November 2025

# CONVERGE

## INDO-PACIFIC CRITICAL TECH COOPERATION

Mark Bryan Manantan, Editor
Kristi Govella, Ph.D.
Merve Hickok
Maria Monica Wihardja, Ph.D.
Brad Glosserman
Ben Scott
Daisuke Kawai
Sameer Patil, Ph.D.
Manoj Harjani

PACIFIC FORUM
INTERNATIONAL

東京大学 先端科学技術研究センター
Research Center for Advanced Science and Technology
The University of Tokyo

November 2025

# CONVERGE

## INDO-PACIFIC CRITICAL TECH COOPERATION

Mark Bryan Manantan, Editor
Kristi Govella, Ph.D.
Merve Hickok
Maria Monica Wihardja, Ph.D.
Brad Glosserman
Ben Scott
Daisuke Kawai
Sameer Patil, Ph.D.
Manoj Harjani

PACIFIC FORUM INTERNATIONAL

## About the Pacific Forum

Based in Honolulu, Pacific Forum International (Pacific Forum) is a foreign policy research institute focused on the Asia-Pacific Region. Founded in 1975, Pacific Forum collaborates with a broad network of research institutes around the Pacific Rim, drawing on Asian perspectives and disseminating project findings and recommendations to global leaders, governments, and members of the public throughout the region.

The Forum's programs encompass current and emerging political, security, economic, and cybersecurity, and critical technology policy issues, and work to help stimulate cooperative policies through rigorous research, analyses, and dialogue.

## The Pacific Forum

Web: www.converge.pacforum.org
Facebook: Pacific Forum
Twitter: @PacificForum
Instagram: @pacforum
Podcast: Indo-Pacific Current
Email: pacificforum@pacforum.org

**CONVERGE: Indo-Pacific Critical Tech Forum** is made possible through the generous funding support from the Bureau of Oceans and International Environmental and Scientific Affairs, US Department of State.

All facts, positions, and perspectives contained in this report are the sole responsibility of its authors and do not reflect the institutional views of the Pacific Forum or its board, staff, or supporters.

# Acknowledgement

東京大学 先端科学技術研究センター
Research Center for Advanced Science and Technology
The University of Tokyo

## RCAST - The University of Tokyo

The Research Center for Advanced Science and Technology (RCAST), the newest institute attached to the University of Tokyo, aims to contribute to the development of science and technology by expeditiously taking on new challenges arising from the advancement of science and coincident changes in society, and by exploring new areas of advanced science and technology for the benefit of humankind and society since its establishment in 1987. More than 40 eponymous labs for a wide variety of specialized fields are pursuing advanced research in science and technology as well as in social sciences and the field of barrier-free research. We extend these research areas over a wide range, from basic and applied fields further to the social system.

https://www.rcast.u-tokyo.ac.jp/en/about/

The information in this document is for general informational purposes only and is provided in good faith. We make no representations or warranties regarding the accuracy, reliability, or completeness of the content. We are not liable for any loss or damage resulting from the use of this information. External links are not monitored for accuracy, and we do not endorse or assume responsibility for third-party content. Use this information at your own risk.

# Contributing Authors

**MARK BRYAN MANANTAN** SERIES EDITOR
is the Director of Cybersecurity and Critical Technologies at the Pacific Forum.

**KRISTI GOVELLA, PH.D.** is Associate Professor of Japanese Politics and International Relations at the University of Oxford and Senior Adviser and Japan Chair at the Center for Strategic and International Studies (CSIS).

**MERVE HICKOK** President and Policy Director at Center for AI and Digital Policy, and International Affairs Fellow at Council on Foreign Relations – Hitachi.

**MARIA MONICA WIHARDJA, PH.D.** is Visiting fellow and Co-coordinator of the Media, Technology, Society Programme, ISEAS-Yusof Ishak Institute.

**BRAD GLOSSERMAN** is Director of Research and Senior Advisor at Pacific Forum.

**DAISUKE KAWAI** is Director of the Economic Security and Policy Innovation Program, and Project Assistant Professor at the Research Center for Advanced Science and Technology, University of Tokyo.

**BEN SCOTT** was a Senior Advisor at the National Security College, Australian National University.

**SAMEER PATIL, PH.D.** is Director, Centre for Security, Strategy and Technology at the Observer Research Foundation, India.

**MANOJ HARJANI** is Research Fellow at S Rajaratnam School of International Studies.

**United States Department of State**

***Washington, D.C. 20520***

Participants of CONVERGE:

As the Science and Technology Adviser to the U.S. Secretary of State, the Honorable Antony J. Blinken, I thank you for your attendance at this conference about a topic of paramount importance: a free and open Indo-Pacific region, which is inclusive and resilient.

Our diplomats have recognized the transformative power of critical and emerging technologies to support sustainable development in the Indo-Pacific and deliver economic and social benefits. We are not just collaborating on specific technologies like trusted, secure and robust telecommunications networks, artificial intelligence, and synthetic biology. We are also uplifting the next generation of scientists, technologists, engineers, and mathematicians through the Quad Fellowship, which expanded this year to include students from Southeast Asian countries.

Your conversations at CONVERGE are critical in an ongoing dialogue about how we think about the future of the Indo-Pacific region. I encourage you to embrace other perspectives, meet new people, and formulate new ways of looking at the issues we jointly face.

Sincerely,

Pat Gruber

Dr. Patricia Gruber
Science and Technology Adviser to the
Secretary
U.S. Department of State

# Contents

# Introduction

## Mark Bryan Manantan

The Indo-Pacific is at the forefront of a technology revolution. In the coming decades, the deployment of critical and emerging technologies (CET) such as artificial intelligence (AI) will create trillions of dollars of value for the region. Conversely, Indo-Pacific countries will play a pivotal role in the realignment of resilient supply chains essential to CET industries, particularly semiconductors.  However, technology collaboration in the Indo-Pacific is also enormously complex. Collaboration and governance occur on multiple interacting levels, including bilateral, regional, and multilateral groupings and institutions. There is a limited understanding of how these interactions affect cross-border research and development (R&D), investment, and commercialization on a practical level.

**Examining the challenges and opportunities facing different CET actors operating in the Indo-Pacific in these specific technology verticals is warranted. It offers a means to identify best practices for enhancing Indo-Pacific tech cooperation while building trust between existing stakeholders.**

This publication builds on the key outcomes and findings from *CONVERGE: The Indo-Pacific Critical Tech Forum on AI and Semiconductors 2024*, a Track 1.5 dialogue that aimed to examine key technical, policy, and operational approaches of certain Indo-Pacific countries on AI and semiconductors. This sought to harmonize efforts and achieve an interoperable and collaborative tech environment between public and private actors operating in different contexts and borders. In cultivating a vibrant tech ecosystem in the Indo-Pacific, CONVERGE convened leading experts, practitioners, and thought leaders from government, industry, academia, and civil society from the Quadrilateral Security Dialogue—or the Quad—comprising the United States (US), Japan, Australia, and India, alongside two Southeast Asian countries: Singapore and the Philippines.

The goal in convening the Quad and two Southeast Asian countries is two-fold: Evaluate the prospects of fortifying closer linkages between the Quad grouping and Southeast Asia to build trust; and foster concrete pathways in advancing a stable, secure and prosperous regional tech environment. Cognizant that Southeast Asian countries have varying perceptions and openness toward the Quad, CONVERGE sought to engage Singapore and the Philippines as test cases for compatibility. Over the long term, it is hoped that CONVERGE leads to the institutionalization of QUAD-Southeast Asia cooperation to promote a wider Indo-Pacific collaboration on critical and emerging technologies.

Evidently, tech innovation does not occur in a silo. Thus, CONVERGE undertakes a pragmatic approach of equally emphasizing academic, policy and industry perspectives to ensure that the insights and recommendations generated are feasible in the real-world setting. Accompanying the key findings of the Track 1.5 dialogue are policy chapters written by experts that further provide a deep dive into the varying contexts and prospects of the US, Japan, Australia, India, Singapore, and the Philippines in AI and semiconductors in the evolving Indo-Pacific landscape.

This publication begins with three chapters offering broad perspectives and reflections on Quad and ASEAN relations before focusing on regional trends in AI and semiconductors. What follows are specific country chapters that incisively assess the state of play in AI and semiconductors based on key indicators that are vital to achieving CET collaboration: *Economic security and supply-chain resilience, Cybersecurity and risk management, AI and data governance, Capacity-building, and international partnerships and collaboration*.

Emerging from these chapters are complex and distinct analyses of the opportunities and challenges that these countries face in CET innovation. However, despite the contextual differences that underpin each state's innovation journey, one constant factor that arises is the need to leverage international partnerships. Taken altogether, the chapters reflect a strong desire towards more consultation and breaking down barriers among communities, institutions, and across borders. This compendium hopefully inspires more institutionalized engagement between Quad and the remaining ASEAN member states—one that is built in pragmatism and prudent desire to realize mutually beneficial outcomes.

# Key Findings

Mark Bryan Manantan

On October 10-11, 2024, Pacific Forum in collaboration with the Research Center for Advanced Science and Technology, University of Tokyo convened a Track 1.5 dialogue to harness the Indo-Pacific's tech potential in artificial intelligence (AI) and semiconductors amid deepening great power rivalry, shifting regional and international supply-chains, and technological disruptions.

Held under the Chatham House Rule, the closed-door dialogue brought together esteemed experts, practitioners, and policymakers from the United States (US), Japan, Australia, India, Singapore, and the Philippines to examine the prospects of fortifying closer linkages between the Quad grouping and Southeast Asia.

## Setting the context

The Quad regularly acknowledges ASEAN centrality and its convening power through regional dialogue mechanisms like the East Asia Summit and the ASEAN Regional Forum, however, skepticism remains high toward the minilateral grouping. Despite its recent rebranding as a public goods provider through its COVID-19 vaccine diplomacy during the pandemic, the Quad's evolving and implicit strategic agenda that aims to counterbalance China's assertiveness remains a major source of anxiety among policy elites in Southeast Asia as it could undermine regional stability. Additionally, ASEAN has a longstanding uneasiness toward the Quad's embrace of "like-mindedness" because it promotes a binary choice of us versus them narrative, which can lead to potential division and/or exclusion of other parties.

The simmering disparity between the Quad and ASEAN's perspectives on what constitutes a stable, secure and prosperous regional architecture may inadvertently promote misunderstanding and misperceptions. Therefore, a neutral forum to foster trust and transparency among the key decisionmakers, influencers, and stakeholders from the Quad and ASEAN is warranted.

CONVERGE: The Indo-Pacific Critical Tech Forum 2024, a track 1.5 dialogue seeks to narrow the prevailing trust deficit between the QUAD and Southeast Asian countries. Instead of emphasizing the usual 'US-China factor,' CONVERGE, sought to reframe the prevailing policy discussions by finding a common technological agenda to formulate practical pathways for collaboration that would bring mutual benefits to the Indo-Pacific. Track 1.5 and by extension, track 2 dialogues are vital bulwarks for novel policymaking. Such informal channels facilitate the exchange of ideas to promote practical understanding on the most pressing challenges especially in the rapidly evolving international environment. The outcomes of intellectual and policy exercises can build trust and confidence that could later spill over into constructive government to government interactions and foster multistakeholder cooperation. To this end, CONVERGE convened leading experts and stakeholders from government, industry, academia, think tanks, and civil society to explore the fundamental building blocks to achieving an open and interoperable tech ecosystem based on key emerging themes of economic security, cybersecurity, AI and data governance, capacity-building, and international partnerships.

Cognizant that Southeast Asian countries have varying perceptions and openness toward the Quad, the workshop sought to engage Singapore and the Philippines as test cases for compatibility. Over the long-term, CONVERGE hopefully leads to the institutionalization of QUAD-Southeast Asia cooperation to promote wider Indo-Pacific collaboration on critical and emerging technologies. Key findings from the two-day discussions are:

### Taking stock of the current tech environment

Participants agreed that overall, there is no clearly accepted definition or list of critical technologies in the Indo-Pacific. Certainly, AI and semiconductors are defined in the critical technologies category. But beyond formulating a list, there are two major factors worth considering: first, the nature of technology is rapidly evolving—what is considered critical and emerging today may not be relevant in the short to medium term. Second, even with its technological prowess, it is unsustainable for the any actor let alone states to dominate the innovation and diffusion of all critical and emerging technologies indefinitely.

China's advancement in critical technologies is a major concern for US allies like Japan and Australia especially its potential misuse of technologies like AI and semiconductors for military purposes. On the contrary, Southeast Asian countries view China less of a threat but more as an opportunity to further develop their digital economy. However, discreet discussions among stakeholders in Southeast Asia reveal the upside associated with US and its allies' de-risking efforts against China. Some policy elites in Southeast Asia view the ongoing reconfiguration in the global value chain as an opportunity for some countries to position themselves as alternative production hubs particularly in semiconductors.
Still, achieving concrete and practical technological collaboration among friends and partners is easier said and done. Even among US allies and partners, there are several roadblocks that could hinder mutually beneficial collaboration: accountability in governing technologies, the integrity of supply chains, data privacy and cybersecurity as well as bias in datasets.

### Economic Security

With increasing US restrictions aimed at reducing Chinese access to semiconductor manufacturing know-how and equipment, China is not backing down. China is also imposing its countermeasures through its evolving export controls on rare earth minerals like graphite, gallium and germanium. The tit-for-tat response from the two rivals will likely continue to escalate. Given the increasing uncertainty, some participants saw the need for more analysis devoted to assessing the implications of Chinese retaliatory measures to the overall supply-chains.

Interestingly, there was an ensuing debate among academic and policy experts and industry practitioners regarding the value of tighter export control measures in ensuring one's leadership in critical and emerging technologies. Academic and policy experts recognize that evaluating the effects of economic protection and collaboration is becoming increasingly difficult. Industry representatives emphasized that bolstering regulations solely based on reactive and knee-jerk reactions may pose more harm than good due to the costs, and disruption to the overall innovation cycle over the medium to longer-term.

With national security becoming a dominant force in (re)shaping trade and economic policy, some participants argued that setting a coordinated baseline on restrictions would help ensure all relevant actors are on the same page is a practical measure. Establishing partnerships through multistakeholder outreach and consultations can also offset the negative externalities from tech controls of critical and emerging technologies in the long-haul.

## Cybersecurity

With the increasing cyber-AI nexus, the cybersecurity threat landscape is evolving at breakneck speed, necessitating the need for novel methods of raising resilience. In cyber defense, AI is instrumental in augmenting threat analysis, response, and recovery. Unfortunately, some actors are also leveraging AI for malicious purposes such as phishing to malware generation. With geopolitical events like the Ukraine war and Israel-Hamas conflict along with rising tensions in the Indo-Pacific, state-sponsored advanced persistent threat actors are likely to engaged in more covert operations to gain more access to geopolitical intelligence. The advent of adversarial AI enables threat actors to attack machine learning models through data-poisoning and model inversion.

Similarly, AI has been integral in ramping up research and development for advanced semiconductor design and production. However, threat actors are capitalizing on AI to compromise the integrity of supply chains either through avoiding detection or installing a backdoor. Amid the amplification of cyber defense and offense through AI and adversarial AI, existing AI governance frameworks must be updated to adversarial testing, benchmarking, and evaluation of system security, particularly in relation to AI's application in the military and civilian domains.

## AI and Data Governance

There is significant inconsistency in AI regulations across countries, which complicates regulatory governance. Each nation has its own approach, leading to gaps in data protection and ethical standards. Moreover, the deepening tech rivalry between the US and China impacts the progress of developing and implementing interoperable AI governance frameworks. Participants agreed that national security has been clouding priorities like democratic values and human rights.

While AI is global, it is also local. All experts have agreed that AI regulations should be adapted to the specific cultural and social contexts of each country, recognizing local values and norms in the governance process. Many countries in the Indo-Pacific face significant challenges in upskilling their workforce for AI adoption, stifling the realization of the AI boom and widening digital inequities.

Building public trust in AI systems is crucial, necessitating transparency from both governments and private companies about data usage and algorithmic decisions. Academia, think tanks, and civil society must ensure governments and large tech companies develop and maintain systems of accountability.

## Capacity-building

Across countries, there is a growing deficit in skilled labor, particularly in the AI and semiconductor sectors in large part due to talent migration and lack of practical pathways for talent mobility. Legal frameworks for talent mobility in the AI and semiconductor industry remain underexplored. Other parameters, such as labor demographics, labor capacity and talent migration processes are also impacting talent mobility.

Capacity building and collaboration are vital to addressing the prevailing talent shortage. Several multinational companies are leading collaborations with the government, business, NGOs, and academic sectors to increase capacity building through AI upskilling and reskilling. Their goal is to provide AI-skilling resources and training to benefit the public, business employees, local education institutions, and the government sector in their everyday use of technology.

With the ongoing trend of supply chain restructuring, strategic partnerships in capacity building and research and development (R&D) in AI and the semiconductor industry are crucial. While R&D investments are increasing in the Indo-Pacific region, the lack of capable talents pose a significant challenge. The triple helix of government, private sectors, and academic institutions' partnership and collaboration are vital to building a skilled workforce in AI and semiconductors, especially in emerging markets like Southeast Asia.  But beyond expanding technical skills, capability-building efforts must focus on other related critical skills such as AI literacy, environmental sustainability, ethical considerations, and cybersecurity to ensure the responsible and sustainable use of AI technologies.

## Policy Recommendations

Based on the two-day deliberation among experts, the following policy recommendations are suggested to foster a collaborative regional tech environment:

**Economic Security**

- The Quad countries and Southeast Asia must develop a working list of critical and emerging technologies and collaborate on a strategic roadmap designed to achieve synergy in three key areas: regulation, trade and financial investment, and capacity building.

- Raise the technology policy expertise of government officials, representatives, and staff across foreign affairs' departments and ministries to guarantee deeper and sustained political and diplomatic investment on critical technology-related issues.

- Because total decoupling is infeasible over the short-to-medium term, it is still important to engage China based on appropriate rules and mechanisms through establishing safeguards must balance national security and economic interests. In doing so, governments must coordinate and initiate open discussions and consultations especially with the private sector to identify and clarify clear parameters of such engagements.

- Organize forums and workshops that bring together governments, tech companies, academic institutions, and civil society to undertake scenario-planning and foresight exercises to buffer against unexpected shocks from the evolving and disruptive nature of dual-use technologies like AI and semiconductors, and the uncertainty arising from geostrategic challenges.

**Cybersecurity and supply-chain resilience**

- Strengthen regional cooperation through the alignment of cybersecurity standards in intellectual property protection, data protection, reporting, and protocols assessment. Because cybersecurity is a team sport, international cybersecurity partnerships must include regularly scheduled joint exercises, like red or blue teaming, and developing interoperable cybersecurity protocols and guidelines.

- With the increasing cyber-AI nexus, it is vital to protect critical infrastructure, safeguard technology supply-chains, adopt a secure by design approach, and ensure the government's active cyber defense in AI and the semiconductor industry.

- Support industry-led cybersecurity initiatives to highlight the importance of public-private partnership to identify specific scenarios that reflect a good balance of national security and economic security.

**AI and Data Governance**

- Develop a regional framework that promotes harmonization of AI regulations across Indo-Pacific countries, while respecting local contexts. This could involve a coalition of countries agreeing on minimum standards as a key starting point.

- At the country level, encourage collaboration between government and private sector companies to create shared standards for data governance, ensuring both parties take responsibility for ethical AI deployment.

- Invest in educational initiatives that focus on AI literacy, ethics, and governance. This should include partnerships with universities and tech firms to develop curricula tailored to local and regional needs.

- Create a set of ethical guidelines for AI development and use-case that prioritizes human rights, privacy, and societal well-being, integrating input from diverse stakeholders, including civil society. For instance, Southeast Asia and India's linguistic diversity requires AI models that accommodate multiple languages to avoid discrimination.

**Capacity-building**

- Establish a comprehensive legal policy framework that facilitates the international mobility of talents and experts in the AI and semiconductor industries. This approach can contribute to efficient talent flow to meet the increasing demand for highly skilled labor.

- Enhance the partnership between academic institutions and the private sector to expand education programs in AI and the semiconductor industry. Building graduate-level programs and training that align with industry needs will contribute to bridging the talent gap and fostering a skilled workforce.

- Integrate critical initiatives such as AI literacy, cybersecurity training, AI ethics, and sustainability into capacity-building efforts. Government and the private sector can lead the development of AI capability-building framework to ensure the adoption of environmentally responsible practices, advance sustainable technological growth, and responsible use of AI technology.

- Focus on inclusive capacity-building initiatives that promote public-private-academic collaboration in AI training and education for underserved regions, small businesses, and nonprofit organizations. Equitable access to AI and training for integrating tech skills can bridge the work talent gap  in the AI and semiconductor sectors.

# Advancing Quad-Southeast Asia Engagement on Critical and Emerging Technologies

Kristi Govella, Ph.D.

## Key Findings

- The Quadrilateral Security Dialogue among Australia, Japan, India, and the United States ("the Quad") can be used as a building block for broader regional engagement with Southeast Asian countries on critical and emerging technologies through a combination of consultation, coordination, and cooperation.
- Without expanding Quad membership or creating new institutions, the existing working groups and initiatives of the Quad can function as hubs to scale up initiatives, expand benefits, and broaden policy coalitions.

## Policy Recommendations

When advancing Quad-Southeast Asia engagement on critical and emerging technologies, policymakers should consider four potential overlapping roles for Southeast Asian countries in their engagement with the Quad as:

- Consumers: Quad governments can engage in information sharing and capacity building to help Southeast Asian governments and individuals make their own informed decisions about adopting specific technologies, and Quad governments can cooperate to bring down the cost of Open-RAN and other technologies from trusted providers to increase consumer appeal.

- Producers: Quad governments can expand existing efforts to map collective capacity and supply chain vulnerabilities to include Southeast Asian countries, provide workforce capacity building in relevant tech industries, and locate some parts of supply chains in Southeast Asia. Quad governments can also expand initiatives such as the Quad Investors Network and the Quad STEM Fellowship to engage Southeast Asian partners.
- Adopters (i.e., "standard takers"): Southeast Asian governments can consider coordinating their policies with standards such as the Quad Principles on Critical and Emerging Technology Standards, the Quad Common Statement of Principles on Critical Technology Supply Chains, and the Quad Principles on Technology Design, Development, Governance, and Use.

- Influencers (i.e., "standard makers"): Quad governments can expand opportunities for Southeast Asian state and non-state stakeholders to consult in the development of principles and standards for critical and emerging technologies.

## Introduction

Since the Quadrilateral Security Dialogue among Australia, Japan, India, and the United States ("Quad") was revived in 2017, it has embraced an expanding agenda. Critical and emerging technologies were taken up by the Quad in March 2021, when the US hosted the grouping's first leader-level summit. At that meeting, the leaders of the four countries created the Critical and Emerging Technology Working Group, which has since focused on aligning national efforts related to technical standards, 5G diversification, Open Radio Access Network (RAN) deployment, technology supply chains, artificial intelligence (AI), and biotechnology. Initiatives related to technology have also been embedded in other structures such as the Quad Investors Network, the Quad Cyber Security Working Group, and the Quad Partnership for Cable Connectivity and Resilience.

Although the Quad has primarily focused on deepening engagement among its four members to date, its members' concerns about critical and emerging technologies—and many other issues—cannot be fully addressed by the four governments alone, which creates opportunities to partner with other regional actors. Southeast Asia has become an important area of focus for the Quad, which has sought in recent years to position itself as a provider of public goods to the region. Consequently, despite some initial skepticism about the Quad as an organization and concern that it might provoke negative reactions from China, many Southeast Asian countries have gradually become more receptive to the idea of working with the Quad for the sake of mutual benefits, with critical and emerging technologies as a promising area for expanded engagement.

