). The remote poaching model: How China's Bitmain acquired Taiwan's edge AI chip technology and its implications for economic security. *DSET.* https://dset.tw/en/research/00039/

100. See recent investigations of the MJIB. Lin, Y.-J. (2025, March 28). Bureau of Investigation uncovers 11 PRC firms "illegally poaching talent in Taiwan," with SMIC implicated [調查局查獲 11 間中企『非法在台挖角』，中芯國際也涉案]. *TechNews.* https://archive.ph/4Ls52

101. Anandarajah, K., Tang, T., & Seet, J. (2025, April 9). Singapore Issues Advisory on Export Controls on Advanced Semiconductor and AI Technologies. *Rajah & Tann Asia.* https://archive.is/176qj

102. Nellis, S. (2025, May 15). U.S. lawmakers introduce bill to address AI chip smuggling. *Reuters.* https://archive.ph/vkIY7

103. Wu, Z., & Leng, C. (2025, August 21). China turns against Nvidia's AI chip after 'insulting' Howard Lutnick remarks. *Financial Times.* https://archive.ph/9fHIX

104. Huang, R., & Lin, L. (2025, June 12). Chinese AI companies dodge U.S. chip curbs by flying suitcases of hard drives abroad. *The Wall Street Journal.* https://archive.ph/8syqZ

105. Gupta, S., Axboe, J., Ravi, M., Upadhyaya, K., & Saab, P. (2025, March 4). A case for QLC SSDs in the data center. *Engineering at Meta.* https://archive.ph/XfBbR

106. Grossman, D. (2024, February 8). The good and the bad for Biden in Southeast Asia. *RAND Corporation.* https://archive.ph/c2bBP

107. Heim, L. (2025, May 2). China's AI models are closing the gap—but America's real advantage lies elsewhere. *RAND Corporation.* https://archive.ph/Zwm9G

108. Liggett, T., Helmus, T. C., & Grocholski, K. R. (2024). How the United States can support allied and partner efforts to counter China in the gray zone: Affirmative engagement. RAND Corporation. Also see Kuo, R. C. (2020). *Contests of initiative: Countering China's gray zone strategy in the East and South China Seas.Westphalia Press.*

Research Institute for **Democracy**, **Society**, and **Emerging Technology**