This article argues that the Quad can be used as a building block for broader regional engagement with Southeast Asian countries on critical and emerging technologies through a combination of consultation, coordination, and cooperation. Without expanding Quad membership or creating new institutions, the existing working groups and initiatives of the Quad can function as hubs to scale up initiatives, expand benefits, and broaden policy coalitions. In addition, the article argues that policymakers can benefit from thinking about four potential overlapping roles for Southeast Asian countries in their engagement with the Quad: as consumers, as producers, as adopters (i.e., "standard takers"), and as influencers (i.e., "standard makers"). By conceptualizing regional engagement in this way, policymakers can formulate a comprehensive set of policy recommendations on critical and emerging technologies that will generate mutually reinforcing outcomes.

## Quad Initiatives on Critical and Emerging Technologies

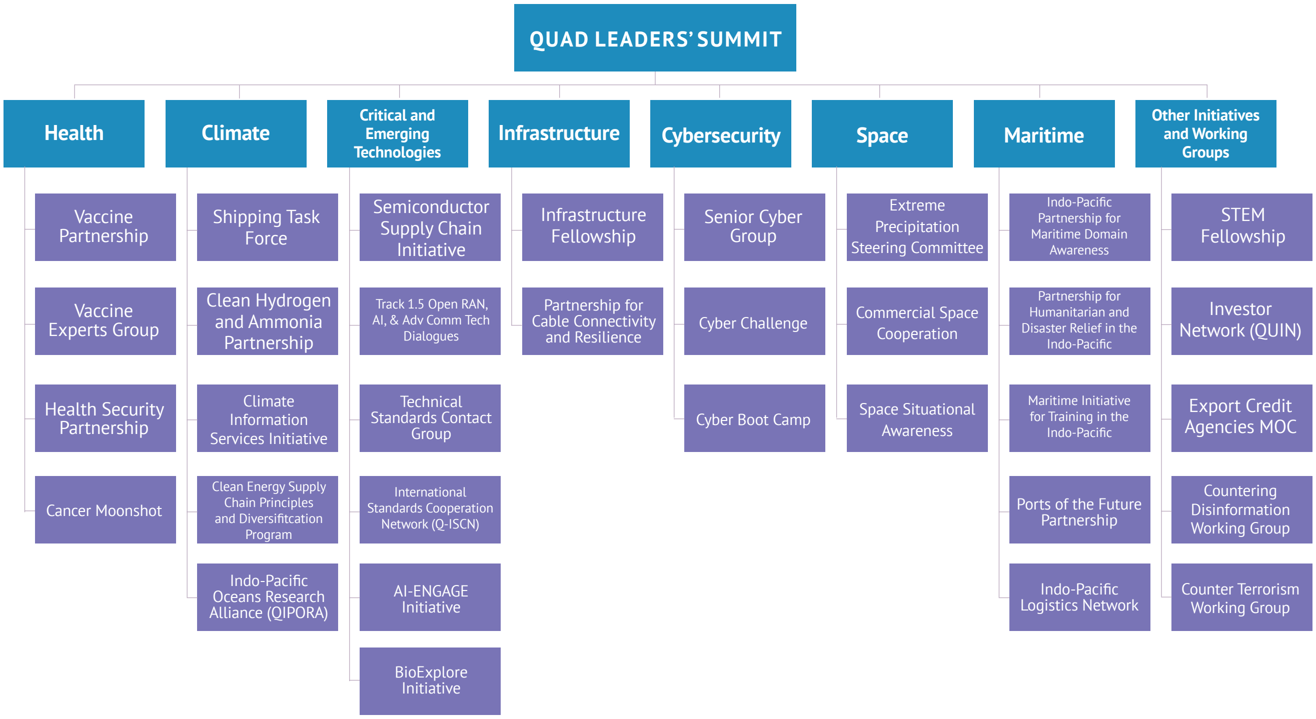
This section provides a brief overview of existing Quad initiatives related to critical and emerging technologies. When discussing the Quad, it is important to recognize that the grouping is still primarily focused on deepening internal engagement among its four members, which remains uneven—in many cases, collaboration among Quad countries tends to be bilateral or trilateral instead of fully quadrilateral. For example, in the area of AI, research shows that although Australia, India, and Japan each have strong bilateral research partnerships and bilateral investment links with the US, the three countries collaborate much less with one another.[1] When it comes to difficult questions about how technologies pose risks or opportunities for their societies, there are different perspectives among the four governments—and even within each country, there is often disagreement among various state and non-state stakeholders about how technologies should be developed, used, and regulated. [2]

Despite these challenges, the Quad has taken concrete steps toward strengthening engagement among the four countries through an evolving structure of working groups and targeted initiatives, as shown in Figure 1. This section reviews Quad efforts in its Critical and Emerging Technology Working Group related to 1) technical standards; 2) 5G diversification and Open Radio Access Network (RAN) development; 3) technology supply chains; and 4) AI and biotechnology. It also briefly touches on relevant efforts that are embedded within other Quad working groups and initiatives. Overall, Quad undertakings in this issue area have aimed at creating an open, accessible, and secure technology ecosystem.

*Figure 1. Quad Organizational Schematic as of September 2024* [3]

First, the Quad Principles on Technology Design, Development, Governance, and Use were launched in 2021 to address standards, emphasizing the importance of support for universal values, building trust, integrity, and resilience, and fostering healthy competition and international collaboration to advance the frontier of science and technology.[4] The Quad also launched two Track 1.5 dialogues on AI and Advanced Communications Technologies to promote international standardization cooperation.

Second, the Quad has been active in promoting 5G diversification and Open RAN development, largely due to concerns about the potential security risks posed by the involvement of Chinese companies in the 5G supply chain. In 2022, the four governments signed a Memorandum of Cooperation on 5G Supplier Diversification and Open RAN to foster technical exchanges and testbed activity to advance interoperability and telecommunications cybersecurity. In 2023, the Quad released an Open RAN Security Report and announced its first Open RAN deployment in the Pacific to support the telecommunications ecosystem in Palau. The Quad also announced plans to increase support for ongoing Open RAN field trials and the Asia Open RAN Academy (AORA) in the



QUAD LEADERS' SUMMIT

- Health
  - Vaccine Partnership
  - Vaccine Experts Group
  - Health Security Partnership
  - Cancer Moonshot
- Climate
  - Shipping Task Force
  - Clean Hydrogen and Ammonia Partnership
  - Climate Information Services Initiative
  - Clean Energy Supply Chain Principles and Diversifitcation Program
  - Indo-Pacific Oceans Research Alliance (QIPORA)
- Critical and Emerging Technologies
  - Semiconductor Supply Chain Initiative
  - Track 1.5 Open RAN, AI, & Adv Comm Tech Dialogues
  - Technical Standards Contact Group
  - International Standards Cooperation Network (Q-ISCN)
  - AI-ENGAGE Initiative
  - BioExplore Initiative
- Infrastructure
  - Infrastructure Fellowship
  - Partnership for Cable Connectivity and Resilience
- Cybersecurity
  - Senior Cyber Group
  - Cyber Challenge
  - Cyber Boot Camp
- Space
  - Extreme Precipitation Steering Committee
  - Commercial Space Cooperation
  - Space Situational Awareness
- Maritime
  - Indo-Pacific Partnership for Maritime Domain Awareness
  - Partnership for Humanitarian and Disaster Relief in the Indo-Pacific
  - Maritime Initiative for Training in the Indo-Pacific
  - Ports of the Future Partnership
  - Indo-Pacific Logistics Network
- Other Initiatives and Working Groups
  - STEM Fellowship
  - Investor Network (QUIN)
  - Export Credit Agencies MOC
  - Countering Disinformation Working Group
  - Counter Terrorism Working Group

Philippines, including expansion of AORA to South Asia and the possibility of additional projects in Southeast Asia.[5]

Third, on technology supply chains, the Quad governments have mapped their collective capacity and vulnerabilities in global semiconductor supply chains, launching the Common Statement of Principles on Critical Technology Supply Chains to provide a cooperative foundation for enhancing regional resilience. They also finalized a Memorandum of Cooperation for a Semiconductor Supply Chains Contingency Network.

Fourth, the Quad has addressed AI by announcing the Advancing Innovations for Empowering NextGen Agriculture (AI-ENGAGE) initiative in 2023 to harness AI, robotics, and sensing for agriculture. The four governments are also seeking interoperability among artificial intelligence governance frameworks being discussed in various forums. On biotechnology, the Quad announced plans to launch a BioExplore Initiative to support joint AI-driven exploration of non-human biological data across all four countries. This project will also be underpinned by the forthcoming Quad Principles for Research and Development Collaborations in Critical and Emerging Technologies.[6]

Fifth, outside the Critical and Emerging Technologies Working Group, there are also other projects related to critical and emerging technologies that are embedded in other Quad structures. For example, the Cyber Security Working Group and the Quad Partnership for Cable Connectivity and Resilience are both engaged in important work in this area. In addition, the Quad Investors Network (QUIN) is a nonprofit initiative that was launched to accelerate investments in critical and emerging technologies by bringing together investors, entrepreneurs, technologists, and public institutions. Moreover, related discussions are also taking place through other streams of Quad dialogues; for example, semiconductors and other critical and emerging technology issues were expected to be on the agenda at the inaugural meeting of Quad commerce and industry ministers.[7]

## The Quad as a Building Block for Regional Engagement

Although there is currently limited interest among the Quad governments in formally expanding the grouping's membership, the four governments have demonstrated increasing attention to providing public goods to the Indo-Pacific region over time, and considerable mutual benefits can be achieved through informal engagement between the Quad countries and other partners.[8] As an informal organization, the Quad's strength stems from its ability to bring together like-minded countries for specific common purposes and to catalyze action flexibly at the top leadership level. How can the Quad build on its existing activities to become a platform for broader regional collaboration on critical and emerging technologies?

First, in terms of the menu of options for engagement, the Quad can help facilitate engagement with specific individual Southeast Asian countries or with the Association of Southeast Asian Nations (ASEAN) at several different levels, ranging from shallow to deep: consultation (i.e., exchanging information), coordination (i.e., deconflicting or harmonizing policies), and cooperation (i.e., acting jointly to achieve a common aim).[9] All three types of engagement are essential in the realm of critical and emerging technologies, and acting together as the Quad instead of as four individual governments can be more effective and efficient when trying to expand engagement to additional partners.[10] Over time, this engagement may progressively deepen from consultation to coordination to cooperation, but this is not necessarily required: consultation may be sufficient to accomplish some shared goals, while other goals may demand more concerted cooperation.

Second, the Quad's institutional structures can be used a building block for broader regional engagement, without formally expanding its membership.[11] This type of collaboration has sometimes been referred to as "Quad Plus," but there is no agreed-upon definition of this term. At the most informal level, the Quad's existing working groups and initiatives can be used as hubs to scale up existing Quad initiatives to include Southeast Asian partners, increasing the benefits for everyone involved, and Southeast Asian partners can also be invited to consult with Quad governments through these institutional structures to help inform future initiatives. A more formal possibility might look similar to the "ASEAN Plus X" model, with the Quad governments bringing in additional partners on an ad hoc basis, or it could take the form of a standing Quad-Plus grouping. The following section discusses ways to conceptualize and operationalize opportunities for this kind of engagement.

## Policy Recommendations to Advance Quad Engagement with Southeast Asia: Considering Consumers, Producers, Adopters, and Influencers

Given the potential opportunities, where are the most promising avenues for the countries of the Quad and Southeast Asia to advance a more resilient technological ecosystem? Policymakers can benefit from thinking of four potential overlapping roles for Southeast Asian countries in this ecosystem: as consumers, as producers, as adopters, and as influencers. These roles are intertwined and overlapping. Although there is often a tendency to see the developing countries of Southeast Asia as consumers of technologies and adopters (or "takers") of technology standards, experts and policymakers from these countries increasingly express the desire to play larger roles as producers and as influencers (or "makers") of standards.[12]

By conceptualizing regional engagement in terms of these loosely defined roles, policymakers can formulate a comprehensive set of policy recommendations on critical and emerging technologies. Since these roles are interconnected, the related policies can be mutually reinforcing. For example, an actor may be more likely to become an adopter of a specific standard if it also played a role in influencing it. Similarly, relocating production to a country may increase consumption of the product in that country by improving local market access. These roles are helpful in thinking not only about partnerships with Southeast Asian countries but also with other countries around the world.

## Consumers

Southeast Asian countries play an important and growing role as consumers in the technological ecosystem, so it is important to consider which technologies their governments and their people currently purchase to advance their own developmental and social goals and which will they choose in the future. For example, Quad governments have expressed concerns about risks posed by 5G technology involving Chinese providers, advocating for 5G diversification and the adoption of Open RAN as a more secure alternative. However, if Quad governments wish for their recommendations to become reality, their preferred providers and technologies need to win over consumers in places such as Southeast Asia. The decisions of these consumers impact the security of Quad countries because vulnerabilities in one country's tech ecosystem create vulnerabilities for other interconnected partners. From a consumer perspective, Chinese products are generally attractive because they provide functionality at an affordable price; therefore, ensuring that more secure technologies succeed means also ensuring that they are competitive enough in terms of cost and features to appeal to consumers.

To address these factors, Quad governments can engage in information sharing and capacity building to help Southeast Asian governments and citizens make their own informed decisions about purchasing specific technologies. In addition, to appeal to price-conscious Southeast Asian consumers, Quad governments can cooperate to bring down the cost of Open RAN and other technologies from trusted providers. These policies can encourage consumers to buy more secure technologies.

## Producers

Southeast Asian countries also play important roles as producers: how are companies and individuals in these countries involved in making critical and emerging technologies? Many Southeast Asian governments hope to create jobs, attract investment, and foster indigenous innovation in tech industries to boost their economic development. This desire complements the desire of Quad governments to diversify their technology supply chains to Southeast Asia away from China to bolster their resilience and strengthen their economic security. The producer role can be complex, since companies from these countries may be competing with one another, but nonetheless, there are many complementarities among the capacities of the Quad and Southeast Asia.

With respect to the producer role

of Southeast Asian countries, Quad governments have several potential policy options related to technology supply chains. First, they can expand their current efforts to map collective capacity and vulnerabilities in global semiconductor supply chains to include Southeast Asian countries. Second, Quad governments can consult with Southeast Asian partners regarding their existing workforce capacity in relevant tech industries, and then Quad governments can coordinate and cooperate to provide capacity building to train a skilled tech workforce, which will support supply chain relocation. Third, Quad governments can coordinate to locate some parts of supply chains for Open RAN, semiconductors, and other technologies in Southeast Asian countries.

There are also opportunities to tie Southeast Asian producers into other kinds of Quad initiatives. For example, the Quad Investors Network can encourage cooperation with Southeast Asian actors in private sector opportunities relevant to critical and emerging technologies. Governments from the Quad countries and Southeast Asian countries may also cooperate with ASEAN to expand the Quad STEM Fellowship, or they could coordinate to create a similar parallel program for Southeast Asia.

### Adopters

International technology standards have long been subject to geopolitical competition, and while the US and Europe have traditionally adopted a more bottom-up, laissez-faire approach to standard setting, they are now adjusting their strategies to compete with the rise of China's relatively top-down, government-led approach.[13] Many Southeast Asian countries are currently in the position of being adopters—or "standard takers"—who adopt rules set by the US, Europe, or China, rather than "standard makers" who set the rules. However, the decisions of these countries as adopters are important in determining which standards attract enough followers to achieve market dominance in the future. Therefore, it is essential to consider which standards their governments and companies will choose to adopt for telecommunications, artificial intelligence, and other critical and emerging technologies.

There are clear areas for Quad governments to reach out to Southeast Asian partners as potential adopters of standards. Southeast Asian governments may consider coordinating their policies with standards that the Quad has formulated, such as the Quad Principles on Critical and Emerging Technology Standards, the Quad Common Statement of Principles on Critical Technology Supply Chains, the Quad Principles on Technology Design, Development, Governance, and Use, and the forthcoming Quad Principles for Research and Development Collaborations in Critical and Emerging Technologies.

This coordination can help to broaden support for responsible practices in these areas. Southeast Asian governments may also consider coordinating their policies with other relevant Quad principles, such as the Critical Infrastructure Principles and the Software Security Principles. Adoption of some or all of these standards by Southeast Asian countries can serve as a foundation for deeper engagement in the future.

### Influencers

Although Southeast Asian actors are currently not at the forefront of writing the rules for critical and emerging technologies, they have a vested interest in these rules and an increasing desire to influence them, so it is necessary to reflect upon how technology standards can be formulated in ways that are more inclusive of—and therefore appealing to—countries from this region. In ongoing discussions about emerging technologies such as artificial intelligence, for example, state and non-state actors from Southeast Asia have expressed their desire to influence their future regulation and to have their data used in responsible ways. Including stakeholders from Southeast Asia and beyond should also increase the appeal of the resulting standards, leading them to be more readily adopted, as discussed in the previous section. When considering Southeast Asian countries as potential influencers or "makers" of standards, Quad governments can expand opportunities for Southeast Asian state and non-state stakeholders to consult in the development of principles and standards for critical and emerging technologies. Although these efforts will take more time and energy, they will increase buy-in from Southeast Asian actors.

## Conclusion

This article has argued that the Quad can be used as a building block for broader regional engagement with Southeast Asian countries on critical and emerging technologies through a combination of consultation, coordination, and cooperation. Without expanding Quad membership or creating new institutions, the existing working groups and initiatives of the Quad can be used as hubs to scale up initiatives, expand benefits, and broaden policy coalitions. In addition, by conceptualizing regional engagement in terms of consumers, producers, adopters, and influencers, policymakers can formulate a comprehensive set of policy recommendations on critical and emerging technologies that will generate mutually reinforcing outcomes.

Throughout this process, building trust is essential to advancing engagement on critical and emerging technologies among the Quad and Southeast Asia. These countries do not necessarily share the same concerns about economic security or perceive potential threats in similar ways. Instead, each country has its own distinct interests and interpretations of current technological trends. However, by understanding the various roles that countries play in the technology ecosystem, policymakers can better understand areas of complementarity and find mutually beneficial pathways forward.

## Notes

1 Husanjot Chahal et al., "Assessing AI-Related Collaboration between the United States, Australia, India, and Japan" (Washington, DC: Georgetown Center for Security and Emerging Technology, May 2022).

2 See for example, Jolyon Ford and Damian Clifford, "Embracing Difference: Governance of Critical Technologies in the Indo-Pacific," Quad Tech Network Series (Acton: The Australian National University, February 2021).

3 Adapted from Garima Mohan and Kristi Govella, "The Future of the Quad and Emerging Security Architecture in the Indo-Pacific" (Washington, DC: The German Marshall Fund of the United States, June 2022).

4 The White House, "Quad Principles on Technology Design, Development, Governance, and Use," September 24, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/.

5 The White House, "Fact Sheet: 2024 Quad Leaders' Summit," September 21, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/09/21/fact-sheet-2024-quad-leaders-summit/.

6 The White House.

7 US Department of State, "Digital Press Briefing with National Security Council Director for Indo-Pacific Affairs Josh Rubin, US Deputy Assistant Secretary of State for East Asian and Pacific Affairs Camille Dawson, and Deputy Assistant Secretary of State for South and Central Asian Affairs Nancy Izzo Jackson," September 23, 2024, https://www.state.gov/digital-press-briefing-with-national-security-council-director-for-indo-pacific-affairs-josh-rubin-u-s-deputy-assistant-secretary-of-state-for-east-asian-and-pacific-affairs-camille-dawson-and-depu/.

[8] Garima Mohan and Kristi Govella, "The Future of the Quad and Emerging Security Architecture in the Indo-Pacific" (Washington, DC: The German Marshall Fund of the United States, June 2022).

[9] Kristi Govella, Garima Mohan, and Bonnie Glaser, "Expanding Engagement among South Korea and the Quad Countries in the Indo-Pacific" (Washington, DC: The German Marshall Fund of the United States, May 17, 2022).

[10] Manoj Harjani, "Envisioning a 'Quad Plus' in Southeast Asia," Asia Dispatches, Wilson Center, August 20, 2024, https://www.wilsoncenter.org/blog-post/envisioning-quad-plus-southeast-asia.

[11] Kristi Govella, "Introduction," in Building a Quad-South Korea Partnership for Climate Action, ed. Kristi Govella (Washington, DC: The German Marshall Fund of the United States, 2022), 3–5.

[12] See for example, Elina Noor and Mark Bryan Manantan, "Raising Standards: Data and Artificial Intelligence in Southeast Asia" (Washington, DC: Asia Society Policy Institute, 2022), https://asiasociety.org/policy-institute/raising-standards-data-ai-southeast-asia.

[13] Nicholas Zúñiga et al., "The Geopolitics of Technology Standards: Historical Context for US, EU and Chinese Approaches," International Affairs 100, no. 4 (2024): 1635–52.

# Quad and Southeast Asia: Building trust and partnership in AI Policy in Indo-Pacific

Merve Hickok

## Key Highlights:

- The AI policy and governance landscape in Indo-Pacific is fragmented. However, there is significant opportunity to converge.
- The relationship between Quad and Southeast Asian countries needs to move from a rule-maker and rule-taker one to that of a partnership.
- It is in the interest of both Quad and the Southeast Asian countries to coordinate and cooperate on AI governance.

## Policy Recommendations:

- Establish an AI governance and interoperability fund to build capacity in AI governance and tech stack
- Meet Southeast Asian countries where they are and proactively engage towards convergence on AI governance
- Coordinate and cooperate on AI policy and governance to avoid regulatory havens.

AI governance has been a hot topic of conversation and deliberation across the world, and in many international and regional institutions for many years. Since 2016, we have seen a proliferation of policy frameworks and a high-level consensus on the values and principles that should be embedded in AI systems. Some of these include the OECD AI Principles, the UNESCO Recommendations on Ethics of AI, the EU AI Act, the UN AI Resolutions, as well as the Hiroshima AI Framework and the Council of Europe's Treaty on AI.

However, different socio-cultural contexts, as well as varying digital maturity levels and innovation capabilities across countries can impact AI policy and regulations—complicated further by power imbalances and geopolitical issues that pervade these regions.

The Indo-Pacific region is one such example, encompassing almost three-quarters of the world's population, and accounts for more than 60% of the world's GDP.[1] Its vibrant and energetic technological landscape, home to some of the world's leading countries in semiconductors and robotics, places the region as a nexus for AI. Japan, China, India, South Korea and Singapore also play crucial roles in AI governance. ASEAN countries, on the other hand, prioritize capacity-building and AI implementation to increase their economic competitiveness. Compared to its European and African partners, which have established EU-wide regulations and continent-wide strategies respectively, the AI policy landscape in the Indo-Pacific region remains fragmented. The Indo-Pacific is not a single internal market with harmonized rules. Fragmentation on AI policy in the region can be prone to exploitation by powerful nations and large technology companies, while creating legal uncertainty and additional burdens for smaller enterprises. Quad countries can work with the Southeastern Asian countries in the region to address the gaps and shape a more cohesive approach. Collaboration and trust building in such work is critical to negate the existing frustrations on rule-maker vs rule-taker divisions.

Several Southeast Asian countries walk on a tight rope when it comes to forging alliances and strengthening economic relations in the region. There are significant trade and security dependencies in the region on China, while at the same time some of these countries are aspiring to advance their democracies. Many of the Southeast Asian countries are interested in building partnerships where their voices are heard, where they are respected as partners, where they are not subject to unilateral change of status quo by policy shifts or by use of force. The smaller countries of the region are concerned about the changes in the United States administrations, and its implications for the region. They are equally concerned about policy changes from China, in response to the United States and its allies. Restrictions around AI technology best exemplifies this lopsided relationship. American or Chinese unilateral decisions on export controls on advanced chips and models, tariffs, restrictions in trade of goods, raw materials or energy all mean that the region suffers the consequences. An alliance with the US may be critical for some of these countries. However, given the region's trade relationships, security concerns, and interactions with China, there is also a need to engage with China in constructive ways. As Japan Prime Ministers Fumio Kishida and Shigeru Ishiba have stated, relations with China must nurture "a mutually beneficial relationship based on common strategic interests" and "a constructive and stable relationship." In the region, "cooperation and division are intricately intertwined."[2]

This analysis assesses the current AI policy and regulatory landscape in the Indo-Pacific and provides policy recommendations on how Quad countries and Southeast Asia can build trusted partnerships. Partnerships between Quad countries and Southeast Asian can be strengthened by:

- Investment in the AI capacity-building and transparent infrastructures
- Proactive efforts to engage and converge on AI governance
- Coordinate and cooperate to avoid regulatory havens

# State of AI policy and regulatory landscape in the Indo-Pacific

The current AI policy landscape in the Indo-Pacific reflects more fragmentation than other regions of the world. Several major countries have published their national AI strategy, and a few introduced legislations focused on AI and its impact on society. One unifying element is the overlaps in representation in international organizations such as UNESCO, OECD, G7 and G20. These organizations established major AI policy frameworks over the last few years.

# A look at national AI strategies in Indo-Pacific countries

### Japan

Japan's national AI strategy focuses on accelerating AI adoption in traditional and small businesses to resolve some of its fundamental issues in labor shortage, aging population, and disaster response. Japan aims to become the "world's most AI-friendly country." With this strategy, AI is expected to be deployed in every aspect of daily and commercial life. In the meantime, Japan is  focused on ensuring that risks from AI  are mitigated.  Japan led several critical governance initiatives internationally, such as its hosting of the G7 Summit in 2016, where the East Asian nation introduced AI principles to gather consensus on future AI governance.[3] These principles are very similar to the final ones adopted by OECD and then G20 later.[4] Several years later, Japan repeated its initiative in response to the introduction of generative AI and has led the development of Hiroshima AI Process Framework in 2023.[5] Domestically, Japan passed its first AI-specific legislation. Act on the Promotion of Research, Development, and Utilization of Artificial Intelligence-Related Technologies" to encourage both businesses and individuals to adopt AI to create new economic opportunities and solutions.[6]

### India

India's national AI strategy focuses on using AI for economic growth and social development, especially in healthcare, agriculture, education, smart cities, and infrastructure. Its government believes that AI should be accessible to everyone and benefit all layers of society. With a focus on scalable and practical solutions and the launch of its AI for All campaign, India is interested in being a model which can be "replicated in other similarly placed developing countries."[7] Meanwhile, the country is committed to advancing global consensus on AI governance.

### South Korea

Similar to India, South Korea's national AI strategy focuses on economic vitality, competitiveness and improving the life of its citizens.[8] South Korea is one of the first countries in the region to introduce AI-specific regulations. It has been active in aligning its national framework with other globally recognized AI governance ones.[9]

### Singapore

Despite its size,  Singapore has emerged as one of the leading countries in AI governance. In 2019, Singapore released its first edition of the Model AI Governance Framework[10] – one of the pioneering governance frameworks in the region at the time. While it is not a member of OECD, and while its principles omit references to privacy, the Framework remains consistent with governance frameworks that followed. Like India, Singapore's focus has been on deploying scalable AI solutions in sectors most impactful to its citizens and businesses.[11]

### China

China launched its New Generation Artificial Intelligence Development Plan in 2017, which outlines three phases for achieving this ambition: leadership in technology and applications by 2020, major breakthroughs by 2025, and the world's primary AI innovation center by 2030.[12] China's AI policy benefits from state-funded research, extensive data collection and ability of state to impose certain values to be reflected in the privately developed AI systems. As Xu argues, Chinese regulators are most concerned about the "ideological and political implications of algorithmic applications" on the population.[13] While China's Ethical Norms for New Generation AI are similar to OECD AI Principles or the Europe's Guidelines for Trustworthy AI, the spirit and focus are different. The Interim Administrative Measures for Generative Artificial Intelligence Services came into effect in 2023.[14] AI products are expected to promote social harmony and positive energy. China has been experimenting with many AI regulations and is pushing the boundaries of AI governance possibilities. Over the years, China has introduced many interim measures requiring companies to provide more transparency, explainability and bias assessments for their algorithms. Although AI policy documents refer to 'right to know' and 'rights to choose' , these only apply to commercial products. AI-related rules in China target major AI companies and platforms, rather than how the state itself uses this powerful technology.

The influence of Chinese AI software and hardware raises concerns about data privacy, surveillance, and social manipulation both domestically, and when exported to other countries. One of the most critical aspects is that the AI-powered products exported by China can lay the infrastructure for mass surveillance. Such an infrastructure gives the importing countries advanced abilities to monitor their population. The undemocratic values are embedded into the enabling hardware.

## Regional level

The Quadrilateral Security Dialogue (Quad): The Quad is an alliance between the United States, Australia, India, and Japan committed to maintaining a peaceful, stable, and prosperous Indo-Pacific region. The grouping was revived under the first Trump administration in 2017 and received bipartisan support in the US. In 2021, President Biden hosted the first in-person Quad Leaders' Summit, underscoring Washington's commitment to stability in the Indo-Pacific region. One of the outcomes of this Summit was reiterating commitment to 'building quality infrastructure in the Indo-Pacific region' – especially in the critical and emerging technologies.[15] The "Quad Principles on Technology Design, Development, Governance, and Use" affirm that the ways in which "technology is designed, developed, governed, and used should be shaped by our shared democratic values and respect for universal human rights."[16] It is important to remember that Quad Principles sit between the OECD AI Principles of 2019, UNESCO Recommendation on Ethics of AI of 2021 and more recently the Hiroshima AI Framework of 2023.[17] Quad Principles provide a bridge and continuity for these principles. The first meeting of the Quad with the new Trump administration confirmed reiterated a commitment to this group.[18] In July 2025, the Quad Foreign Ministers Meeting cemented commitments to deepening research and expanding their work on AI in the Indo-Pacific. [19]

### Free and Open Indo-Pacific (FOIP)

In 2016, Prime Minister Abe Shinzo's government introduced FOIP vision, a set of principles for peace, economic prosperity, regional stability and security in the region – while countering Chinese ambitions in Asia with increased diplomacy. This approach was adopted by the first Trump administration national security apparatus. Former PM Kishida updated Japan's Free and Open Indo-Pacific policy by a renewed focus on 1) Promotion of "business and human rights" as international value achieved through "support for development and operation of laws, regulations and policies to protect the rights of workers, of human rights due diligence" and "capacity-building of government agencies in developing countries through technical cooperation,"[20] and 2) Ensuring a free, fair and secure cyberspace to "strengthen capacity building in the field of cybersecurity" and translating shared knowledge and understanding into "formulating international rules, and confidence building measures."[21] As it relates to AI policy in the region, this approach can significantly contribute to AI safety and security capacity building partnerships in the region. Similarly, a focus on human rights-centered AI governance in private sector can create soft change.[22]

## Path to trusted partnerships between Quad and Southeast Asian countries

Strengthening the relationships between Quad and Southeast Asian countries will require a multi-pronged approach. This approach needs to translate existing commitments into actual implementations. Since 2019, Quad countries either led or endorsed several major AI policy frameworks. Now is the time to reflect these in both domestic AI policies, and the regional investments.

## Investment in the AI capacity-building and transparent infrastructures

In most cases, Southeast Asian countries are deployers of AI. Their national policies are focused on using AI to expand public services, improving everyday lives of their populations, and boosting their economies, particularly for industries such as e-commerce, digital services, and tourism.

Not every nation in the world needs to pour resources into hyperscale AI infrastructure. However, each country does need a clear pathway to ensure AI works for its needs and priorities, and it has internal capacity to deploy and govern AI in a way that is safe and secure for its people. A critical step for Quad countries would be to further invest in the AI governance capacity-building in the region. Quad countries already have deep commitments to transparency, accountability, robustness and inclusivity in AI governance. Their investments must reflect such norms. Critical infrastructure technology and capacity building can be thought of as the manifestation of values and priorities. Technology is never neutral. It comes with embedded values and choices. Sometimes those choices allow parties to have asymmetric power over others. For example, the choice to invest in Chinese surveillance technology, communication monitoring, or kill switches for a country's internet access to outside world are all intentional decisions by governments. Assistance in the form of low-cost, AI-based surveillance infrastructure can pave the way for the recipient country to move away from human rights, the rule of law, and freedom of expression. Once in place, such infrastructure rarely goes away. Investing in AI-related capacity building can be twofold – covering both the technological stack (both hardware and software) within the public infrastructure and building human capacity.  The AI infrastructure investments need to go hand-in-hand with upskilling human capital. Quad can establish an AI governance and interoperability fund to promote AI governance in both public and private sector. The fund could support projects which advance better understanding of regional sensitivities in governance.

## Proactive efforts to engage and converge on AI governance

Since 2019, several AI policy frameworks have been developed by international organizations. First major framework was introduced by The Organization for Economic Co-operation and Development (OECD) in 2019.[23] OECD's AI Principles were also endorsed by G20 countries shortly afterwards. In 2021, UNESCO Recommendation on Ethics of AI was endorsed by 193 countries.[24] The Council of Europe finalized the first treaty on AI in 2024.[25] The Hiroshima AI Process was launched and completed by the G7 under Japan's presidency in 2023 to respond advanced AI systems.[26] However, each of the organizations involved in the development of these frameworks suffer different limitations. AI governance can be more effective and inclusive by widening the net.

OECD AI Principles influenced many of the other AI governance deliberations which followed. However, OECD, an organization representing democracies with market-based economies has its representational shortcomings. The Global Majority countries do not have a voice at the table. The same shortcoming applies to both G7 and G20, although the latter recently welcomed the African Union as a +1 member. The Council of Europe has 46 member states and the European Union, and many observer states which actively participated in its treaty negotiations. However, Council of Europe Framework Convention on AI is open to any state to sign. UNESCO can boast for the most inclusive framework, although a legally non-binding one.

Several opportunities arise here. First, Quad countries can engage with the countries in the region to understand better the cultural nuances, differences and priorities reflected. Especially for the United States, understanding the diversity and gaps in governance approaches can help identify impactful opportunities and mutual learning. There is already an opening for further cooperation in this realm. The ASEAN Digital Masterplan 2025 highlights the need for a digitally enabled society and economy across the ASEAN, with a need to "build trust in digital services and to harmonize regulation and standards across ASEAN."[27] The ASEAN Guide on AI Governance and Ethics, highlights the importance of incorporating cultural and linguistic differences across the region.[28] The Guide reflects many of the globally established norms for governance, and in fact recommends "ASEAN should prioritize alignment and interoperability with the work of bodies like ISO, NIST, and the OECD to reduce fragmentation and support cross-border trade."[29] ASEAN Community Vision 2045, adopted at the 46th ASEAN Summit in May 2025, further reiterates commmitment to "principles of democracy, the rule of law and good governance, respect for and protection of human rights and fundamental freedoms" while advancing "productivity and innovation-driven growth, and incorporating sustainability across and along the value chain." [30]

Second, the Quad can contribute to further convergence on AI governance by supporting the engagement of these countries with the likes of OECD and G7 in more meaningful ways – similar to Japan's initiative with the Hiroshima AI Process Friends Group. After completing its G7 Presidency in 2023, Japan embarked on expanding support. The Friends group countries voluntarily endorse the spirit of the Hiroshima AI Process, toward achieving safe, secure, and trustworthy AI and commit to its implementation. As of December 2024, the group has endorsement from 60 countries (including Thailand, South Korea, Viet Nam, Singapore, Cambodia and Lao) plus the European Union, a number far beyond the initial G7 countries. Given that ASEAN Guidance on AI Governance also favors interoperability with OECD, there is a significant opportunity for the Friends Group to bring together the rest of the Southeast Asian countries. [31]

Third is to encourage Southeast Asian countries to sign the Council of Europe's Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law. The Convention is the first-ever international legally binding treaty. Although it was drafted by the COE member and observer countries, the Convention can be signed and ratified by any country in the world. The 'framework' convention does not prescribe how countries should implement the obligations. The flexible implementation approach respects the legal and cultural differences, as long as the countries are committed to the norms enshrined.

## Avoiding regulatory havens

For the last few years, a false narrative of "regulation impeding innovation" has been pushed forward by those with vested interests. Stringent regulations that do not take the existing regulations into account may create confusion and frustration with the private sector. However, a total lack of regulation where there are known risks and harm creates bigger problems in the long run. Regulation can provide clarity to the private sector and establish the contours of expected behavior. This takes away the gray zones and unknowns for the companies and makes it easier for them to invest and develop AI systems. Regulation can put safety and security obligations in place, so companies prioritize safety over short-term gains. Regulation can help narrow the power imbalance between individuals and corporations by imposing liability for harms. In the long run, regulations contribute to better and safer products. Regulation helps build trust with consumers, citizens and businesses.

In a global race to attract more AI-related investments, some countries may be tempted to offer more relaxed regulatory environments to global companies, with unbounded access to data and energy. One can draw a parallel to tax havens such as some Caribbean islands that host offshore financial wealth, or banking secrecy havens such as Switzerland. However, such an AI policy may be short-sighted for the host country. Major AI companies may benefit from local data collection, energy subsidies, or other regulatory protections without reciprocating long-term investments into the country. Powerful nations may exploit the lack of guardrails. Such regulatory havens for AI companies can also undermine the AI governance cooperation efforts globally.

It is in the interest of both Quad and the Southeast Asian countries to coordinate and cooperate on AI governance, rather than undermining each other's efforts and becoming testbeds and experiments for more powerful actors.

## Notes

[1] The U.S. Department of State. The Indo-Pacific Strategy. https://www.state.gov/indo-pacific-strategy/

[2] Prime Minister's Office of Japan. Policy Speech by Prime Minister KISHIDA Fumio at the Indian Council of World Affairs (ICWA). March 20, 2023. https://japan.kantei.go.jp/101_kishida/statement/202303/_00013.html

[3] Ministry of Internal Affairs and Communications AI Network Society Promotion Council. Draft AI Development Guidelines for International Discussion, 2016. https://www.soumu.go.jp/main_content/000507517.pdf

[4] Center for AI and Digital Policy. AI and Democratic Values Index. 2024. https://www.caidp.org/reports/aidv-2023/

[5] Hiroshima AI Process. 2023. https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html

[6] Cabinet Office, 'Act on the Promotion of Research, Development, and Utilization of Artificial Intelligence-Related Technologies'. 2025. https://www.cao.go.jp/houan/pdf/217/217anbun_2.pdf

[7] NITI Aayog, National Strategy for AI. 2018. https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf

[8] Government of Republic of Korea. The National Strategy for Artificial Intelligence of Korea. 2019. https://www.msit.go.kr/bbs/view

[9] Center for AI and Digital Policy. AI and Democratic Values Index

[10] Personal Data Protection Commission of Singapore. Model AI Governance Framework. 2019. https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework

[11] Center for AI and Digital Policy. AI and Democratic Values Index

[12] The People's Republic of China State Council. New Generation Artificial Intelligence Development Plan. 2017. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

[13] Jian Xu. Opening the 'black box' of algorithms: regulation of algorithms in China. 2024. https://www.tandfonline.com/doi/full/10.1080/22041451.2024.2346415

[14] Cyberspace Administration of China. The Interim Administrative Measures for Generative Artificial Intelligence Services. 2023. https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm and  https://www.chinalawtranslate.com/en/generative-ai-interim/

[15] Quad Leaders' Summit. Fact Sheet. 2021. https://www.mofa.go.jp/files/100238181.pdf

[16] The White House. Quad Principles on Technology Design, Development, Governance, and Use. 2021. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/

[17] Hiroshima AI Process.

[18] The U.S. State Department. Joint Statement by the Quad Foreign Ministers. January 2025. https://www.state.gov/joint-statement-by-the-quad-foreign-ministers/

[19] The U.S. State Department. 2025 Quad Foreign Ministers' Meeting Fact Sheet. July 2025. https://www.state.gov/releases/office-of-the-spokesperson/2025/07/2025-quad-foreign-ministers-meeting

[20] Prime Minister's Office of Japan. Policy Speech by Prime Minister KISHIDA Fumio at the Indian Council of World Affairs (ICWA).

[21] Ministry of Foreign Affairs of Japan. Addressing Challenges in an Indo-Pacific Way. 2023. https://www.mofa.go.jp/files/100484659.pdf

[22] United Nations Human Rights Council. "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework". 2011. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

[23] OECD. AI Principles. 2019. https://oecd.ai/en/ai-principles

[24] UNESCO. Recommendation on Ethics of AI. 2021. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence

[25] The Council of Europe.  Framework Convention on artificial intelligence and human rights, democracy, and the rule of law. 2024. https://www.coe.int/en/web/portal/-/council-of-europe-opens-first-ever-global-treaty-on-ai-for-signature

[26] Hiroshima AI Process. 2023. https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html

[27] ASEAN. Digital Masterplan. 2025. https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

[28] ASEAN. Expanded ASEAN Guide on AI Governance and Ethics – Generative AI. 2025. https://asean.org/wp-content/uploads/2025/01/Expanded-ASEAN-Guide-on-AI-Governance-and-Ethics-Generative-AI.pdf

[29] ASEAN. Expanded ASEAN Guide on AI Governance and Ethics – Generative AI

[30]  ASEAN. Community Vision 2045: ASEAN COMMUNITY VISION 2045 "Resilient, Innovative, Dynamic, and People-Centred ASEAN". 26 May 2025. https://asean.org/wp-content/uploads/2025/05/05.-ASEAN-Community-Vision-2045_adopted.pdf

[31] Hiroshima AI Process. Supporters. December 2024. https://www.soumu.go.jp/hiroshimaaiprocess/en/supporters.html

CONVERGE
INDO-PAC
CRITIC
FORU
PACIFIC FORUM INTERNATIONAL
INDO-PACIFIC CRITICAL TECH FORUM 2024
Maria Monica W

# Building a Trusted ASEAN-QUAD Partnership to Advance Resilient Supply Chains

Maria Monica Wihardja, Ph.D.

## Key Points:

- Increasing economic interdependence in the semiconductor supply chain networks and concentration in only a few firms and a few countries for markets or inputs has prompted the US to put in place a complex set of trade protectionist measures including extraterritorial export controls and foreign direct product rules, with the main target of Chinese entities.

- Given its relatively neutral stance in the US-China geopolitical rivalry and their national strategic policies as well as favourable business climate, Southeast Asian economies have been benefiting from the global supply chain reconfiguration in the semiconductor sector in terms of trade flows, foreign direct investment (FDI) inflows and R&D.

- However, an intensifying US-China trade war, especially under the Trump 2.0 scenario, could more than offset the short-run benefits that some of the Southeast Asian economies have been enjoying while hurting the global supply of semiconductor, the global business environment and the rate of global technological innovation.

## Policy Recommendations

- The IPEF Supply Chain Pillar can be a useful mechanism to build stronger partnership between the Quad and ASEAN in advancing more resilient semiconductor supply chains.

- To win the minds and hearts of ASEAN countries, the Quad could help ASEAN countries build their domestic production and export capacity in the semiconductor industry.

- To build a fair and resilient supply chain, Quad countries could refrain from financing massive subsidies in the semiconductor sector which will create an unfair and uneven level playing field with ASEAN countries who cannot afford to roll out huge subsidy programs because of their fiscal constraints.

- An ASEAN-Quad partnership in advancing more resilient supply chains in semiconductor could also build on ASEAN vision for sustainability, which could further catalyse the Southeast Asian region to build a more sustainable future.

### A. Southeast Asia’s Approach to Semiconductor Supply Chains Amidst the US-China Technology Competition

The global supply chain has evolved over the past 100 years —from those that were mostly local in nature to complex, globalized supply. For example, the Extreme Ultra-Violet (EUV) lithography—a cutting-edge technology for manufacturing the most advanced chips below 7 nanometer process nodes—developed solely by ASML Holding in the Netherlands, contains about 100,000 parts, provided by over 5,000 specialized suppliers spread across the globe.[1]

Increasing economic interdependence in the global semiconductor supply chain networks—where missing a sub-component part can choke off the entire supply chain—and increasing concentration on only a few firms and a few countries for markets and inputs[2] have prompted many countries, especially the US, to diversify, derisk and even decouple.  By the end of 2020, only two companies could manufacture the most cutting-edge chip processors: Taiwan's TSMC and South Korea's Samsung.[3] In fact, Taiwan produces more than 60 percent of the world's semiconductors and over 90 percent of the most advanced ones.[4] As far as the US is concerned, both Taiwan and South Korea are problematic, just being off the coast of China, its strategic competitor.

Semiconductor is the backbone of most advanced technologies. Because of their dual use (the civilian and the military), the US has been restricting the exports of "emerging and foundational technologies" to entities abroad whenever those technologies are "essential to the national security of the US".[5] The main target was China, which has emerged as a science and technology superpower.[6]

Export controls are not new but the US-China strategic rivalry blurs the line between legitimate uses of export controls and economic coercion. Although the idea was to restrict exports exclusively for advanced technologies that could endanger national strategic interest – dubbed as the 'small yard, high fence' strategy – these export restrictions were later expanded in terms of both technologies and entities. In 2020, the 2018 export restrictions to ban Huawei's access to semiconductors were extended to cover all foreign technology that use US chipmaking equipment and software tools (known as the foreign direct product rule).  The extraterritorial foreign direct product rule was applied to Dutch and Japanese semiconductor manufacturing equipment manufacturers such as ASML, the Dutch manufacturer of cutting-edge lithography machines.

In August 2022, the CHIPS Act was issued and in October 2022, a new set of export restrictions were issues to cut off China's access to advanced AI chips and choke point technologies, including AI chip design, electronic design automation software, semiconductor manufacturing equipment, and equipment components.  Export restrictions were expanded into restrictions on direct investment, financial investment, as well as restrictions on individuals who hold US passports from working for Chinese chip companies.

On 3 December 2024, the Biden administration issued the third package of export controls and foreign direct product rules as well as investment controls. It added 140 companies to the Entity List including Chinese semiconductor, semiconductor-manufacturing equipment and software companies.  The controls on products include high-bandwidth memory chips (crucial component for rapid data transfers enabling powerful AI computing), two dozen types of semiconductor-manufacturing equipment and three types of software tools.

Most recently, on 3 December 2024, the Biden administration issued the third package of export controls and foreign direct product rules as well as investment controls. It added 140 companies to the Entity List including Chinese semiconductor, semiconductor-manufacturing equipment and software companies.  The controls on products include high-bandwidth memory chips (crucial component for rapid data transfers enabling powerful AI computing), two dozen types of semiconductor-manufacturing equipment and three types of software tools.

Under the foreign direct product rules, American companies and global companies (regardless of their geographic location) that use US chips or US chip technology will be barred from exporting to China and those in the Entity List unless they receive license exemptions. The new foreign direct product rules will affect semiconductor-manufacturing equipment producers not only in Taiwan and South Korea but also in Southeast Asia, including Malaysia and Singapore, who use US chips or US chip technology destined for China.

## How has the US-China technology trade war affected the Southeast Asian region?

Chip production-related activities, including assembling, packaging and testing, accounts for a significant share of GDP and/or exports of some of ASEAN countries, namely Malaysia, Singapore, Thailand and the Philippines.[7] In Malaysia, for example, semiconductor production accounts for six percent of GDP and 40 percent of exports and in the Philippines, it accounts for almost 60 percent of exports, while in Singapore, the semiconductor industry contributed almost seven percent of its GDP in 2021.[8] ASEAN as a region is the second-largest semiconductor exporter globally with a 22.5 percent share of global semiconductor exports and five ASEAN countries—Malaysia, Singapore, Vietnam, the Philippines and Thailand—are among the world's top 15 semiconductor exporters in 2019.[9] Table 1 shows the spread of specialization in the semiconductor value chain across ASEAN. (See table on the next page)

Because of ASEAN's attempt to stay neutral in the US-China geopolitical rivalry and technological trade war, Southeast Asian economies have been benefiting in terms of trade flows, foreign direct investment (FDI) inflows and research and development (R&D).[10] However, a ballooning of Section 301 Tariffs of the US Trade Act of 1974 on Chinese goods and an expansion of export controls, foreign direct product rules and investment controls, especially under the Trump 2.0 scenario, could more than offset the benefits that some of the Southeast Asian economies have been enjoying including those benefits in the semiconductor sector.

There are at least three channels through which the US-China geopolitical and technological rivalry has impacted the semiconductor sector in Southeast Asia.

First is through trade flows. Changes in trade flows may materialize as:

1. New trade, especially in terms of increased semiconductor exports to the US as China's exports to the US in semiconductor declined because of higher tariffs and other restrictions.  This could be due to enhanced domestic production and export capacity.
2. Old trade being rerouted through some ASEAN countries, especially semiconductor-related exports using US chips or technology from third countries such as Taiwan destined for China, or Chinese semiconductor-related exports going to the US.

The US-China tech war, especially the escalating restrictions to China's access to the US technologies that started in 2018, has been reflected in trade of chip between the two countries, between ASEAN and the US, and between ASEAN and China.[11] The US import share of chip has shown an increasing reliance on ASEAN and a decreasing reliance on China. Both ASEAN and China accounted for 34 percent of US import of chip in 2017—but while ASEAN's share increased to 48 percent in 2022, China's share was halved to 17 percent. China's chip export destination pattern has also slightly shifted. The share of China's chip export to the US dropped from 19 percent in 2018 to 11 percent in 2022, despite the positive trend of US import of chips, increasing from US$79.7 billion in 2018 to US$87.2 billion in 2022. At the same time, the share of China's chip export to the ASEAN countries slightly increased from 18 percent in 2018 to 20 percent in 2022.

| **R&D and design** | **Wafer fabrication** | **Backend manufacturing** |
|---|---|---|
| Malaysia, Singapore, Vietnam, Philippines, Thailand | Malaysia, Singapore | Malaysia, Philippines, Thailand, Vietnam, Indonesia |
| **Engineering software** | **Wafer production** | **Equipment production** |
| Singapore, Thailand | Malaysia, Singapore | Malaysia, Singapore |

**Source: EDB, 2022**

Second is through FDI flows.

There are at least three main reasons for increased investment in the manufacturing sector in Southeast Asia.[12] First, downstream industries such as assembly have been shifting away from China to avoid China's rising labor costs and higher US tariffs, as well as economic sanctions against products coming from China. Second, the supply chains' shift from 'just-in-time' to 'just-in-case' has resulted in significant expansion of production capacity outside China, including in Southeast Asia, as a 'spare' capacity. Third, the adoption of the 'China Plus One' or 'China Plus Two or Three' model by multinational corporations (MNCs) broadens their supply bases outside China while maintaining presence in China. Many ASEAN countries including Singapore, Malaysia and Vietnam have attracted investment in the semiconductor industry given their strategic national policies and favorable investment climate as well as cost advantages in some ASEAN countries (such as Malaysia and Vietnam) and a strong R&D ecosystem as in the case of Singapore.

The numbers are telling. FDI inflows to ASEAN reached an all-time high of US$224 billion and exceeded FDI inflows to China for the second consecutive year in 2022. Manufacturing investments notably scored much stronger growth than in previous years when its share in total FDI inflows to ASEAN rose more than three folds from just nine percent in 2020 to 28 percent in 2022. The electronics and electrical industry accounted for more than 70 percent of new manufacturing investments at US$37 billion, with semiconductors and electronic components alone making up 27 percent of the 70 percent of new manufacturing investment in the electronics and electrical industry. Investment in the electronics industry, which consisted of mostly semiconductors and electronic components, reached US$9.5 billion in 2022, six times the annual average between 2010 and 2019.

At the firm level, international investors in electronics and semiconductors expanded operations and production capacities or turned to ASEAN for the first time to diversify production and stepped into ASEAN supply chain networks. These included:

1. Major MNCs with or without existing footprints in the region.

2. Manufacturers from China and Taiwan Province of China, which invested for the first time in the region as they also follow the 'China Plus One' strategy.

3. Lead firms and their anchor supplies as well as lower-tier suppliers.

Third is through R&D. Although this may only materialize in the long term, we can expect that there will be more technology transfers and semiconductor-related R&D being conducted in Southeast Asia as the industry and domestic production capacity, as well as markets, expand. Most ASEAN countries do not have the capability (e.g., human capital, physical capital, and regulatory ecosystem such as intellectual property and patent laws) to do cutting-edge R&D except Singapore. Moreover, not all ASEAN countries can afford to engage in a subsidy race for R&D.

Technology has also become synonymous with geopolitical alignment and trust is a prerequisite to technology transfers. The US as the largest investor in ASEAN is key to bringing new technology to ASEAN, as investment often comes with technology transfers.

There are at least two recent updates in the second Trump administration that could slow down or even reverse the benefits that Southeast Asian economies have enjoyed partly because of the 'China Plus One' strategy adopted by many multinational companies (MNCs).

First, unlike his first administration, the second Trump administration targets not only China but also Southeast Asian economies with high tariffs. While bilateral deals with the US, especially the China-US trade deal, are on-going and evolving, China's position relative to some ASEAN countries in the second Trump administration could be better compared to its relative position under Trump's first administration. This may mean that, for example, foreign investment in semiconductor may stay rather than leave China.

Second, the second Trump administration has been pushing harder to bring the semiconductor supply chains home. Given Trump's August announcement to impose 100-percent tariffs on imported chips, more MNCs in the chips supply chain are more pressured to invest in the US, especially if their largest clients are in the US. Incorporating the risk and uncertainty of what Trump might do to imported chips, including a possible component tariffs in the future, MNCs have been putting their bets on investing in the US. This means less investment going to Southeast Asia although the impacts might not be felt immediately since it takes time to build a chip fab.

## B. Building a Trusted ASEAN-QUAD Partnership in Advancing Resilient Semiconductor Supply Chains

The Quad as a grouping and/or individual countries could build a stronger partnership with countries in Southeast Asia to advance more resilient semiconductor supply chains. Here are some of the possible approaches:

### 1. Build on existing mechanisms especially IPEF

Invited ASEAN countries (which exclude Lao PDR, Myanmar and Cambodia) have given the US-led Indo-Pacific Economic Framework (IPEF) the benefit of the doubt since its inception in 2022. There ASEAN countries see the initiative as 'all sticks but no carrots' and question its sustainability, effectiveness and credibility.[13]

The initiative comprises four pillars, one of which is the Supply Chain Pillar. The IPEF Agreement Relating to Supply Chain Resilience was the first to be concluded and signed among the 14 IPEF members in 2023. As part of the Agreement, three coordination bodies were established: the Supply Chain Council, the IPEF Supply Chain Crisis Response Network, and the Tripartite Labor Rights Advisory Board.[14]

even ASEAN countries—Malaysia, Singapore, Indonesia, the Philippines, Brunei, Thailand, and Vietnam—are members of IPEF, the Supply Chain Pillar can be a useful mechanism to build stronger partnership in advancing more resilient semiconductor supply chains.

First, despite some scepticism, IPEF has already been perceived as an acceptable platform for the seven ASEAN countries to engage economically with the US and its six partner countries namely Japan, South Korea, Australia, New Zealand, India and Fiji, at least before Trump took office for the second time in 2025. Therefore, there is no need for the US to put any additional efforts into finding a new mechanism or platform to onboard ASEAN countries to engage in building more resilient semiconductor supply chains. Second, given the diversity and natural complementarities of the IPEF members—from mineral-rich Australia and Indonesia to technology-advanced Japan and the US—strengthening cooperation among IPEF members through the Supply Chain Pillar could help build more resilient supply chains in semiconductor. Third, the IPEF supply chain pillar has seen rapid progress, with an agreement being concluded and signed last year and a table-top exercise being conducted under the Supply Chain Crisis Response Network this year.

However, it remains unclear whether the Trump 2.0 administration will pull the US out of IPEF and whether IPEF would survive or continue without the US. The fact the US has pulled out from Trans-Pacific Partnership (TPP) under the Trump 1.0 administration, which was originally driven by the US, gives a negative precedent to IPEF. Similar to TPP, IPEF is an executive order, which does not pass through a parliamentary process, and hence could be relatively easy to reverse by the new administration, except those agreements that have been made legally binding.

By the time this paper is written, it is clear that the second Trump administration focuses on transactional bilateral deals, not plurilateralism or multilateralism. His approach in the Indo-Pacific region is also less about the US's potential strategic role in the region, for example, by being a trusted and credible security guarantor to its allies and friends in Indonesia Pacific, but more about MAGA (Make America Great Again). He even targeted his long-time economic partners and military allies with tariffs such as Japan, South Korea, and Singapore.

By the time of the writing, the US has not pulled out from IPEF. But there are a few possibilities of what could happen to IPEF if the US pulls out. Other countries might take over the leadership of IPEF, similar to Japan taking over the leadership of TPP when the US pulled out of it. Whether or not the US pulls out of IPEF, IPEF might be significantly reduced in its scope, and if some pillars were to be scrapped, it may make sense to keep the Supply Chain Pillar since it is the pillar that has made the most significant progress. If the US pulls out and IPEF continues under a different leadership, the question is whether IPEF membership will change. One implausible but not impossible evolution of IPEF membership if the US pulls out is China joining IPEF. China and Taiwan submitted their bids to join the 12-member Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) although the decision over their applications still remain a contentious issue.[15] But, China can do the same with IPEF.

### 2. Help ASEAN build their domestic production and export capacity

To win the minds and hearts of ASEAN countries, the Quad as a grouping, as well as its individual member-states, could help ASEAN countries build their domestic production and export capacity to reduce dependence on technology imports. This is a preferable strategy to pressuring them to decouple from the Chinese supply chains, which may make them align closer to China. Increased domestic production and export capacity in semiconductor-related industries in ASEAN countries while using existing quid pro quo partnerships such as IPEF for economic cooperation without explicitly restricting their access to the Chinese inputs or market could help build more resilient supply chains in semiconductor with minimal disruptions. Sensitive products could be an exception when it comes to access to the Chinese market.

This strategy could increase both security and prosperity of the Quad and ASEAN countries and avoid cutting into a corner solution of only security but without prosperity, or only prosperity but without security. How to avoid a middle-income trap before getting old is a key economic imperative for many ASEAN countries, including Malaysia, Thailand, Vietnam and Indonesia, and export-led growth—a development model that has helped the four Asian Tigers namely Hong Kong, South Korea, Singapore, and Taiwan progress to becoming high-income countries—is still very much relevant to these middle-income ASEAN countries.[16]

Building domestic production and export capacity as well as domestic competitiveness in the manufacturing sector including the semiconductor industry will help these ASEAN countries achieve the needed higher economic growth rates, build more skilled human capital, and graduate to a high-income country before they get old.

What can the Quad do to help ASEAN countries build their domestic production and export capacity in semiconductors?  It will involve more investment, technology transfers and nurturing more technology talents (e.g., opening opportunities for ASEAN students to study in Japanese and American universities in semiconductor-related technologies).  It will need more than just money but also trust and partnership.

The Quad and ASEAN countries could use existing mechanisms, including IPEF, ASEAN Framework on Integrated Semiconductor Supply Chain, ASEAN Plus One mechanisms—such as with Japan, India, the US, and Australia—, East Asia Summit, Asia-Pacific Economic Cooperation (APEC), and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), to further nurture trust and partnership among Quad and ASEAN.  With emerging ASEAN start-ups working on semiconductor-related areas, Quad countries could also provide seed funding to semiconductor-related startups and their R&D activities.  They can also reach out ASEAN universities to help them build the capacity to nurture students in the semiconductor-related fields. They can help ASEAN countries build their own indigenous MNCs by localizing production.

### 3. Create a level playing field with ASEAN partners

In the world of increasing trade protectionism, massive subsidies in the semiconductor sector by the Quad countries including the US Chips and Science Act will create an unfair and uneven level playing field with ASEAN countries who cannot afford to roll out huge subsidy programs because of their fiscal constraints.  To build a fair and resilient supply chain, there must be some level playing field.  Subsidies have been used by many countries before as part of their industrial policies.  The four Asian Tigers used them extensively before during their high-growth industrialization developmental stage. They are not necessarily welfare-reducing for other countries nor are they always banned by the WTO.  They are exceptions when they can be used and welfare-enhancing.  However, when economic superpowers namely China and the US use them, which also results in a subsidy race, the effects on the middle and small economic powers could be deleterious.

The US has also been considering “component tariffs” where tariffs are imposed based on the origins of the components that make up the final goods, instead of the originating country of the final product.  This is one anti-circumvention strategy to 'punish' manufacturers in ASEAN countries, which are suspected to be conduits of Chinese goods.  A ballooning of tariffs and complexity of tariff regulations will increase the costs of compliance, straining companies' profits; cause supply chain disruptions due to the complex cross-border semiconductor value chains; slow production and even lead to shortages for the downstream industries; impair business and investment climate; and reduce the competitiveness of the overall economy.[17]

If manufacturers in ASEAN countries feel too much pressure because of the intensifying US trade controls, anti-circumvention inspections, and/or protectionist measures, they may decide to leave the US market and align themselves closer with the Chinese supply chains while China will continue to accelerate its 'self-sufficiency' goal in advanced technology as it is increasingly being isolated by the US and its allies.

### 4. Focus on Sustainability

An ASEAN-Quad partnership in advancing more resilient supply chains in semiconductor could build on ASEAN vision on sustainability. It could be weaved into the proposal of "A Single Green Market" as Armstrong and Drysdale from Australian National University suggested in terms of the next-generation regional cooperation.[18] Quad cooperation with ASEAN in building resilient supply chains in semiconductors should not be defined as diversifying away from China, which may make ASEAN countries align closer to China.  It should be defined by an open and transparent trading system and a rule-based international order, both of which have contributed to ASEAN's economic growth performance in the past three decades.

Although the US under the Trump 2.0 administration will presumptively be absent from any climate change actions or initiatives and even pull out from existing climate change agreements and institutions[19], other Quad member countries could still push for strengthening the sustainability aspects in semiconductor supply chains including in terms of water security and greater use of renewable energy.  Even if the US is absent from such efforts, other Quad countries could offer collaboration and partnership in building not only resilient but also sustainable semiconductor supply chains in the region and beyond.  Both the Quad and ASEAN countries (minus the US) could be thinking more seriously about the environmental damages caused by the industry, as well as better water conservation and the use of renewable energy to support this water- and energy-intensive semiconductor industry.

By offering ASEAN countries the opportunity to kill two birds with one stone, such as adding the sustainability dimension to a resilient semiconductor supply chain, it could dilute the conversation around security issues that are usually sensitive to ASEAN countries that want to stay neutral in the US-China geopolitical rivalry. It could also bring a cleaner and greener environment while contributing to the global public good, which benefit not only companies but also people in the region and beyond.

In conclusion, greater cooperation between the Quad and ASEAN in advancing more resilient supply chains in semiconductor must start with greater trust.  This essay highlights the importance of using existing mechanisms especially the IPEF Supply Chain Pillar, helping ASEAN build its domestic production and export capacity, creating a fairer and more even level playing field, and catalysing the Southeast Asian region to build a more sustainable future.

## Notes

[1] Varas, Antonio, Raj Varadarajan, Jimmy Goodrich, Falan Yinug. 2021. Strengthening the Global Semiconductor Supply Chain in an Uncertain Era. Boston Consulting Group (BCG) and Semiconductor Industry Association (SIA) Publication. Link: https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf

[2] Dahlman, Abigail, and Mary E. Lovely. 2023. 'US-led Effort to Diversity Indo-Pacific Supply Chains Away from China Runs Counter to Trends'. Peterson Institute for International Economics (PIIE) Publication. Link: https://www.piie.com/blogs/realtime-economics/us-led-effort-diversify-indo-pacific-supply-chains-away-china-runs-counter; Pangestu, Mari Elka. 2023. 'Critical Minerals: Challenges for Diversification, Climate Change and Development'. Slide Presentation at Peterson Institute for International Economics Webinar, on 27 April 2023. Link: https://www.piie.com/sites/default/files/2023-04/2025-04-27pangestu-ppt.pdf

[3] Miller, Chris. 2022. Chip War. The Fight for the World's Most Critical Technology. Scribner Publication.

[4] Nguyen-Quoc, Thang. 2023. 'The Deglobalization Myth: How Asia's Supply Chains Are Changing'. Hinrich Foundation Publication. Link: https://www.hinrichfoundation.com/research/wp/trade-and-geopolitics/how-asia-supply-chains-are-changing/

[5] Bradford, Anu. 2023. Digital Empires: The Global Battle to Regulate Technology. Oxford University Press.

[6] Gaida, Jamie, Jennifer Wong-Leung, Stephan Robin and Danielle Cave. 2023. 'ASPI's Critical Technology Tracker. The Global Race for Future Power.' Australian Strategic Policy Institute. Policy Brief Report No. 69/2023. Link: https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-08/ASPIs%20Critical%20Technology%20Tracker.pdf?VersionId=nVmWySgLSX2FMaS1U.uQVgQvvd_W427G

[7] Economic Development Board Singapore (EDB). 2022a. 'Southeast Asia's Rising Semiconductor Fortunes'. Link:

https://www.edb.gov.sg/en/business-insights/insights/southeast-asia-s-rising-semiconductor-fortunes.html; Economic Development Board Singapore (EDB). 2022b. ‘Diverse Capabilities, Infrastructure Help Drive Chips Industry in Singapore’. Link: https://www.edb.gov.sg/en/business-insights/insights/diverse-capabilities-infrastructure-help-drive-chips-industry-in-singapore.html

8 EDB, 2022b

9 EDB, 2022a

10 Doarest, Aufa, and Maria M. Wihardja. 2024. ‘The Impacts of Supply Chain Reconfiguration on ASEAN Economies’. Perspective. ISEAS-Yusof Ishak Institute Publication. Link: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2024-35-the-impacts-of-supply-chain-reconfiguration-on-asean-economies-by-aufa-doarest-and-maria-monica-wihardja/

11 Doarest and Wihardja, 2024

12 Nguyen-Quoc, 2023

13 Wihardja, Maria M. and Siwage Dharma Negara. 2024. ‘Indonesia’s Perspectives on the Indo-Pacific Economic Framework’. Konrad Adenauer Stiftung Publication. Link: https://kas-japan.or.jp/en/pub/indonesias-perspective-on-the-indo-pacific-economic-framework-ipef/

14 Source: https://www.ipef.gov.sg/supply-chain-agreement/

15 Source: https://www.politico.eu/article/china-taiwan-applications-dodged-by-indo-pacific-trade-bloc-cptpp/

16 Siregar, Reza, and Maria M. Wihardja. 2024. ‘Demographic Transitions in Southeast Asia: Reframing How We Think and Act About Ageing’. Perspective. ISEAS-Yusof Ishak Institute Publication. Link: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2024-14-demographic-transitions-in-southeast-asia-reframing-how-we-think-and-act-about-ageing-by-maria-monica-wihardja-and-reza-siregar/
17 Tan, George, and Maria M. Wihardja (forthcoming).

18 Armstrong, Shiro and Peter Drysdale. 2024. ‘Making Australia a Partners in the Global ASEAN Vision’. East Asia Forum. Link: https://eastasiaforum.org/2024/12/15/making-australia-a-partner-in-the-global-asean-vision/

19 Martinus, Melinda. 2024. ‘Trump’s Return a Spanner in the Works’. East Asia Forum. Link: https://eastasiaforum.org/wp-content/uploads/2024/12/East-Asia-Forum-Quarterly_Volume-16-Number-4.pdf

# US Policy Toward Semiconductors and Artificial Intelligence

Brad Glosserman

## Key Findings:

- The United States has rightfully determined that leadership in the semiconductor industry and in the development of Artificial Intelligence (AI) is vital to its national security and that securing both demands a whole-of-society approach.
- Ensuring that semiconductor supply chains are resilient requires a multilateral effort; the width and breadth of that coalition is not yet determined but it must be expansive.
- Cooperation on the development of AI remains nascent – reflecting the maturity of the technology – but like-minded partners should already be working to ensure that it is safe and secure and its benefits enjoyed by all nations.
- Effective policy in both fields must promote innovation and ensure that the resulting intellectual property is protected. Governments must adopt both offensive and defensive strategies

## Recommendations:

- Survey the range of multilateral initiatives across each sector to identify opportunities for rationalization and coordination.
- Establish a high-level regional economic security dialogue to assess opportunities and obstacles along with areas of consensus and divergence among key partners.
- The US should be especially alert to opportunities for cooperation with countries in Southeast Asia, which are eager to more deeply integrate into semiconductor supply chains.

The United States has long understood the centrality of semiconductors to its national security. Some 40 years ago, then-President Ronald Reagan argued that chips were central to efforts to counter the Soviet Union's numerical superiority in all things military. Artificial intelligence (AI) – the "great enabler" of virtually all new technologies that has been likened to electricity in its importance— has assumed a similar place in US national security thinking. In both areas, the US has concluded that it must be a leader in global development and production.

This paper examines U.S. policy toward semiconductors and AI, traces its history and current contours, and explores future options, focusing on regional and international cooperation and collaboration in the Indo-Pacific. It concludes with recommendations for ways to promote cooperation in the region.

## Semiconductors: from leader to lost

The integrated circuit, the precursor of today's semiconductor, was invented in the United States in 1959. Since then, the US "has been the long-standing global leader in semiconductors, with a 45 percent to 50 percent share of worldwide revenues in the last 30 years."[1] While the US retains a commanding position in the entire industry, its share of manufacturing has fallen—from 37 percent in 1990 to 12 percent in 2021—to a point where administrations worry about the ability to secure chips in times of crisis. Upon taking office, the Biden administration launched a 100-day review of the resilience and vulnerabilities of supply chains critical to US national security, semiconductors among them. It concluded that US companies "depend on foreign sources for semiconductors, especially in Asia, creating a supply chain risk."[2]

That review, the product of a whole-of-government assessment, yielded an equally sweeping response. A combination of executive orders and legislation has sought to transform the semiconductor sector in the United States. The most significant is the passage by Congress in July 2022 of the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act, which aims to strengthen domestic semiconductor manufacturing, design and research, fortify the economy and national security, and reinforce US chip supply chains. Significantly, it earmarked US$52.7 billion to stimulate reshoring of semiconductor manufacturing and innovation in this field. Biden signed the bill into law in August.

Most of those funds—US$39 billion—are for the construction of semiconductor fabrication facilities, with US$2 billion set aside specifically for legacy semiconductors that are critical to the military and other key industrial sectors such as automobiles and manufacturing. The rest is to stimulate innovation, including research and development and workforce development. The legislation contains an innovative provision that prohibits recipients of CHIPS funds from expanding semiconductor manufacturing in China and countries defined by US law as posing a national security threat to the country.

The Biden administration trumpeted the fruits of that legislation, reporting that the bill has prompted businesses to commit to more than US$395 billion in investments in semiconductors and electronics. As a result, the US is on track to produce almost 30 percent of the world's supply of leading-edge chips by 2032, up from zero when Biden took office. The US now has facilities for all five of the world's leading-edge logic, memory, and advanced packaging providers.[3]

Under the Trump administration, semiconductors remain a priority, even if the means of promoting that sector have shifted. The president has been called "a fierce critic" of the CHIPS act, "wary of using public money to promote domestic manufacturing." His administration has been "actively renegotiating CHIPS grants, pushing manufacturers to put more skin in the game."[4]

Efforts to stimulate domestic production and innovation are one side of US policy. The other half, equally important, focuses on restricting the flow of semiconductors and related technologies to potential adversaries. These strategic trade controls, often referred to as export controls, have a long history. They were most famous during the Cold War, when the US and its allies devised multilateral programs to restrict Soviet access to the West's most advanced technologies with potential military uses.

Since the end of that conflict, trade controls primarily restricted access to goods that could be used for weapons of mass destruction (although some applied to missiles and related technologies) and the coalition of concerned nations expanded to include former Cold War adversaries. Today, however, geopolitical competition has shifted the contours of strategic trade controls to include new and emerging technologies and that new coalition is breaking down.

Concerned about China's use of technology for security purposes, the US—and in some cases, its allies—has again attempted to restrict access to those goods. In 2018, the Trump administration convinced the government of the Netherlands to deny a license to the Dutch company ASML, the sole producer of some of the most critical semiconductor manufacturing equipment, to sell its most advanced products to Chinese companies. The following year, the Trump administration put Huawei and ETZ, prominent Chinese telecommunications companies, on the Commerce Department's Entity List, which bans companies from buying controlled US exports – in this case advanced semiconductors -- without a license. (ETZ was later removed.) Other Chinese companies were subsequently added to the list. Restrictions on Huawei were expanded to include the Foreign Direct Product Rule, which requires companies that use controlled US technology in their production processes to comply with US restrictions; in other words, any company anywhere that uses US technology to makes chips must apply for a license to sell to Huawei.

In October 2022, the US enacted new export controls on advanced semiconductor technology that restricted US companies from exporting advanced semiconductors to China, as well as the equipment needed to make chips smaller than 14 nanometers. The measures were considered "the single most substantial move by the U.S. government to date in its quest to undermine Chinese technology capabilities."[5] Cognizant that unilateral actions are fruitless when other nations can provide the same products, the Biden administration worked with two other nations critical to semiconductor manufacturing, Japan and the Netherlands, to get them to sign on to the US restrictions. They agreed the following year. The US continues to tweak and update those rules to close resulting loopholes.

Another unprecedented move is the executive order directed on August 9, 2023 that limits certain US investments in key Chinese technology sectors, such as semiconductors and microelectronics, quantum information technologies, and artificial intelligence, to prevent the financing of Chinese military advancement.

In the second Trump administration, the push to constrain Chinese access to advanced chip technology continues. Industry observers argue that the emphasis has shifted to greater reliance on "the stick" of sanctions over the Biden team's preference for "the carrot" of investment subsidies.[6]

## AI commands new attention – and gets it

The US has been equally concerned about leading the development of artificial intelligence (AI), but since the technology is relatively new, the history of policy engagement is much shorter. President Trump issued two executive orders on AI: the first established the American AI Initiative (E.O. 13859) and the second promoted the use of trustworthy AI in the federal government (E.O. 13960). The American AI initiative articulated US interest in AI, noting that "Continued American leadership in AI is of paramount importance to maintaining the economic and national security of the United States and to shaping the global evolution of AI in a manner consistent with our Nation's values, policies, and priorities."[7]

Congress took action with passage of the National Artificial Intelligence Initiative Act of 2020, which established an American AI Initiative and provided guidance on AI research, development and evaluation activities at federal science agencies. Since then, Congress has considered dozens of bills with an AI component, but has enacted only a handful.[8]

In the absence of Congressional action, the White House has issued executive orders or policy directives from its agencies, following the course charted by the Trump administration.[9] President Biden issued executive order on the "Safe, Secure, and Trustworthy Development and Use of AI," which was released in October 2023 and was the US AI strategy.[10] It incorporated many previous orders and directives to ensure that the US maintains its leadership in this critical field, but also developed and deployed AI to promote shared prosperity, without promoting discrimination and ensured that the resulting technology is safe, secure, and trustworthy.

The Trump administration released its AI Action Plan six months after taking office.[11] The plan followed up on Executive Order 14179, "Removing Barriers to American Leadership in Artificial Intelligence," which was issued days after Trump took office for his second term. It called "for America to retain dominance in this global race and directing the creation of an AI Action Plan." It seeks to "establish American AI—from our advanced semiconductors to our models to our applications—as the gold standard for AI worldwide and ensure our allies are building on American technology." To do that, the plan rests on three pillars: innovation, infrastructure, and international diplomacy and security. The Trump team took considerable pride in announcing that it "rescinded the Biden Administration's dangerous actions on day one."

Unlike the semiconductor industry, there are ample private funds available for AI research, and the US government has not had to step in to fill that need. For the most part, the government's role has been restricted to guidance for the development and use of this technology.

The Biden administration tried to control the spread of AI technology, however. In this endeavor, there is considerable overlap with its semiconductor trade controls since many of the same countries are considered potential adversaries and hardware is often the key to the development of AI. Many of the chips that are denied to China are used for AI purposes: The Department of Commerce's Bureau of Industry and Security (BIS), which is responsible for enforcing US strategic trade controls, issued rules in October 2022, October '23, and April 2024 that sought to limit China's access to the most advanced chips used for AI computing.[12] In October 2024, the Biden administration announced that it was finalizing rules to limit US investments in AI and other emerging technology sectors in China that could threaten U.S. national security.[13] Those rules stem from Biden's August 2023 executive order that banned certain investments in China.[14]

While the Trump administration remains committed to US leadership in this field, its policies have meandered. After banning the sale of top-line AI chips to China in April, it reversed course and allowed the sale of the H20 chip, created by Nvidia, one of the world's leading AI semiconductor companies, to maintain access to the Chinese market after the Biden administration halted the export of chips with high processing power. [15] A similar approval was given to chipmaker AMD. In a comment, Matt Pottinger, deputy national security advisor in Trump's first term, said that by allowing the exports "Trump just handed China the tools to beat America in AI." [16]

## Are they working?

The US has sought to best China in the race to master new and emerging technologies, spurring innovation and denying its chief competitor easy access to its fruits. If success is measured by research, development, and manufacturing of those critical technologies on US soil, then the policies should be considered a qualified success. Investment is up, companies are building facilities in the United States, and output is increasing. Competition will intensify, however, and various technology trackers indicate that Chinese capabilities are formidable.

Concern has focused on the effectiveness of technology controls. First, there is worry that the restrictions have not been effective. China has been stockpiling chips in anticipation of the US controls. In addition, Chinese end users set up shell companies and intermediaries to continue purchasing items that they otherwise could not.[17]

US policies have confirmed the view in China that the West seeks to slow or stop its technological progress and reinforces autarkic tendencies. That said, this view is difficult to take seriously given the longstanding determination of China's leadership to nurture world-beating domestic champions in most key tech sectors and the resulting billions of yuan that Chinese authorities have provided to the semiconductor industry – in May 2024 China announced the launch of a US$47.5 billion investment fund to boost semiconductor capacity, the third round of state-led investment in the industry over the last decade.[18]

Second, China has introduced countermeasures to push back. They typically include restrictions on the export of raw materials, such as germanium and gallium, which are needed to manufacture semiconductors. China has also closed its market to US companies, denying them a substantial potential source of revenue. One authoritative analysis concluded that because of US trade controls, "affected suppliers have negative abnormal stock returns, wiping out US$130 billion in market capitalization, and experience a drop in bank lending, profitability, and employment. [US firms'] total number of customers declines, potentially inflicting collateral damage upon the same US firms whose technology export controls are trying to protect."[19]

Finally, China has courted alternative suppliers, using the allure of its huge market and the prospect of better relations with the Chinese government, to encourage other companies to step up when the United States has stepped back. This strategy has had mixed results as Washington has become increasingly alert to the need for international cooperation and coordination if it is to succeed in reducing its own supply chain vulnerabilities and to ensure that other competitors do not backfill gaps created by US policy.

## All for one…

The US is increasingly focused on the cooperative dimensions of its high-technology policy. Virtually all bilateral and multilateral relationships have a tech element to them, a means to promote supply chain resilience and innovation. The US and Japan have launched an "economic 2+2 meeting" to ensure that the two governments properly address economic security concerns. Washington and Seoul in 2023 launched the US-ROK Next Generation Critical and Emerging Technologies (CET) Dialogue that "will drive cooperation across six main strategic technology areas," semiconductors and AI among them.[20] The US, Japan, and South Korea agreed to establish a trusted AI ecosystem across the three countries, and are strengthening commercial collaboration around AI chips as well as strengthening engagement on AI safety.[21] The commerce ministers from the three countries agreed this summer to promote the development of critical and emerging technologies and strengthen the security and resiliency of our economies. They will prioritize cooperation to reinforce the resilience of supply chains in key sectors such as semiconductors and deepen coordination on innovation of advanced technologies, export controls on those technologies, and efforts to develop international standards and ensure safe, secure, and trustworthy use of AI.[22]

Cooperation on critical and emerging technologies is a key element of the agenda of the Quadrilateral Security Dialogue of the US, Australia, India, and Japan. Those governments have made semiconductor supply chain resilience a priority and have moved forward on AI cooperation in specific areas, such as agriculture. More can be done. The Biden executive order on AI calls for the expansion of bilateral and multilateral AI engagements, accelerated development and implementation of AI standards, and promotion of the safe, responsible, and rights-affirming development and deployment of AI abroad to address global challenges.

Additional forums include the Chip 4 Alliance, an "aspirational tech partnership" between the US, Japan, South Korea, and Taiwan—which collectively account for 82% of global semiconductor output—that aims to diversify semiconductor supply chains.[23] That initiative is still taking shape, having first met in February 2023. The Indo-Pacific Economic Framework for Prosperity," a 14-member group that is addressing four separate 'buckets'— trade, supply chains, decarbonization and infrastructure, and fair economy issues such as anti-corruption and transparency—identified semiconductors, critical minerals, batteries, and chemicals as critical sectors under its supply chain resilience agreement concluded earlier in 2024. While semiconductor production capacity varies wildly across the group's members, there is great potential for the group to meet its goal of diversifying and strengthening chip supply chains.

## Where do we go from here?

Realizing the potential of IPEF, and other multilateral groups, remains the core task of the United States as it seeks to maintain its leadership in these emerging technology sectors. No state can go it alone in the semiconductor industry or in artificial intelligence. The US government and the industries themselves have recognized this basic truth and have embedded it in their strategies. As the US contemplates future action in these areas, three recommendations come to mind.

First, the US and its partners should survey the range of multilateral initiatives across each sector to identify opportunities for rationalization and coordination. As noted, there are technology collaborations in virtually every venue and engagement. This proliferation must be rationalized to avoid duplication, repetition and the eventual overloading of bureaucracies.

Second, the US should support the establishment of a high-level regional economic security dialogue to assess opportunities and obstacles along with areas of consensus and divergence among key partners. While there are many bilateral and minilateral discussions of these issues (along with other topics that are part of the economic security conversation), no venue offers the opportunity for an assessment of regional (and global) views of these topics. That gap must be filled.

Third, the US should be especially alert to opportunities for cooperation with countries in Southeast Asia. These nations are the focus of geopolitical competition between the West and China, yet they wish to remain above the fray. They are also eager to more deeply integrate into semiconductor supply chains, for economic opportunities and to promote the development of high-tech industries within their national economies. Focusing on these countries can provide extensive dividends, beyond the purely economic returns.

# Notes

[1] Antonio Varas et al., Government Incentives and U.S. Competitiveness in Semiconductor Manufacturing, Semiconductor Industry Association and Boston Consulting Group, September 2020, at https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-inSemiconductor-Manufacturing-Sep-2020.pdf.

[2] The White House, "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Demand-Based Growth: 100 Day Reviews Under Executive Order 14017," June 2021, p. 22.

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2024/08/09/fact-sheet-two-years-after-the-chips-and-science-act-biden-%E2%81%A0harris-administration-celebrates-historic-achievements-in-bringing-semiconductor-supply-chains-home-creating-jobs-supporting-inn/

[4] Aaron Mak, "the 'Chip War' under Trump," Politico, June 10, 2025 https://www.politico.com/newsletters/digital-future-daily/2025/06/10/the-chip-war-under-trump-00397048

[5] https://carnegieendowment.org/posts/2022/10/bidens-unprecedented-semiconductor-bet?lang=en

[6] Mak, op cit.

[7] https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

[8] https://crsreports.congress.gov/product/pdf/R/R47644

[9] Lists are available at the https://ai.gov/actions/ and the OECD https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-27577 and

[10] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[11] https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

[12] https://www.brookings.edu/articles/the-tension-between-ai-export-control-and-u-s-ai-innovation/

[13] https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/28/fact-sheet-addressing-u-s-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern/?utm_source=substack&utm_medium=email

[14] https://www.reuters.com/world/white-house-detail-plans-restricting-some-us-investments-china-source-2023-08-09/

[15] John Liu, "Trump relaxed restrictions on a key AI chip for China. Beijing isn't saying thank you," CNN Business, Aug. 18, 2025, at https://edition.cnn.com/2025/08/17/tech/nvidia-china-beijing-trump-ai-intl-hnk

[16] https://www.fdd.org/analysis/2025/08/11/trump-just-handed-china-the-tools-to-beat-america-in-ai/

[17] Ryan Fedasiuk, Carson Elmgren and Ellen Lu, "Silicon Twist: Managing the Chinese Military's Access to AI Chips, Georgetown Center for Security and Emerging Technology, June 2022.

[18] https://www.csis.org/analysis/collateral-damage-domestic-impact-us-semiconductor-export-controls

[19] Matteo Crosignani, Lina Han, Marco Macchiavelli, and André F. Silva, "The Anatomy of Export Controls," Liberty Street Economics, April 12, 2024, at https://libertystreeteconomics.newyorkfed.org/2024/04/the-anatomy-of-export-controls/

[20] https://kr.usembassy.gov/120923-joint-fact-sheet-launching-the-u-s-rok-next-generation-critical-and-emerging-technologies-dialogue/

[21] https://www.whitehouse.gov/briefing-room/statements-releases/2024/11/15/joint-statement-of-japan-the-republic-of-korea-and-the-united-states/#:~:text=In%20addition%2C%20Japan%2C%20the%20ROK,strengthening%20engagement%20on%20AI%20safety.

[22] https://www.commerce.gov/news/press-releases/2024/06/joint-statement-japan-republic-korea-united-states-commerce-and

[23] https://www.csis.org/analysis/securing-semiconductor-supply-chains-indo-pacific-economic-framework-prosperity

# Artificial Intelligence and Semiconductors: Australia and the Indo-Pacific

Ben Scott

## Key points:

- Australia's approach to economic and cyber security is evolving rapidly, and the government's power – and willingness -- to intervene is expanding.
- Australia is yet to focus on developing national artificial intelligence (AI) or semiconductor fabrication capabilities, aside from new support for critical minerals that are used in semiconductors.
- But Australia's interest in the international governance and security of these technologies is growing, evidenced most clearly by government-proposed "mandatory guidelines" for AI.

## Policy recommendations

- Australia should seek to extend successful domestic policy innovations on the governance and security of AI regionally and internationally.
- Domestic lessons about building trust as an enabler of cyber threat information sharing should be applied regionally.
- In due course, the government should look to extend "secure by design" principles and government-backed cloud computing to the region

## Australia's growing interests in AI and semiconductors

The growing importance of artificial intelligence (AI) has prompted Australia's focus on the safe deployment of these technologies and the security of the global supply chain for advanced semiconductors on which the country relies. Australia's limited sovereign capabilities also heighten this interest, as the Pacific country does not possess a domestic semiconductor manufacturing industry, sitting within the 10th and 20th spots in global rankings of national AI capabilities, which corresponds with the size of Australia's economy.[1] Therefore, Australia prioritizes the global governance and security of critical technologies, with a strong focus on fostering arrangements in the Indo-Pacific, particularly with closely connected Southeast Asian and Pacific Island nations, or those it aims to engage with.

## Evolving critical and emerging technology policy

The Australian government's interest in the security and regulation of critical and emerging technologies—including AI and semiconductors—is relatively recent, with a continuously evolving policy. In 2018, Canberra faced a catalytic year in deciding whether to permit Chinese telecommunications network Huawei to participate in the rollout of Australia's 5G network due to what it perceived as potential national security risks. The decision to exclude "high risk vendors" such as Huawei was, according to journalist Paul Kelly, the "single most important security-related decision in years".[2] The decision was far from straightforward, however. At the time, it was widely assumed that Australia's economic future would depend heavily on its 5G infrastructure, and that Huawei offered the best deal. If other Western countries, including the United States, had not followed Australia's lead, Huawei might still have emerged as the unrivaled leader in the 5G market, leaving Australia isolated from this technological ecosystem and economically weakened.[3]

The Huawei decision prompted the government to seek a framework for managing the security risks of critical and emerging technologies. Canberra adopted the "critical infrastructure" framework and enshrined it in the foundational Security of Critical Infrastructure Act of 2018. The supply chain disruptions that followed the outbreak of COVID-19 and undeclared Chinese economic sanctions against Australia reframed the issues in economic security terms.

## 1. Economic security

In 2024, the government badged its economic security policy as the "Future Made in Australia". The most authoritative articulation is contained in a May 2024 speech delivered by Treasurer Jim Chalmers to the Lowy Institute, which laid down guidelines for future industry policy.  This includes a proposed Future Made in Australia Act that would provide a "National Interest Framework" to guide decision-making about "public investment that facilitates private sector investment in the national interest."

Australia has not yet made a major public investment in AI or semiconductors, despite the urging of some commentators that it do just that. For example, writing in the ASPI Strategist, Bronte Munro, Alex Capri, and Robert Clark argue that "opting out of semiconductor manufacturing for the long term would severely constrain Australia's growth as a technological nation and consign it to second-tier status."[4] Separately, a coalition of Australian AI experts has long advocated government investment in "sovereign AI".[5]

Professor Anton van den Hengel argues that "Australians should be able to use a large language model (LLM) without sending data and IP to foreign countries or companies". He sees an Australian LLM as "the first step in building Australia's sovereign AI capability" which is necessary to forestall a future where AI is applied by foreign companies such as Uber to extract huge profits from the Australian market.[6]

The government's apparent reluctance to follow this advice may reflect the reality that, in Chalmers words, "the scale of subsidies in the 3 major global economies … dwarfs anything Australia can offer".

## Securing critical minerals for semiconductors

Foreign investment controls are another tool for strengthening economic security. Through a package of reforms which took effect in July 2024, the Australian government has increased the scrutiny of foreign investment while simultaneously reassuring foreign investors that such controls will be imposed only sparingly, and where necessitated by a risk-based assessment of the investor, the investment, and the transaction.[7]

Critical minerals, including those that are essential for the production of semiconductors, have been a particular focus of foreign investment controls and subsidies. Under the Biden administration, Australia was designated as a 'domestic source' of minerals under the Defense Production Act, enabling Australian companies to access US Inflation Reduction Act subsidies, provided the Australian companies have no more than 25% ownership, voting rights or board seats held by 'foreign entities of concern'.[8]

Chalmers has excluded investors linked to China from critical minerals projects in Australia. In 2023, the treasurer blocked one China-linked investor, the Yuxiao Fund, from nearly doubling its investment in Northern Minerals Limited (NML). NML aimed to become the first substantial producer of dysprosium, a rare-earth mineral used in electric vehicles outside China. In June 2024, the treasurer further ordered five international companies linked to China to sell their shares—totaling 10.4 per cent—in NML.

The government's Critical Minerals Strategy 2023–2030 lays out Australia's plan to "build sovereign capability in critical minerals processing" and to implicitly offset dependencies on China. This followed China's tightening of export controls on gallium and germanium from July to October 2023.[9] In October of that year, the government announced 2 billion Australian dollars in additional support for the critical minerals sector. [10] Part of the fund was allocated towards the Australian Critical Minerals Research and Development Hub that had been established in  October 2022. In 2024, Australian government scientists announced plans to explore extracting gallium and germanium as by-products from existing mining operations, especially the refining of alumina and zinc, receiving support from the hub.[11]

Export controls are not yet a key tool of Australian economic security, with Canberra using export controls to regulate the export of military and dual-use goods and technology.

## 2. Cybersecurity standards and risk management

Adversarial AI is sharpening threats to cybersecurity, both by refining offensive tools—such as code writing, vulnerability detection, and spear phishing—and creating new attack surfaces. AI is vulnerable to the manipulation of inputs through methods such as "data poisoning," which corrupts the training data for AI or machine learning models, or "prompt injection," hijacking AI systems by crafting malicious inputs to cause unintended behavior in large language models.

The range of actors threatening Australian cybersecurity is wide. Canberra has become progressively more willing to identify China as the main source of state-based cyber-enabled threats to Australia and the Indo-Pacific. That includes cyber-enabled economic espionage and intellectual property theft, as well as potential sabotage. But at the same time, Australia has been compelled to pay more attention to non-state cyber actors, chiefly criminals, by unsophisticated large-scale data extractions perpetrated in 2022 against Optus, a major telecommunications network, and Medibank, Australia's largest private health insurance company.

The PRC's use of cyber means to steal intellectual property and big data has become increasingly relevant to AI security and geopolitical competition. Although this theft is old news – it was described over a decade ago as the "greatest transfer of wealth in history" by the Director of the US National Security Agency – it has taken on a new dimension with the acceleration of development of big-data-dependent AI. In October 2023, FBI Director Wray said China had "a bigger hacking program than that of every other major nation combined". Mike Burgess, director-general of the Australian Security Intelligence Organization, pointed out that "all nations spy" but Chinese intellectual property theft "goes well beyond traditional espionage."

### Preventative intervention

Australia describes its response to these threats as "preventative intervention". To strengthen cybersecurity, the government has asserted more authority over privately owned critical infrastructure while also compelling private owners to take more responsibility for cybersecurity. This trend began with the passage of the Security of Critical Infrastructure Act of 2018, and is being advanced through the recently introduced Cybersecurity Bill. Tighter regulation of AI will almost certainly follow, including through further legislation.

Canberra has decided that "high-risk" AI is inadequately regulated and proposes to impose "mandatory guardrails". The government is consulting on how best to do so. The three main options are: (1) a "domain-specific" adaptation of existing regulatory frameworks; (2) the creation of new "framework legislation," modifying a range of other Acts; (3) a new "whole-of-economy" Australian AI Act.[12] The government has specified that reform will be guided by the goal of aligning with international standards and enhancing interoperability with international partners. For example, one argument for an AI Act is to improve interoperability with EU partners and, potentially, Canada.

## Secure by design

Australian concerns about the potential for supply chain disruptions and even sabotage have been growing since the Huawei decision in 2018. Australia has yet to develop a national framework for assessing the national security risks presented by vendor products and services; however, creating one has been identified as a priority in the Australian Cyber Security Strategy 2023-2030 (ACSC). The objective is to help industry manage supply chain risks and make informed procurement decisions about the security of products and services.

As part of the new Cybersecurity Bill, Canberra also proposes to require minimum cybersecurity standards for smart devices. These "secure by design" principles for Internet of Things (IoT) devices would be comparable to the US Cyber Trust Mark Program. These standards would likely complement the government's effort to impose such mandatory guardrails on "high-risk AI" by compelling producers to address and mitigate AI-related risks.

Importantly, more secure IoT devices would also impede adversaries' efforts to build a hostile covert cyber infrastructure on networked devices in Australia and the region. Insofar as "secure by design" principles can be internationalized, they would also help counter this region-wide threat. Since August 2023, Microsoft has observed Chinese threat actor Storm-0940 stealing credentials from multiple Microsoft customers via password spray attacks launched from a network of compromised devices (CovertNetwork-1658).[13] Earlier, Microsoft identified Advanced Persistent Threat (APT) 40 as "the most active threat actor in the Pacific region". It typically targets the old and unpatched devices that have joined larger networks as work-from-home arrangements became commonplace after COVID-19. In July 2024, an Australian-led coalition publicly attributed APT-40 to the Hainan State Security Department.

### Trust and information sharing

Although the Australian government is intervening more directly in cybersecurity compared to countries such as the United States, the success of these efforts still depends greatly on information sharing, especially between the public and private sectors.

The Australian Cyber Security Center (ACSC), as part of the Australian Signals Directorate (ASD), disseminates information on cyber threats publicly and shares more sensitive information with trusted partners through its Cyber Threat Intelligence Sharing (CTIS) platform. A CTIS plugin for Microsoft Sentinel allows companies to share their information with ASD. The Security of Critical Infrastructure Act allows the government to compel some companies to install software that transmits directly to ASD. If enacted, the Cybersecurity Act would give the government more power to intervene.

But two-way information sharing still requires improved trust. An initial surge in cyber threat information sharing in Australia tapered and then declined as corporations became more concerned that shared information could be used to regulate or penalize them. To provide more reassurance, the new Cybersecurity Bill proposed limiting the government's use of shared information. Similarly, a new obligation to report ransomware incidents and payments would be made to carry no-fault and no-liability clauses.

The importance of building trust in order to facilitate the two-way exchange of cyber threat information extends beyond the domestic realm. This lesson should be applied more broadly to international information-sharing and cybersecurity efforts.

## 3. International Capacity-building

Although the Five Eyes grouping (composed of Australia, Canada, New Zealand, the United Kingdom, and the United States) still sits at the core of Australia's approach to international cybersecurity, Canberra has increased cooperation with expanded groupings. Australian cybersecurity increasingly depends on cybersecurity and supply chains that extend well beyond the Five Eyes, making it necessary to work with larger coalitions to counter the expanding array of threats.

One example is the aforementioned July 2024 ASD/ACSC-led advisory about Advanced Persistent Threat (APT). The attribution was made by a coalition including the Five Eyes, as well as Japan and South Korea. It described the state-sponsored attack with a high level of specificity. The 68-nation counter-ransomware initiative (for which Australia developed the threat-sharing platform) is also another example.

## Australian international cyber security strategy

Australia's particular interest in the resilience of Southeast Asian and Pacific Island networks. was evident in the government's unusual 2022 decision to grant US$1.33 billion to Australia's largest telecommunications network, Telstra, so that it could outbid a Chinese competitor seeking to purchase Papua New Guinea mobile provider Digicel, with Telstra contributing US$270 million. But such "whack-a-mole" solutions are unsustainable.

A more strategic approach to regional cybersecurity is therefore necessary. Australian cybersecurity capacity-building in the region primarily focuses on the cyber hygiene practices that are foundational to cyber defense, regardless of the sophistication of the threat.[15] Basic cyber hygiene is equally essential to mitigating the more advanced threat posed by and to AI, as detailed in the January 2024 joint advisory on using AI securely from Australia and 10 other countries such as US, UK, Canada, New Zealand, Germany, Israel, Japan, Norway, Singapore, and Sweden. The ASD's Essential Eight measures provide another useful list of foundational cybersecurity actions.[16]

Australia's ambitions for a more cyber-resilient region are set out in the Australian Cyber Security Strategy (ACSS). Globally, Australia still aims to will aims to "shape, uphold and defend international cyber rules, norms and standards," but its regional objectives have become more specific. These include piloting "options to use technology to protect the region at scale ... this includes proactively identifying vulnerabilities – such as end-of-life hardware and software" as well as "scalable solutions that are fit-for-purpose, including security features that mitigate avoidable cyber incidents." This suggests that AI and cloud computing may play a larger role in Australian support for regional cyber capacity-building and resilience.

## A bigger cloud?

The absence of an Australian semiconductor fabrication capability underscores Australia's interest in cloud computing and security. Accordingly, Australian government investments in cloud computing have accelerated. In October 2023, Microsoft announced that it would invest A$5 billion in Australian data centres "to expand its hyperscale cloud computing and AI infrastructure". In July 2024, the government announced a A$2 billion investment and partnership agreement with Amazon Web Services (AWS) in Australia to deliver a "Top Secret Cloud". This is "purpose-built for Australia's Defence and National Intelligence Community agencies to securely host our country's most sensitive information…and harness leading technologies including artificial intelligence and machine learning."

There is clear potential for Australia to use and even expand on these investments to advance its regional cybersecurity goals. A well-secured cloud would provide the basis for the "scalable solution" referred to in ACSS, especially if AI-enhanced capabilities "proactively identify vulnerabilities" were integrated.

But it would not be easy to persuade countries in Australia's region to entrust more of their cybersecurity and data to Australian government agencies and US tech giants. The necessary international trust would have to be built over time. The enhanced information sharing referred above could be a step in this direction.

### Offensive Cyber doctrine

Although the most important cybersecurity measures that most individuals, corporations, and governments need to undertake are straightforward and defensive, so-called "offensive cyber" will play a greater role in international cybersecurity with the growth of adversarial AI. The blunting of Russia's February 2022 cyber offensive against Ukraine appears to have demonstrated the success of US Cyber Command's relatively new strategy of "forward defence" (or "persistent engagement").

Australia is investing an A$10 billion over 10 years in strengthening ASD's offensive cyber capabilities and, for example, leads on "disruption" in the 68-nation "counter ransomware initiative." Still, Canberra has said relatively little about how and when offensive cyber operations would be undertaken. This contrasts sharply with the United States and United Kingdom, where government agencies have encouraged and engaged in an active public debate about the issues in an attempt to sharpen doctrine and build social license. Australia should match its offensive cyber capability with a similar effort to publicly articulate doctrine.[17]

## 4. Conclusion

Australia's response to the emerging challenges posed by AI and the semiconductor supply chain on which it depends is still evolving. The daunting nature of the domestic challenges might be expected to reduce policymakers' bandwidth for considering the international dimensions. But Australia cannot meet these challenges on its own and has interests in the governance and security of these technologies that go well beyond its borders, and well beyond the Five Eyes. For those reasons, once domestic policy innovations—on issues such as information sharing, secure-by-design, and government-backed cloud computing—have proven their worth, Australia should seek to regionalize and internationalize them.

## Notes

1 Australia's AI "capability" is ranked some somewhere between 10th (Tufts TRAIN) and 20th (Global AI index).

2 Paul Kelly, Morrison's Mission: How a Beginner Reshaped Australian Foreign Policy (Australia: Penguin Books, 2022), 43,Chalmers'.

3 https://www.lowyinstitute.org/publications/sharper-choices-how-australia-can-make-better-national-security-decisions

4 ASPI

5 https://kingstonaigroup.org.au/members

6 https://medium.com/@aiml_58187/australias-sovereign-ai-capability-begins-with-an-australian-llm-225fa151e86f

7. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://foreigninvestment.gov.au/sites/foreigninvestment.gov.au/files/2024-04/australias-foreign-investment-policy.pdf

8 https://www.aspi.org.au/opinion/road-critical-mineral-security-leads-through-australia#:~:text=America%27s%20critical%20minerals%20supply%20chains%20cannot%20depend%20on%20a%20single,resilience%20in%20this%20vital%20domain.

9 https://www.industry.gov.au/publications/critical-minerals-strategy-2023-2030, https://asia.nikkei.com/Business/Tech/Semiconductors/China-s-chip-material-export-curbs-4-things-to-know

10 https://www.pm.gov.au/media/2-billion-critical-minerals-boost-crucial-energy-transition

11 https://asia.nikkei.com/Business/Technology/Australia-looks-to-mining-waste-for-cutting-edge-chip-materials

12 Safe and responsible AI in Australia Proposals paper for introducing mandatory guardrails for AI in high-risk settings  September 2024

13 https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/

14 https://www.counter-ransomware.org/

15 https://nsc.crawford.anu.edu.au/department-news/15515/cyber-bootcamp-project

16 patch applications / patch operating systems / multi-factor authentication / restrict administrative privileges / application control / restrict Microsoft Office macros / user application hardening / regular backups.

17 https://www.aspistrategist.org.au/australia-needs-to-talk-more-openly-about-offensive-cyber-operations/

Developing shared security standards for AI and semiconductor infrastructures.
Amy Chang
Daisuke Kawai
Mark Manan

# Forging a Resilient Tech Ecosystem: Japan's Path to Economic Security and Regional Collaboration

Daisuke Kawai

## Key Findings

- Fundamental to Japan's economic security outlook is maintaining an advantage in dual-use critical and emerging technologies (CETs) and actively limiting adversaries' access. Nonetheless, Tokyo recognizes that restricting technology exchanges alone cannot guarantee genuine strategic autonomy.

- For Japan, certain policy trade-offs necessitate collective strategies across aligned nations, reflecting the fundamental recognition that no single state can address these multifaceted threats in isolation and collective action has a distinct and crucial multiplier effect.

- As a critical node in the worldwide semiconductor chain, successful cyber-attacks on Japan's infrastructure may prompt cascading consequences across varied essential industries. In AI, the government is developing guidelines that incorporate "Security by Design" by embedding security measures into systems from their outset rather than retroactively.

## Policy Recommendations

- Japan's economic security aspirations—achieving both strategic autonomy and strategic indispensability—ultimately depend on constructing concrete, cooperative mechanisms that tackle shared vulnerabilities and nurture mutually beneficial interdependencies. This includes aligning cybersecurity standards among Quad and ASEAN members, promoting public-private R&D pipelines via the Quad Investors Network (QUIN), and devising new governance frameworks that strike a balance between security imperatives and the merits of open innovation.

- Tokyo's economic security outlook, therefore, should cement collective action backed by comprehensive knowledge-sharing agendas protected by multiple layers of safeguards.

- Japan must double its efforts toward standardizing cybersecurity protocols, expanding cross-border R&D investments, and shaping consistent governance practices that uphold prudent export controls, preserve IP protection, and facilitate open innovation.

## Background

Over the past decade, the Covid-19 pandemic, Russia's aggression against Ukraine, and escalating U.S.-China technological competition have fundamentally recast economic security as a core facet of state power. Consequently, a global industrial restructuring is underway to determine which country can most effectively produce cutting-edge technologies and attain strategic indispensability through technical preeminence. Such rivalries will, in turn, allow the victors to shape technology standards, influence markets, and mold the broader security landscape. In this context, the Indo-Pacific region has emerged as an epicenter of geopolitical rivalry, fueled by converging strategic tensions, rapid economic development, and intense technological innovation (Zhu 2015) (Raska 2019) (Ahmed 2021).

Sino-Japanese economic integration created beneficial interdependencies, yet Beijing's one-party state has, in many respects, has unequivocally chosen to forego genuine market liberalization in favor of its ambition to occupy the central position in the geoeconomic order (Zenglein and Gunter 2023). From Japan's vantage point, forced technology transfers and military-civil fusion (MCF) policies represent inherently serious threats, reinforcing the notion that Japan's economic survival is at stake. While the country excels at refining advanced technologies, its resource-poor status leaves it especially vulnerable to external pressure. Spurred by these existential concerns, in 2022 Japan introduced the Economic Security Promotion Act (ESPA) ahead of many counterparts aiding Japanese firms in their retreat from risky segments of the Chinese market. Data from the Bank of Japan shows that despite a recent uptick Japanese FDI into China has fallen by roughly 60% from its peak in 2017, a trend mirrored by the diminishing number of Japanese nationals living in the PRC. While the reverse also holds true for the boom in Japanese FDI and expats entering the United States. Although China's once-unassailable role as the "world's factory" is waning due to economic diversification as well as rising labor costs reducing competitiveness and a domestic downturn, it continues to dominate vital technology supply chain chokepoints, rendering complete disengagement impractical. Recent high-profile and controversial US-China trade negotiations are testament to these realities.

Maintaining an advantage in dual-use critical and emerging technologies (CETs) and actively limiting adversaries' access is fundamental to Japan's economic security outlook. Nonetheless, Tokyo recognizes that restricting technology exchanges alone cannot guarantee genuine strategic autonomy (Shiraishi 2024). The core challenge of economic security thus lies in balancing market-driven efficiency with the distinct political value of security (Shiraishi 2024). Japan's approach frames prosperity and security as complementary rather than mutually exclusive, highlighting "friendly" partners to pool resources and establish standards in advanced manufacturing (Edmonstone 2024). Certain policy trade-offs necessitate collective strategies across aligned nations, reflecting the fundamental recognition that no single state can address these multifaceted threats in isolation and collective action has a distinct and crucial multiplier effect.

This paper examines Japan's economic security policy with respect to high-tech manufacturing and the promotion of innovation, before exploring challenges arising from the absence of unified cybersecurity standards in the advanced semiconductor industry. Finally, it presents several policy options that could strengthen Tokyo's capacity to safeguard both its national interests and the broader Indo-Pacific region's stability.

## High Tech Manufacturing

Sino-Japanese relations have produced significant interdependencies that, if abruptly unraveled, could inflict serious damage. In particular, the People's Republic of China (PRC) retains a dominant position across roughly 220 strategic sectors, compared with Japan's leadership in only 15 (Chimits, et al. 2024). Additionally, China controls an estimated 90% of the global refining capacity for rare earth minerals (CSIS 2024). Although Beijing benefits from foreign capital and technology, it has all but rejected liberalization. Meanwhile, transparent competition tends to drive innovation, whereas massive subsidies often hamper the creativity so crucial to technological breakthroughs (Goodman 2024). China's tech landscape, as exemplified by Huawei's fight for survival amid U.S. embargoes, illustrates these complexities. Although U.S. export controls restrict Chinese firms' access to certain high-performance chips, multiple workarounds via third countries have persisted, though these grey channels are increasingly constrained (Allen 2024) (Bloomberg 2025).

Notwithstanding these concerns, Japan strives to uphold the principles of free trade and market openness that historically undergirded its prosperity (Nishimura 2024). From Tokyo's perspective, certain "nefarious actions," such as unjust acquisition of technology, threaten not only security but fundamentally the spirit of equitable global commerce. Indeed, some Chinese enterprises sell networking gear or AI-driven solutions to developing nations using technology obtained through questionable methods (US State Dept 2020) (OPA 2024) (FT 2025).

Consequently, ring-fencing selected dual-use technologies that might deliver future military or economic advantages appears not only financially logical but strategically essential. This undertaking requires continuous review of technology-transfer recipients to deter espionage and illicit acquisition (Shiraishi 2024). In this manner, Japan's stance emulates Washington's "small yard and high fence" policy but can be viewed as less politicized because it is circumscribed by deep Sino-Japanese integration (Edmonstone 2024). Therefore, any constraints informed by national security concerns must be well justified to avoid hindering legitimate commercial engagements.

Further to this, another policy consideration generated by technology competition is to avoid the formation of an exclusive high-tech bloc among advanced states alienating developing countries by raising costs, driving them toward more cost-efficient Chinese options—visible in the rollout of networking technologies, 5G and the broader Belt and Road Initiative (Searight 2024). For this reason, a "tech alliance mindset" rests at the core of Japan's economic security, prioritizing affordable CETs that produce tangible social benefits not just for those with deep pockets but across all societies. As a result, within high-tech supply chains, Tokyo endeavors to forestall where possible excessive protectionism while mitigating existential threats and continuing to "punch above its weight."

## Promoting & Protecting Innovation

The nature of technology competition implies that adhering to free-market principles is potentially the most critical driver for advancing CETs. The U.S.-China trade war underscores how markedly different market philosophies and levels of state support influence the creation of truly cutting-edge innovation beyond just iterative performance gains. Despite the PRC's claims of advanced domestic capabilities, real-world outcomes often diverge from competition-driven pronouncements. Semiconductors, for instance, embody the perpetual pressure to evolve rapidly or risk irrelevance (Trendforce 2024). Previous-generation chips can, however, still fulfill many current applications, and China's massive manufacturing base remains a potent force.

Japan, recognized for its innovative flair, could still leverage its human capital more fully. Historically, science, technology, and innovation (STI) policies followed a "seeds-centered" logic, while defense R&D progressed under "needs-centered" principles—a dichotomy shaped by Japan's pacifist orientation (Kazeki 2022) (Chou 2024). Merging these distinct approaches to innovation has proven challenging because corporate risk-taking is hindered by conservative norms and there remains some reluctance to develop dual-use CETs despite growing demand. Tokyo's existing approach combines traditional industrial policy—offering direct support to prominent multinationals—along with initiatives to cultivate grassroots entrepreneurship (JETRO 2025) (METI 2025). Although universities have started securing R&D grants and some recent efforts at the ministerial level to amend the regulations that delimit Japan's security industries, more robust financing schemes and training programs are crucial for grassroots progress.

The Quad Investors Network (QUIN) potentially addresses some of these gaps but it must evolve into a truly concrete platform capable of injecting early-stage strategic technologies with steady funding while fostering closer ties among research institutes, industry, and policymakers in Australia, India, Japan, and the U.S. (QUIN 2025). In Japan's case, a better harnessed QUIN would integrate the country's industrial base with university-led innovation. While stakeholders recognize the importance of dual-use or high-tech ventures, funding fragmentation, risk aversion, and a dearth of cross-border incubation programs hamper momentum. Should the QUIN become institutionalized effectively, it could support and finance key research breakthroughs without constraining the free flow of talent and ideas that fuels real invention.

Another substantial impediment from Japan's viewpoint is the absence of a credible international authority to enforce economic security standards. Since the WTO cannot arbitrate matters of national security, transparent international rules are essential to clarify precisely when certain products or industries may face export controls. Japan, accordingly, looks to minilateral fora like the G7, Quad, RCEP, or CPTPP, though it remains unclear how these frameworks will handle CETs (Envall, et al. 2024). For instance, the Quad's influence on Japan's defense posture—particularly regarding CETs—has not been thoroughly tested (Kania 2017) (Bitzinger 2021). The hope is that if Japan's regulatory approach proves successful, it might ultimately contribute to global rules and avert conflicting regimes. Above all, Tokyo and its partners cannot permit global trade to lapse into a zero-sum competition as per the Cold War. As pivotal technologies grow more complex, facilitating international knowledge networks and pooling resources becomes imperative. Such cooperation paves the way for new technology consortiums that enhance resilience and expedite breakthroughs. It also strengthens policy coherence across participating nations which is a crucial in its multilateral approach not least because high-value technologies are so vulnerable to leverage in international trade diplomacy. To assist in this fight Japan has recommended a security-clearance mechanism and a nondisclosure patent system to secure sensitive data and ring-fence breakthrough research. More robust economic intelligence would likewise inform Japan's economic security controls by improving much needed visibility into foreign capabilities. Yet, since most data resides in the private sector, deeper public-private collaboration is a fundamental requirement that demands close consultation to mitigate risk while maximizing value (Suzuki 2024). Based on careful deliberation of these factors, Tokyo's economic security outlook, therefore, places a premium on collective action backed by comprehensive knowledge-sharing agendas protected by multiple layers of safeguards.

## Cyber Espionage

Protecting Japan's advanced manufacturing and tech sectors from cyber-enabled intellectual property (IP) theft remains a top priority, given that these industries present critical vulnerabilities. State-backed groups such as APT41 (Google 2024) have allegedly executed wide-ranging espionage campaigns targeting proprietary designs and trade secrets. This threat escalates further with insider risks, which can be malicious or simply due to human error and/or inadequate training.

In response, Japan has integrated enhanced vetting, regularized employee cybersecurity instruction, and enacted stricter access controls. However, even comprehensive internal measures can fail if one link of the chain is compromised. Consequently, aligning Japan's defensive strategies with those of key partner nations is crucial for resilient IP protection. One key way the government, for its part, promotes a more secure global environment for Japanese IP is by expanding economic partnership agreements (MOFA 2024).

## Semiconductor Supply Chain

The semiconductor sector—where Japan invests heavily—is persistently targeted by cyber threats that include ransomware attacks and supply chain intrusions, any of which can destabilize entire production networks. Because Japan is a critical node in the worldwide semiconductor chain, successful attacks on its infrastructure may prompt cascading consequences across varied essential industries.

To counter these risks, Tokyo pursues not only stronger domestic defenses but also collaboration with suppliers, subcontractors, and even competitors. The strategy involves increasing transparency through continuous monitoring, demanding supplier audits, and conducting regular cybersecurity evaluations. A vital component of this work is derisking—pinpointing vulnerabilities in both internal and external frameworks, especially where human factors create inherent fragility (Benson, Mouradian and Palazzi 2024). Despite these efforts, inconsistent cybersecurity standards among regional partners obstruct a truly cohesive defense posture and thus demand closer dialogue on a regular basis to work towards tightening practices and standards (METI 2023).

## Bridging Cybersecurity Standards and Interoperability Issues

One of the most significant obstacles to effective international collaboration is the profound mismatch in cybersecurity norms. Although frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001 offer consistent guidelines, actual enforcement differs from nation to nation. For Japan, harmonizing standards with nations such as Australia, the U.S., and ASEAN members is especially important. Domestically, Japan's regulatory environment can seem more stringent than the flexible approaches prevalent elsewhere, but incremental strides have been made to reduce conflicts and overlaps (JDA 2022). In ASEAN, for example, Japan has championed capacity-building projects and helped craft cybersecurity rules with individual states (NISC 2023).

Japan's rigorous emphasis on IP protection and privacy fosters an all-important sense of caution in practice when sharing critical data with countries lacking comparable defenses. Moreover, in pivotal realms such as AI and semiconductors, where IP theft threatens to erode Japan's technological leadership, officials proceed carefully in drafting data-sharing agreements that seek to increase interoperability between differing regimes via sharing information across platforms and borders. Looking forward, Japan envisages establishing an agreed set of baseline standards for data security, including mandatory incident disclosure and ongoing audits, as a vital stepping-stone to deeper regional cooperation and harmonization.

## Japan's Cybersecurity Strategy in AI and Semiconductors

Recognizing that AI and semiconductors will pivotally shape its economic security, Japan enacted the Economic Security Promotion Act two years ago to safeguard these key arenas from cyberattacks. This legislation provides a sturdier institutional foundation spanning both critical infrastructure and emerging technologies. In AI, the government is developing guidelines that incorporate "Security by Design." Meanwhile, LDP lawmakers are striving to implement "Active Cyber Defense," one of the final aspects yet to be fully operationalized in the 2022 National Security Strategy (LDP 2025).

On the international stage, Japan is intensifying bilateral and multilateral ties in cybersecurity, notably with Southeast Asia and the Quad (IPDF 2025) (Pacific Forum 2024). Such coalitions target expanded threat-intelligence sharing, joint cybersecurity drills, and interoperable defensive protocols for AI and semiconductor ecosystems—work that no nation can manage in isolation.

Domestically, regulatory frameworks and market imperatives are prompting major Japanese firms to adopt more proactive cybersecurity postures. For instance, Toshiba invests in resilient supply chain networks with cybersecurity embedded at every step. Toyota reinforces ties with domestic and foreign suppliers to boost EV supply chain robustness, employing vertical integration to secure essential components. Sony diversifies semiconductor and electronics supply chains by strengthening manufacturing bases in Southeast and South Asia, a strategy for mitigating geopolitical hazards and preventing capacity bottlenecks.

Panasonic is digitalizing and automating its manufacturing processes to bolster efficiency and adaptability, integrating eco-friendly practices where possible. Hitachi, meanwhile, leverages AI and IoT technologies for real-time supply chain oversight and enhanced demand forecasting, enabling rapid intervention when disruptions arise. Collectively, these multi-pronged efforts underscore Japan's resolve to craft a technology supply chain ecosystem capable of handling the full spectrum of contemporary global complexities.

## Japan's Vision for Technology Collaboration

Japan acknowledges that a technology alliance can be no stronger than its frailest link across all domains. Industry-led programs are pivotal for confronting sector-specific needs and ensuring cybersecurity measures remain robust yet adaptable. However, additional work is needed. Engaging directly with government officials and industry specialists, Japan sees a potential for region-wide cooperation to build cybersecurity "Centers of Excellence", which would drive innovation, share leading practices, and equip future technology professionals with high-level cybersecurity skills. Such endeavors not only foster stronger collective resilience but also help establish technology standards and best practices that can be adopted globally.

By harmonizing standards, cultivating industry-driven advances, and reinforcing mutual trust among regional partners, Japan and its allies can assemble a resilient tech ecosystem better prepared to confront emergent challenges. There is a steadfast commitment to deepen cybersecurity cooperation with the United States, Australia, and other like-minded partners to safeguard a shared digital future that is secure, flexible, and primed for the complexities of tomorrow.

## Conclusion and the "Grand Narrative"

Japan's economic security aspirations—achieving both strategic autonomy and strategic indispensability—ultimately depend on constructing concrete, cooperative mechanisms that tackle shared vulnerabilities and nurture mutually beneficial interdependencies. As argued, this includes aligning cybersecurity standards among

Quad and ASEAN members, promoting public-private R&D pipelines via the Quad Investors Network (QUIN), and devising new governance frameworks that strike a balance between security imperatives and the merits of open innovation. By systematically institutionalizing these measures—ranging from AI and semiconductors to quantum computing and advanced biotech—Japan and its partners can forge what might be termed a collective "Grand Narrative," transcending fragmented policy interventions to cultivate an inclusive vision of far-reaching and sustainable technological leadership (Shiraishi 2024). Indeed, recalibration cannot occur in isolation. Through coordinated economic security strategies anchored by transparent international rules, Japan stands to safeguard its national interests while contributing to a broader regional ecosystem in which innovation and security reinforce one another. Moving forward, Tokyo can accelerate these goals by standardizing cybersecurity protocols, expanding cross-border R&D investments, and shaping consistent governance practices that uphold export controls, preserve IP protection, and facilitate open innovation. By advancing these priorities in parallel, Japan consolidates its standing and promotes an Indo-Pacific environment resilient enough to navigate future technological and geopolitical upheavals.

## Notes

[1] Ahmed, Z. 2021. "Great Power Rivalry in Indo-Pacific." Strategic Studies 41 (4): 56-75. doi:10.53532/ss.041.04.0037.
Allen, Gregory C. 2024. Understanding the Biden Administration's Updated Export Controls. CSIS. https://www.csis.org/analysis/understanding-biden-administrations-updated-export-controls .

[2] Benson, Emily, Catharine Mouradian, and Andrea Leonard Palazzi. 2024. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-07/240709_Benson_Economic_Security.pdf .

[3] Bitzinger, R. A. 2021. "The Impact of Emerging Technologies on Asian Security Dynamics." Asia Policy 16 (3): 7-25.
Bloomberg. 2025. US probing if DeepSeek got Nvidia chips from firms in Singapore. News, Bloomberg. https://www.bloomberg.com/news/articles/2025-01-31/us-probing-whether-deepseek-got-nvidia-chips-through-singapore.

[4] Chimits, François, Conor McCaffrey, Juan Mejino Lopez, Niclas Frederic poiters, Vincent Vicard, and Pauline Wibaux. 2024. European Economic Security: Current practices and further development. Policy Department for External Relations Directorate General for External Policies of the Union, European Parliament. https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754449/EXPO_IDA(2024)754449_EN.pdf.

[5] Chou, William. 2024. The Kishida Administration's Quiet Economic and Security Overhaul. The Hudson Institute. https://www.hudson.org/security-alliances/kishida-administrations-quiet-economic-security-overhaul-william-chou .

[6] CSIS. 2024. Waht China's Ban on Rare Earths Processing Technology Exports Means. Center for Strategic and International Studies. https://www.csis.org/analysis/what-chinas-ban-rare-earths-processing-technology-exports-means.

7 Edmonstone, Georgia. 2024. Economic security policies compared: The United States, its allies and partners. United States Studies Centre. https://www.ussc.edu.au/economic-security-policies-compared-the-united-states-its-allies-and-partners .

8 Envall, H.D.P., Thomas Wilkins, Kyoko Hatakeyama, and Miwa Hirono. 2024. Minilateral solutions to the geoeconomic challenges facing Japan and Australia. East Asian Forum. https://eastasiaforum.org/2024/03/02/minilateral-solutions-to-the-geoeconomic-challenges-facing-japan-and-australia/.

9 FT. 2025. OpenAI says it has evidence China’s DeepSeek used its model to train competitor. News, London: The Financial Times. https://www.ft.com/content/a0dfedd1-5255-4fa9-8ccc-1fe01de87ea6.

10 Goodman, Matthew P. 2024. Getting Economic Security Right. Council on Foreign Relations. https://www.cfr.org/article/getting-economic-security-right .

11 Google. 2024. https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust. https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust.

12 IPDF. 2025. The Philippines Strengthens Cyber Defense in Partnership with Japan, the U.S., and Other Allies. Indo-Pacific Defence Forum. https://ipdefenseforum.com/ja/2025/01/%E6%97%A5%E6%9C%AC%E3%82%84%E7%B1%B3%E5%9B%BD%E3%81%AA%E3%81%A9%E3%81%A8%E6%8F%90%E6%90%BA%E3%81%97%E3%81%A6%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E9%98%B2%E8%A1%9B%E3%82%92%E5%BC%B7%E5%8C%96%E3%81%99/.

13 JDA. 2022. Comprehensive Regulatory Review Plan Aligned with Digital Principles. Government, Japan’s Digital Agency, Japan Digital Agency. https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/cb5865d2-8031-4595-8930-8761fb6bbe10/e3650360/20220603_meeting_administrative_research_outline_07.pdf.

JETRO. 2025. Policies and Support Tools, Japan Innovation Bridge (J-Bridge). https://www.meti.go.jp/policy/investment/5references/shisaku.html.

14 Kania, E. B. 2017. Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power. Center for a New American Security (CNAS). https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power.

15 Kazeki, Jun. 2022. “Paper derived from presentation.” Next Alliance Conference workshop in Annapolis. Sasakawa Peace Foundation USA. . https://spfusa.org/wp-content/uploads/2022/12/Mr.-Jun-Kazeki.pdf.

16 Kwan, Chi Hung. 2024. Foreign Companies’ Accelerated Withdrawal from China - A Catalyst for Global Business Restructuring. Government, Tokyo: Research Institute of Economy, Trade and Industry RIETI. https://www.rieti.go.jp/en/china/24101601.html .

17 LDP. 2025. Toward the Implementation of Active Cyber Defense. News, LDP Party, Japan. https://www.jimin.jp/news/information/209817.html.

18 METI. 2023. Industrial Cybersecurity Resilience Project. Government, METI. https://www.meti.go.jp/meti_lib/report/2023FY/000408.pdf.

19 METI. 2025. Startup support measures. Tokyo. https://www.meti.go.jp/policy/newbusiness/startup/index.html.
MOFA. 2024. Economic Diplomacy: Intellectual Property. Japan Ministry of Foreign Affairs. https://www.mofa.go.jp/policy/economy/i_property/index.html.

20 NISC. 2023. Performance Report on Cybersecurity Cooperation. ASEAN-Japan Cybersecurity Community. https://www.nisc.go.jp/eng/pdf/en_ASEAN-Japan_Performance_Report.pdf.

21 Nishimura, Rinato. 2024. Japan would benefit from an economic security strategy. Lowy Institute. https://www.lowyinstitute.org/the-interpreter/japan-would-benefit-economic-security-strategy .

22 OPA. 2024. Chinese National Residing in California Arrested for Theft of Artificial Intelligence-Related Trade Secrets from Google. Government, The United States Dept. of Justice, Office of Public Affairs. https://www.justice.gov/opa/pr/chinese-national-residing-california-arrested-theft-artificial-intelligence-related-trade.

23 Pacific Forum. 2024. US-Japan: Advancing Cybersecurity and Resiliency in the Age of Uncertainty. The Pacific Forum. https://pacforum.org/wp-content/uploads/2024/02/EN-Pacific-Forum-Layout-January-2024-Pass-Pages_Feb7-2.pdf.

24 QUIN. 2025. Quad Investors Network. https://quadinvestorsnetwork.org/.

25 Raska, M. 2019. "Strategic Competition and Future Conflicts in the Indo-Pacific Region." Journal of Indo-Pacific Affairs 2: 83-97. https://www.airuniversity.af.edu/Portals/10/JIPA/journals/Volume-02_Issue-2/06-Raska.pdf.

26 Searight, Amy. 2024. Expanding the US-Japan economic security partnership: Engaging allies and partners. JETRO, Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2024/09/JETRO-Atlantic-Council-Issue-Brief-on-Expanding-the-US-Japan-Economic-Security-Partnership.pdf.

27 Shiraishi, Shigeaki. 2024. Japan's Economic Security Policy. Konrad Adenaur Stiftung, Konrad Adenaur Stiftung. https://www.kas.de/en/web/japan/single-title/-/content/japan-s-economic-security-policy-2#:~:text=Thereafter%2C%20the%20first%20meeting%20of,supply%20chains%20more%20resilient%20and.
Suzuki, Kazuuto. 2024. The shift from economic security to geoeconomics. Institute of Geoeconomics. https://instituteofgeoeconomics.org/en/research/2024041757188/.

28 Trendforce. 2024. Over 22,000 Chinese Chip Companies Shut Down in Five Years Amid U.S. Restrictions. Trendforce. https://www.trendforce.com/news/2024/11/11/news-over-22000-chinese-chip-companies-shut-down-in-five-years-amid-u-s-restrictions/.

29 US State Dept. 2020. Egregious Cases of Chinese Theft of American Intellectual Property. Government, The United States Department of State, Committe on Foreign Affairs, Washington DC: The United States Department of State. https://foreignaffairs.house.gov/wp-content/uploads/2020/02/Egregious-Cases-of-Chinese-Theft-of-American-Intellectual-Property.pdf.

30 Zenglein, Max J, and Jacob Gunter. 2023. The party knows best. Aligning economic actors with China's strategic goals. Mercator Institute for China Studies, MERICS. https://merics.org/sites/default/files/2023-10/MERICS%20Report%20The%20party%20knows%20best-Aligning%20economic%20actors%20with%20Chinas%20strategic%20goals2_0.pdf.

31 Zhu, C. 2015. Strategic Competition and Multilateral Relations in Indo-Pacific Region, In Annual Report on the Development of International Relations in the Indian Ocean Region. Springer, 43-69. doi:10.1007/978-3-662-45940-9_3.

# Advancing trustworthiness and resiliency: India's tech play in artificial intelligence and semiconductors

Sameer Patil, Ph.D.

## Key points:

- India has actively promoted tech self-reliance through 'Make in India' and 'Aatmanirbhar Bharat' initiatives and collaboration with like-minded partners in the Indo-Pacific.

- India views self-reliance in critical and emerging technologies as essential for protecting national interests and preserving its independent foreign policy posture.

- On artificial intelligence (AI), India aspires to advance the principles of Responsible AI and AI for social impact. On semiconductors, it has initiated policy efforts to establish itself as a semiconductor manufacturing hub.

- With its unique position of having tech collaboration with the Global North and South, India can play an important role in fostering regional and international partnerships to promote tech dialogue in the Indo-Pacific, attain regulatory harmonization, advance normative principles for AI governance, and strengthen regional tech literacy.

## Policy recommendations:

- India must lead in promoting a regional dialogue on critical and emerging technologies to help identify respective countries' national tech priorities and potential for collaborative opportunities.

- Drawing upon its own experience with global rule-making, India can advocate for regulatory harmonization that respects unique local contexts and national sensitivities while strengthening regional resilience.

- India must emphasize adopting specific baseline principles for the development and deployment of AI, that advances global AI governance.

- India can strengthen regional tech literacy by focusing on cyber hygiene, and responsible use of AI applications.

## Introduction

The Indo-Pacific region is at the forefront of a technology revolution that promises to significantly reshape its economies. Over the next few decades, the deployment of critical and emerging technologies is expected to generate trillions of dollars in value for these economies. This technological advancement will not only enhance economic growth but also position Indo-Pacific countries as key players in the realignment of resilient supply chains essential for tech industries, especially in semiconductors and pursuit of responsible use of technologies such as Artificial Intelligence (AI).

However, this is easier said than done. Technology collaboration in the Indo-Pacific remains a complex endeavor. It occurs across multiple levels—bilateral, regional, and multilateral, spanning various groupings and institutions. Moreover, there are competing national priorities and initiatives in the tech domain. There is a limited understanding of how these interactions affect cross-border research and development (R&D), investment, and commercialisation at the practical level. To navigate this landscape effectively, examining the challenges and opportunities faced by different actors within specific technology verticals is crucial. This analysis can help identify best practices for enhancing cooperation in the Indo-Pacific while fostering trust among existing stakeholders.

With its vibrant and rapidly growing tech sector, India is an important actor in the emerging tech collaboration across the Indo-Pacific. The country boasts the world's third-largest startup ecosystem, supported by the second-largest internet user base and long-term robust economic growth. On the 2024 Global Innovation Index, India is placed 39th out of 133 countries.[1] New Delhi has actively promoted tech self-reliance through various policies, including tax incentives and subsidies. Initially under the 'Make in India' and then under the 'Aatmanirbhar Bharat' initiatives, the Indian government launched several policy measures to accelerate domestic manufacturing and encourage growth and innovation. Indian policymakers perceive this emphasis on self-reliance in critical and emerging technologies as crucial for safeguarding the national interest and maintaining the 'strategic autonomy' posture in India's foreign policy.

In diplomatic engagements, it has actively built partnerships with other tech powers like the United States (US), Israel, Australia, Japan, and the European Union (EU) at the bilateral and minilateral levels. More importantly, this tech diplomacy extends to the emerging economies and the Global South, which are also emerging as vibrant hubs of tech activity.[2] India has worked with many countries in this geography on digital public infrastructure, cybersecurity capacity building, and advancing dialogue on responsible uses of critical and emerging technologies. These dynamics position the country as a preferred partner for technology collaborations with both advanced and emerging economies.

This brief assesses India's pursuit of tech autonomy through two lenses: its emphasis on the principles of Responsible AI and AI for social impact and its ambitious initiatives to establish a robust national semiconductor ecosystem. The brief also evaluates the potential contribution that New Delhi can make to advance regional and international tech collaboration.

## India's ambitious AI endeavours

India ranks 40th in the world for AI readiness according to the Government AI Readiness Index 2023 (where countries are evaluated across three pillars: government, data and infrastructure, and technology).[3] However, according to another study, the Global AI Index 2024, India ranks 10th worldwide for AI capacity at the international level.[4] India doesn't have a central comprehensive national AI regulation. Instead, a combination of flagship missions, state-level initiatives, and collaborations with international tech giants demonstrate the policymakers' intention to foster a robust AI ecosystem. The flagship IndiaAI Mission aims to position India as a leading global player in AI by promoting innovation, attracting skilled professionals, and ensuring the ethical and responsible development of AI technologies.[5]

India has particularly emphasized the Responsible AI framework. Major AI-related policy documents, such as the 2018 National Strategy for AI (#AIFORALL) and a two-part document of 2021 on Responsible AI (all released by the NITI Aayog, the government's policy think tank) focus on approaches toward and operationalization of Responsible AI principles for the deployment and use of civilian AI architectures.[6] [7] [8] The 2021 documents on Responsible AI highlighted seven principles for deploying AI in India. They include safety and reliability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability and protection and reinforcement of positive human values. In 2026, India is also slated to host the AI Impact Summit, which will also highlight some of these principles.[9]

In this context, the harms caused and risks posed by the generative AI and Large Language Models (LLMs) have also figured in the policymakers' calculations, particularly sector-specific regulators. For instance, an advisory issued by the Ministry of Electronics and Information Technology in March 2024 mandated generative AI companies to monitor their LLMs to ensure that they do not publish or store unlawful content or content that could interfere with the electoral process.[10] Additionally, the advisory stipulated that LLMs and other foundational models that have not been adequately tested or that are potentially unreliable should only be made available to users in India after providing information about the unreliability of their algorithms. It also included provisions for identifying computer or software-generated content—which could potentially be used to create deepfakes or spread misinformation—through unique identifiers or metadata.[11] India has also proposed mandatory disclosure and labelling of AI-generated synthetic media on social media platforms.[12]

The Indian government has also emphasized the critical role of the private sector, industry bodies, and civil society in creating an AI ecosystem. The IndiaAI 2023 expert working group report established a roadmap for dealing with current gaps in India's AI ecosystem, and recommended establishing centers of excellence, upskilling professionals, and handling data governance, among others.[13] In addition, it underlined the importance of having reliable, representative, and unbiased data.

The National Association of Software and Service Companies (NASSCOM), India's industry tech body, embedded the principles of this framework into its "The Developer's Playbook for Responsible AI in India," released in November 2024. It identifies potential risks in AI development and deployment and offers ways to integrate ethics in developing AI systems.[14] In addition, in January 2025, the Ministry of Electronics and Information Technology released the AI Governance Guidelines Development Report that seek to foster the development of a trustworthy and accountable AI ecosystem in India.[15]

The Indian private sector, especially startups, is also taking a keen interest in developing AI systems—particularly AI for social impact to address challenges in the domains of healthcare, education, and skill-building. In the past decade, the private sector and startups invested US$7.73 billion, with 2022 alone witnessing 40 percent of this investment. Moreover, in 2022, AI-based startups received a total funding of US$5.1 billion.[16] The Indian Institute of Technology, meanwhile, has collaborated with the Taylor & Francis Group to advance AI and data science research.[17] There are also industry-based efforts, such as Microsoft's plan to train two million individuals to use AI, and state-level policies, such as Karnataka's HerShakti program, which upskills women by teaching them about AI and other emerging technologies.[18] Another capacity-building effort, though not specific to AI, is the Atal Tinkering Labs network across schools in India that aims to provide STEM tools to children so they can learn about technology at a young age (examples of tools could include 3D printers, computers and open-source microcontroller boards).[19]

NITI Aayog supports these efforts of the state government, as well as the private sector and academia. It has worked with the Center for Development of Advanced Computing (C-DAC) to launch AIRAWAT, an AI-specific cloud computing platform provided to businesses for AI innovation and research, useful for solving business and governance use cases.[20] In January 2024, C-DAC announced that it had engaged more than 25 AI-based startups to use the AIRAWAT platform.[21] Likewise, the National Informatics Centre offers several 'AI as a Service' models for developing AI applications.[22] In addition, India is set to launch a dedicated mechanism, IndiaAI Datasets Platform, that will offer Indian AI developers access to and use of datasets and AI models. [23] The dataset will reportedly be a repository for data collected from government departments and the private sector.

While these domestic initiatives establish an AI ecosystem, India is also partnering with like-minded tech partners to collaborate on AI. Under the India-US initiative on Critical and Emerging Technology, both countries have engaged their national AI invocation ecosystems for several purposes, including social impact applications.[24] India, along with the United Kingdom, has committed to collaborating on AI and other critical technologies under the Technology Security Initiative, launched in July 2024.[25] Similar collaborative initiatives exist with Australia, Japan, and Israel among others. Besides, most recently, Google announced plans to invest US$10 billion in Visakhapatnam, in eastern India for its largest AI hub outside the United States. [26]

## Developing a resilient semiconductor ecosystem

The Covid-19 pandemic accelerated efforts worldwide to secure semiconductor supply chains. India was no exception to this. Realising its critical vulnerability on China and the need for supply chain diversification, New Delhi sought to do a role reversal from being a consumer of semiconductors to manufacturing them. In 2021, it announced two key initiatives, the US$24 billion Production-Linked Incentive Scheme and the India Semiconductor Mission (ISM), that aimed to spur the creation of a domestic ecosystem in manufacturing, packaging and design.[27] [28] The Indian private sector supported these efforts by collaborating with foreign manufacturers. India also mobilized support from like-minded partners to realize its ambition of becoming a semiconductor hub. With these initiatives, the government is preparing to position India as a global semiconductor manufacturing hub. The growing interest of American and Taiwanese chip manufacturers also suggests that India has successfully made a commercial case for manufacturing in the country.

The ISM encompasses several aspects of semiconductor production, including establishing fabrication facilities, supporting the development of display manufacturing, enhancing assembly processes and testing capabilities and encouraging local design capabilities through financial incentives. Establishing fabs is at the top of New Delhi's agenda to ramp up semiconductor production. The government will provide 50 percent of the project cost to eligible applicants to set up these fabs. Under the ISM, India has approved five such fabs so far. Among these is India's first commercial semiconductor fabrication facility at Dholera, Gujarat, to be set up by Tata Electronics Private Limited in collaboration with Powerchip Semiconductor Manufacturing Corp, Taiwan, that will begin production by December 2026.[29] The fab aims to manufacture 3 billion chips annually for electric vehicles, high-power computers, telecom, and other segments.

The other planned facilities are the two semiconductor Assembly, Testing, Marking and Packaging (ATMP) units for specialised chips at Sanand, Gujarat, one by Micron Technology and the other by CG Power, in partnership with Renesas Electronics Corporation, Japan and Stars Microelectronics, Thailand; and a semiconductor ATMP unit at Morigaon, Assam by Tata Group.[30] Additionally, the Government has approved modernising the Semiconductor Laboratory in Mohali, Punjab, as a brownfield fab to expand India's VLSI capabilities.[31] The government has promised these fabs a purchase preference under the Public Procurement (Make in India) Order 2017.[32]

Another key initiative under ISM is the Design-Linked Incentive Scheme, which aims to provide financial and design infrastructure support for 100 domestic companies over five years.[33] Currently, the scheme has identified 16 firms for financial support.[34] The Ministry of Electronics and Information Technology has also begun implementing a capacity-building programme called Chips to Startup that will train 85,000 professionals in semiconductor-related activities, including embedded chip design and VLSI over the next five years.[35]

Semiconductors have also figured prominently on New Delhi's diplomatic agenda, with India working with several countries, including the United States, South Korea, and Germany, to build a resilient semiconductor supply chain. Likewise, in September 2024, the Quad grouping, which India is part of, agreed to establish the semiconductor supply chain contingency network.[36] The newest entrant here is Israel, which is working with India to bring its firms, such as Tower Semiconductor, to set up a plant.[37] So far, India has approved 10 semiconductor projects with total investment of U$18.2 billion that include fabrication plants, and testing and packaging factories.[38]

## Implementing cross-cutting regulatory mechanisms

In order to foster technological development and create a more certain regulatory environment, India has strengthened its policy framework and measures in the past decades, which have dealt an impact on tech companies and the broader ecosystem. These measures span export control mechanisms, foreign investment screening and cybersecurity. From the Indian perspective, these measures are also important as they protect the Indian tech ecosystem from malign operations traced to actors from China: India has witnessed multiple cyberattacks targeting national and commercial computer networks as well as attempts to penetrate the innovation ecosystem through predatory investments. This section takes a brief overview of such measures.

As part of its commitment to promote non-proliferation and uphold international stability by ensuring that sensitive technologies do not fall in the hands of rogue actors—state and non-state—, India periodically updates its SCOMET (Special Chemicals, Organisms, Materials, Equipment and Technologies) List that governs the export of dual-use items, technology, and software, among others.[39] The export of dual-use technology is either permitted by authorization or prohibited entirely, depending on the goods, service, or technology in question and its SCOMET classification. SCOMET is divided into eight categories from Category 0, which includes nuclear-related materials and technology, to Category 8, which includes electronics, information security and other special materials. SCOMET 8A3 imposes restrictions on the export of integrated circuits, including hybrid and multichip integrated circuits, as well as certain types of microcircuits produced by compound semiconductors.[40] There are also provisions for the regulation of software and technology exports.[41]

India does not provide financial incentives that are specifically designed to facilitate export control. However, the Ministry of External Affairs (MEA) and the industry body NASSCOM have underlined the need for Indian organizations to have an internal compliance program (ICP), particularly for dual-use items, such that they stay within India's export controls' scope despite the rapidly evolving (and frequently intangible) nature of technology. This ICP should include, among other stipulations, provisions for physical and technical security as well as internal audits, screening procedures and extensive record-keeping.[42] The MEA has also noted that having an ICP allows the organisation to access the Global Authorisation for Intra-Company Transfers (GAICT) scheme, which allows an exporter to export several types of SCOMET items to affiliated companies in other countries. [43]

Likewise, when it comes to screening foreign investments, India has a consolidated Foreign Direct Investment (FDI) policy, which guides how foreign investment can enter the country.[44] There are two routes for FDI: the automatic route, where no government clearance is required for the non-resident investor; the government route, where competent agencies must first consider and approve an FDI proposal. To further protect national security, the Indian government implemented stringent regulations in April 2020 requiring all FDI from countries sharing land borders with India, including China, to undergo prior government approval.[45] These measures were further strengthened after the border clash between Indian and Chinese military troops in June 2020. These restrictions were only partially relaxed recently when the Indian government approved certain Chinese investments in the electronics manufacturing sector.[46] Yet, the cautious approach towards

Chinese investments persists.

Another related component of the regulatory environment is cybersecurity. This has been the policy focus for India in the past one-and-a-half decades. In 2013, the government released the National Cyber Security Policy, followed by the creation of the office of the National Cyber Security Coordinator in 2015, along with a host of sector-specific regulations and technical guidelines, such as those from the Securities and Exchange Board of India and the Reserve Bank of India.[47] [48] The unveiling of the new National Cyber Security Strategy, set to replace the 2013 policy, has been considerably delayed.[49] However, the cybersecurity ecosystem continues to mature. Several businesses have also worked with the Indian government to create cybersecurity awareness amongst government departments. For instance, Samsung, Microsoft, AWS, IBM and Intel have served as industry partners for the Cyber Surakshit Bharat Initiative, the flagship programme for spreading cybersecurity awareness.[50] India has also worked closely with like-minded partners such as the US, UK, Japan and Australia on cybersecurity matters.

## Charting a course for a collaborative tech environment

As a key player in the global tech landscape and a bridge between the Global North and South, India is uniquely positioned to foster and strengthen both regional and international tech partnerships. New Delhi's contribution to a collaborative tech environment can include promoting dialogue in the Indo-Pacific on critical and emerging technologies, attaining regulatory harmonisation, advancing normative principles and strengthening tech literacy.

### Promoting a regional dialogue on critical and emerging technologies

Given its Quad membership and deep bilateral relationships with countries in the Indo-Pacific region like Singapore, Vietnam, and South Korea, New Delhi can lead in promoting a regional dialogue on critical and emerging technologies. Such a dialogue can identify a few technologies to deliberate dimensions, such as R&D, financial investments, regulation, and capacity building. India can bring the Global South perspective to this dialogue. It will also help identify respective countries' national tech priorities and where they fit in the larger regional matrix and the global push for decoupling and de-risking. In addition, this type of dialogue can also undertake a SWOT analysis to identify collaborative opportunities that can be leveraged and potential challenges that like-minded partners may encounter. Given the challenge adversarial regimes pose to countries interested in a rules-based order, forging minimum alignment on tech priorities is imperative.

### Attaining regulatory harmonisation

Countries in the Indo-Pacific region have implemented a diverse set of regulations that diverge from each other. While these measures have benefitted them in the individual capacity to advance regional collaboration, they will also need to bring in a minimum level of regulatory harmonization. This is particularly true for those technologies where regional governments seek to diversify supply chains and protect themselves from malicious actors. With its consensus-making abilities, New Delhi can contribute to attaining a certain level of harmonisation. Such synchronisation can span policies on supply chain diversification, cyber incident reporting norms, and standard-setting on certain technologies. Drawing upon its own experience with global rule-making, India can advocate for harmonising regulations that respect unique local contexts and national sensitivities.

### Advancing normative principles for AI governance

With AI-based applications and systems rapidly spreading in different domains and fields, building and retaining public trust in AI is crucial. This requires transparency in the functioning of the AI systems from the governments and private tech companies. India can play a role here. With its sustained emphasis on Responsible AI and AI for social impact, it can focus on advancing normative principles as the cornerstone of AI governance. By focusing on human-centric AI and tackling harms caused by faulty AI systems, India can emphasise the need to adopt specific baseline principles for the development and deployment of AI, particularly Generative AI, which has the most potential for misuse.

### Strengthening regional tech literacy and capacity-building

India pursues one of the most proactive cyber diplomacy in the Indo-Pacific, engaging both advanced tech powers like Australia and Japan while also working with other emerging economies like Bangladesh and Vietnam. By collaborating with like-minded partners, India can contribute by investing in tech literacy, particularly cyber hygiene, cybersecurity training, AI literacy and responsible use of AI applications. This will also help address the skilling gap that exists in many countries of the Indo-Pacific.

# Notes

[1] https://www.wipo.int/web-publications/global-innovation-index-2024/assets/67729/2000%20Global%20Innovation%20Index%202024_WEB2.pdf

[2] https://www.orfonline.org/research/the-rise-of-global-south-new-consensus-wanted

[3] Page 47, https://oxfordinsights.com/wp-content/uploads/2023/12/2023-Government-AI-Readiness-Index-2.pdf

[4] https://www.tortoisemedia.com/intelligence/global-ai/#rankings

[5] https://indiaai.gov.in/

[6] https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

[7] https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf

[8] https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf

[9] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2168319

[10] https://www.meity.gov.in/writereaddata/files/Advisory%2015March%202024.pdf

[11] https://rbihub.in/mule-hunter-ai/

[12] https://www.thehindu.com/news/national/it-ministry-proposes-strict-rules-for-labelling-deepfakes-amidaimisuse/article70189322.ece

[13] https://www.meity.gov.in/writereaddata/files/IndiaAI-Expert-Group-Report-First-Edition.pdf; https://www.meity.gov.in/content/indiaai-2023-expert-group-report-–-first-editionthe-ministry-electronics-and-information

[14] https://nasscom.in/ai/pdf/the-developer’s-playbook-for-responsible-ai-in-india.pdf

[15] https://indiaai.gov.in/article/report-on-ai-governance-guidelines-development

[16] https://www.orfonline.org/public/uploads/posts/pdf/20240430205801.pdf

[17] https://www.indiatoday.in/education-today/news/story/iit-madras-partners-with-taylor-francis-group-for-data-science-and-ai-to-amplify-research-1856455-2021-09-23

[18] https://news.microsoft.com/en-in/microsoft-to-provide-ai-skilling-opportunities-to-2-million-people-in-india-by-2025/

[19] https://aim.gov.in/atl-overview.php

[20] https://www.niti.gov.in/sites/default/files/2020-01/AIRAWAT_Approach_Paper.pdf

[21] https://www.linkedin.com/posts/cdacindia_airawat-npsf-youngindians-activity-7152935018321870848-ZW3z/

[22] https://www.nic.in/emergings/centre-of-excellence-for-artificial-intelligence/

[23] https://economictimes.indiatimes.com/tech/artificial-intelligence/indiaai-datasets-platform-to-launch-by-january-2025/articleshow/114088962.cms?from=mdr

[24] https://indiaai.gov.in/article/us-and-india-collaborate-in-ai-and-quantum-tech-for-social-good

[25] https://www.gov.uk/government/publications/uk-india-technology-security-initiative-factsheet

[26] https://blog.google/intl/en-in/company-news/

our-first-ai-hub-in-india-powered-by-a-15-billion-investment/

[27] ENS Economic Bureau, “Cabinet Decisions: Chip, display units: Nod to Rs 76K-cr scheme,” The Indian Express, December 16, 2021.

[28] https://pib.gov.in/PressReleasePage.aspx?PRID=1885367

[29] https://economictimes.indiatimes.com/tech/technology/first-chip-from-dholera-plant-by-2026-end-psmc-chairman-frank-huang/articleshow/108443331.cms?from=mdr

[30] https://economictimes.indiatimes.com/tech/technology/five-approved-semiconductor-units-across-india-and-projects-in-pipeline/articleshow/113173492.cms

[31] https://www.vssc.gov.in/SCL.html

[32] https://www.meity.gov.in/writereaddata/files/Notification%20Modified%20Scheme%20for%20Compound%20Semiconductor%20ATMP.pdf; https://d2p5j06zete1i7.cloudfront.net/Cms/2023/May/31/1685527229_Guidelines_for_Modified_Scheme_for_setting_up_of_Semiconductor_Fabs_in_India.pdf

[33] https://chips-dli.gov.in/

[34] https://chips-dli.gov.in/DLI/financialSupport

[35] https://www.meity.gov.in/content/capacity-building-4

[36] The White House, “Fact Sheet: 2024 Quad Leaders’ Summit,” September 21, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/09/21/fact-sheet-2024-quad-leaders-summit/.

[37] https://www.thehindu.com/sci-tech/technology/israels-tower-semiconductor-adani-plan-10-bln-chip-project-in-india/article68613405.ece

[38] https://www.cnbc.com/2025/09/23/india-is-betting-18-billion-to-build-a-chip-powerhouse-heres-what-it-means.html

[39] https://content.dgft.gov.in/Website/dgftprod/a2f58730-df83-49df-a437-b5f6345abb66/FTP2023_Chapter10.pdf

[40] Page 146, https://content.dgft.gov.in/Website/append3_0.pdf

[41] https://dae.gov.in/frequently-asked-questions-faq-on-the-export-control-of-nuclear-related-items/#1673947529618-a543811f-9c7a

[42] Page 9, https://www.mea.gov.in/Images/CPV/NASSCOM-GoI-Elements-of-an-Effective-Internal-Compliance-Programme.pdf

[43] Page 8, https://www.mea.gov.in/Images/CPV/NASSCOM-GoI-Elements-of-an-Effective-Internal-Compliance-Programme.pdf

[44] https://dpiit.gov.in/sites/default/files/FDI-PolicyCircular-2020-29October2020.pdf

[45] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1780251

[46] https://economictimes.indiatimes.com/news/economy/foreign-trade/forbidden-no-more-india-begins-oking-chinese-proposals/articleshow/112691334.cms

[47] https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html

[48] https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html

[49] https://www.business-standard.com/article/current-affairs/india-in-final-stages-of-clearing-national-cybersecurity-strategy-121102700663_1.html

[50] https://www.meity.gov.in/writereaddata/files/CISO%20Training%20Programme%20Brochure%20%281%29.pdf

# Leveraging its global hub status: Singapore on addressing future challenges with AI and semiconductors

Manoj Harjani

## Key Points:

- A key factor driving Singapore's approach is its prized position and reputation as a globally relevant hub for business, finance, trade, and innovation.

- Economic security—Singapore does not have a publicly documented economic security strategy, but it aims to match other advanced economies in terms of its economic security infrastructure, for example, investment screening.

- Cybersecurity—Singapore's approach is focused on building resilient infrastructure, enabling a safer cyberspace, and enhancing international cyber cooperation. The broad baseline of cybersecurity capabilities among companies in Singapore is supported by the 'Cyber Essentials' and 'Cyber Trust' certifications.

- AI and data governance—a major difference between Singapore's approach to AI governance versus data governance is that the latter is driven by obligations enshrined in law, whereas AI governance is implemented on a voluntary basis.

- Capacity building—Singapore's capacity building activities are typically focused on the region and tend to emphasise governance.
- International partnerships and collaboration—Singapore has consistently emphasised the importance of supporting multilateral institutions and participation in multilateral dialogue. Its approach is driven by the practical needs of companies within the domestically based ecosystem, and the need to ensure access to and participation in global supply and value chains.

## Policy Recommendations

- Economic security – consider the need for a specific law focused on economic security, and measures to ensure research security.

- Cybersecurity – consider addressing research security and adversarial attacks on AI systems through further amendments to relevant laws and regulations.

- AI and data governance – look beyond voluntary frameworks and guidelines to ensure that companies developing and adopting AI systems are accountable for any resulting societal harm caused.

- Capacity building – leverage leadership position in the region to advance dialogue on governance of military AI systems.

## Introduction

Singapore may be a small country—having a total population of just over 6 million and a land area of only around 740 square kilometres—but it constantly works to position itself as a globally relevant hub. Semiconductors dominate manufacturing in Singapore, contributing to approximately 40 percent of total national manufacturing value added in 2023.[1] Globally, Singapore accounts for about 10% of chip output.[2] While AI's economic contribution is more difficult to measure in comparative terms, in terms of potential, Singapore is a clear regional leader and is competitive globally. The city-state topped the International Monetary Fund's AI Preparedness Index in 2023,[3] and ranked tenth in Stanford's Global AI Vibrancy Tool for 2024.[4]

As part of its "Singapore Economy 2030" plan announced in 2023, the government aims to increase manufacturing value-add by 50% by 2030[5], and the semiconductor sector is expected to be a significant contributor towards this goal. Key pillars of the overall strategy for the sector include: (1) advance allocation of land and energy infrastructure, (2) domestic talent development through scholarships and industry partnerships, (3) investments in R&D through the Research, Innovation and Enterprise plans, (4) building a domestic ecosystem of suppliers for global companies operating in Singapore through the Partnerships for Capability Transformation scheme, and (5) supporting manufacturers to raise their energy efficiency and lower their carbon footprint.[6]

For AI, the second iteration of Singapore's national strategy, published in 2023, has laid out a vision of being a "pace-setter—a global leader in choice AI areas that are economically impactful and serve the public good."[7] Fifteen actions have been identified up to 2028, including: (1) anchoring new AI centres of excellence in Singapore-based companies, (2) strengthening the AI startup ecosystem through accelerator programmes, (3) accelerating public sector adoption of AI, (4) updating national AI R&D plans, (5) setting up a dedicated team to identify, engage and attract top global talent to Singapore, (6) scale up the domestic AI practitioner pool to 15,000, (7) supporting AI adoption by the private sector, (8) establishing a dedicated physical space for AI in Singapore, (9) secure access to compute, and (10) enhance capabilities in data management and privacy enhancing technologies.

Taken together, Singapore's prospects in terms of semiconductors and AI appear to be on a firm footing. However, much will also depend on events that are largely out of the city-state's control, including the approach of the Trump administration, the response to actions taken by the United

States from China and other critical countries and regions for semiconductors and AI, and how globally leading companies and research institutions navigate these geopolitical currents. There will also be cyclical economic factors and other risks to consider, particularly around the future sustainability of both the semiconductor and AI sectors.

## Economic Security

Singapore does not have a publicly documented economic security strategy, but its considerations go beyond narrow definitions of national security and encompass maintaining its reputation as a trusted venue for global business, finance, and trade. In a lecture delivered in April 2025, Singapore's Prime Minister Lawrence Wong noted that there was a "trilemma between economic interdependence, economic security and geopolitical competition—only two can coexist at the same time, but not all three."[8] Singapore's broad approach to navigate this trilemma has been to double down on global cooperation and the rules-based order, deepen regional cohesion and integration, and strengthen its networks and partnerships.[9]

Nevertheless, Singapore has also aimed to match other advanced economies in terms of its economic security infrastructure. In March 2024, the Significant Investments Review Act (SIRA) entered into force, containing provisions similar to inbound investment screening regimes employed by other countries.[10] Potential investors in companies designated as entities critical to Singapore's national security interests are required to notify the Ministry of Trade and Industry (MTI) within seven days of acquiring a 5 percent stake, while acquisitions of higher stakes—12, 25 or 50 percent—require prior approval.[11] Existing investors intending to relinquish a 50 or 75 percent stake are also required to obtain prior approval from the MTI.[12] Designated entities are also obligated to seek prior approval from the MTI when appointing new key personnel, and face restrictions on voluntarily winding up, dissolution, or termination.[13]

At present, ten companies have been designated under SIRA.[14] While none of the currently designated companies appear to be directly involved in semiconductor manufacturing, at least one of them—ST Engineering Digital Systems—is likely to be involved in producing AI applications related to defence and public security for government clients.[15] Given the composition of Singapore's semiconductor sector—which is dominated by foreign players mainly serving markets overseas rather than Singapore itself—it is less likely that there will be companies deemed critical to Singapore's national security interests.

However, investment screening does not account for potential reputational risks arising from 'Singapore-washing.'[16] This refers to a practice where Chinese companies shift their base of operations to Singapore to gain access to intellectual property, talent, and technology that would otherwise not be available to them, particularly if they are subject to export controls or sanctions elsewhere. Several Singapore-based companies with links to China's chip industry—an example being the Singapore affiliate of Corad Technology, which supplies China's government and defence industry with printed circuit boards—have been included in the US Department of Commerce's Entity List, which points to the possibility that this is not an isolated phenomenon.

For AI, the considerations are different given the importance of compute, or the quantity of computational resources used for training an AI model.[17] Compute, in turn, depends on a "stack" that includes both hardware and software, within which a type of semiconductor chip called a Graphics Processing Unit (GPU) and cloud computing infrastructure based in data centres are critical components.[18] The scarcity of GPUs and cloud computing resources has created a bottleneck in the race to develop more advanced AI models, and "is central to the emerging geopolitical landscape around AI. It is being used by countries as a core support in their industrial policy ambitions and as a retaliatory measure aimed at curbing the advancement of adversaries."[19]

Singapore's National AI Strategy 2.0 specifically mentions compute as an enabler and commits to "significantly increase high-performance compute available in Singapore."[20] In addition to procuring sufficient GPUs for domestic needs, Singapore is also focusing on the land and energy infrastructure needed for data centers, and on ensuring that its national pool of data centers grows sustainably based on guidelines set out in a Green Data Centre Roadmap announced in May 2024.[21] Furthermore, cloud computing service providers and data center operators now face additional scrutiny following amendments in May 2024 to the Cybersecurity Act, which expanded Singapore's cybersecurity agency's scope to cover outsourced cloud-based systems used by critical infrastructure owners.[22] The government is also considering a specific law focusing on digital infrastructure to ensure cloud computing service providers and data centre operators minimise disruptions and outages that pose wider risks.[23]

A key policy recommendation for economic security is to consider the need for a specific law focused on economic security, drawing on practices from other countries such as Japan, which enacted an Economic Security Promotion Act in May 2022. Japan's economic security law is also supported by relevant institutions, such as a dedicated division within its National Security Secretariat and a ministerial position overseeing economic security issues. Although Singapore has existing laws dealing with specific dimensions of economic security, such as investment screening, an overarching legal framework, it generally avoids disrupting market mechanisms.

Related to the need for a specific law on economic security is the need to ensure research security, given the importance of R&D in both the semiconductor and AI sectors. Research security is also intertwined with the challenge posed by foreign influence, which has become a major concern for universities and research institutions globally. While Singapore's major universities and research institutions all have research security policies in place, it is unclear how effective they have been and whether they are sufficient given the current geopolitical landscape. At the national level, Singapore's Foreign Interference (Countermeasures) Act passed in 2021 has been the primary legal tool to mitigate and manage foreign influence[24], although it does not have any specific provisions relating to R&D activities that often involve cross-border collaboration.

## Cybersecurity

Singapore's approach to cybersecurity is intertwined with sustaining its position as a trusted and secure hub for global business, finance, and trade. Since 2019, digital defence is also one of the six pillars of 'Total Defence', which has been Singapore's national defence strategy since 1984. The main institution responsible for cybersecurity nationally is the Cyber Security Agency of Singapore (CSA), which was founded in 2015. In 2016, CSA developed Singapore's first national cybersecurity strategy, which was updated in 2021 and features three strategic pillars—build resilient infrastructure, enable a safer cyberspace, and enhance international cyber cooperation—and two foundational enablers—develop a vibrant cybersecurity ecosystem and grow a robust cyber talent pipeline.[25]

The legal framework supporting CSA's work is the 2018 Cybersecurity Act[26], which was amended in 2024. The focus of the Cybersecurity Act is on protecting critical information infrastructure, empowering CSA to prevent and respond to threats and incidents in cyberspace and providing frameworks for sharing of information and licensing of cybersecurity service providers. Singapore also has a dedicated law to address cybercrime, the 1993 Computer Misuse Act[27], which has been amended regularly to keep up with trends in cybercrime and new modes and methods of computer misuse.

The broad baseline of cybersecurity capabilities among companies in Singapore is supported by the 'Cyber Essentials' and 'Cyber Trust' certifications that were launched by the government in 2022 to encourage Singapore-based organizations to implement fundamental cybersecurity measures.[28] Nevertheless, a survey conducted by the Cybersecurity Agency of Singapore (CSA) in 2023 highlighted gaps in implementation of measures under the two certifications, with most organisations surveyed indicating a lack of knowledge and experience as the primary barrier. [29]

Although there is no specific cybersecurity regulation for the semiconductor sector, one key challenge is ensuring research security, which was highlighted in the previous section. Given the highly digitalised nature of R&D activities, research security needs to encompass cybersecurity, particularly to safeguard intellectual property. In 2023, an espionage campaign allegedly linked to China targeted semiconductor companies in Hong Kong, Singapore, and Taiwan using malware.[30] At the time, Singapore did not publicly attribute the incident, but it may do so in the future, given that it made its first ever attribution in July 2025 in response to its critical infrastructure being targeted.[31]

For AI, the main cybersecurity challenge involves adversarial attacks that can take a wide variety of forms, including poisoning, backdooring, evasion, membership inference, and model extraction.[32]. Current solutions to address adversarial attacks are hampered by the fact that standards for the design and security of AI systems[33] are still nascent. In October 2024, CSA published guidelines on securing AI systems  as well as a companion guide for companies.[34] The guidelines adopt a lifecycle approach and contain specific recommendations across various stages including planning and design, development, deployment, operations and maintenance, and end of life.

A key policy recommendation for cybersecurity is for Singapore to consider addressing research security and adversarial attacks on AI systems through further amendments to relevant laws and regulations. These issues are not isolated in nature—concerns over research security apply beyond the semiconductor and AI sectors. Regarding adversarial attacks, the consideration here is to minimise the attack surface as AI is increasingly adopted across multiple sectors. Singapore could consider focusing on critical infrastructure sectors as a start, ensuring that its adoption of AI also accounts for relevant cybersecurity concerns.

## AI and Data Governance

As with cybersecurity, Singapore's approach to AI and data governance is driven by its focus on creating an enabling environment for business driven by trust and security. This point is also reflected in how Singapore structures its international partnerships and collaborations, which is addressed in the later section that focuses on this area. While AI and data governance are naturally focused on the AI sector, the semiconductor sector is also affected by policies and regulations in this area, along with companies across all economic sectors that operate in Singapore. A major difference between Singapore's approach to AI governance versus data governance is that the latter is driven by obligations enshrined in law, whereas AI governance is implemented on a voluntary basis.

For data governance, the fundamental core of Singapore's approach is the 2012 Personal Data Protection Act[35]—which was amended in 2020—and its associated regulations, most of which were put in place since 2021. Public sector data governance falls under a different set of rules that are defined in the 2018 Public Sector (Governance) Act[36] and the government's internal instruction manual on IT systems management. In addition to this, there are guidelines for critical sectors such as finance and healthcare developed by the relevant government agency overseeing the sector. Some of these guidelines are driven by international best practices—for example, the Monetary Authority of Singapore issued an information paper[37] in 2024 on data governance and management practices in the financial sector that drew in part on guidelines developed by the Basel Committee on Banking Supervision.

In contrast to data governance, Singapore's approach to AI governance relies on a voluntary framework—the Model AI Governance Framework first developed in 2018, which has since been updated in 2020. [38] There are no obligations stemming from a specific national law focused on AI in the same way that there are for data governance. This approach sets Singapore apart from jurisdictions like the European Union that have opted for an AI-specific law, although many countries have adopted an approach like Singapore's which favours leveraging existing legal frameworks. For now, it is unclear which approach is more effective, given that metrics for success can be defined in highly contradictory terms.

Another challenge for Singapore's approach to AI governance is that it relies on a delicate balancing act between several government agencies that, in some cases, have overlapping roles.[39] While this is not a challenge unique to Singapore, it has emerged as a point of discussion in multilateral dialogue on AI governance, where alternative institutional models for governing AI, such as through the creation of a single, AI-focused government agency, have been proposed as potential options for countries to consider as they decide on a model that suits their domestic needs.

One aspect that sets Singapore's AI governance approach apart is its emphasis on AI testing and evaluations. In 2022, Singapore launched AI Verify, comprising a testing framework for AI governance principles and a software toolkit.[40] While voluntary in nature, AI Verify was an important step forward in terms of translating governance principles into practice, providing companies with a way to demonstrate assurance. In 2024, Singapore expanded AI Verify to cover benchmarking and red teaming of large language models under Project Moonshot.[41] Singapore has leveraged AI Verify to align the private sector with voluntary guidelines developed by the public sector, while creating a feedback loop to improve the practical application of these guidelines.

A key policy recommendation for AI governance is for Singapore to look beyond voluntary frameworks and guidelines. This does not assume that having an AI-specific law is the preferred solution—rather, it is about ensuring that companies developing and adopting AI systems are accountable for any resulting societal harm caused. Voluntary frameworks and guidelines are not structured to incentivise accountability, and while Singapore's experiment with AI Verify has demonstrated the value of what can be achieved by focusing on implementation, important gaps remain, such as around ensuring the protection of AI systems against adversarial attacks highlighted earlier.

## Capacity Building

Singapore's capacity building efforts are traditionally focused on the Southeast Asian region and are defined by its membership of the Association of Southeast Asian Nations (ASEAN). For the semiconductor sector, Singapore's approach is more geared towards market access and strengthening regional supply and value chains, rather than capacity building per se. For AI, there is a clearer dynamic where Singapore has engaged in capacity building activities, particularly related to governance. This is also a major area for Singapore in terms of its international partnerships and collaborations, which will be highlighted in the subsequent section.

At ASEAN, Singapore played a key role in developing the ASEAN Guide on AI Governance and Ethics that was launched in February 2024, which drew heavily on Singapore's Model AI Governance Framework.[42] During its chairmanship of the ASEAN Digital Ministers' Meeting in 2024, Singapore also established the ASEAN Working Group on AI Governance (WG-AI) which has become the focal platform driving work across ASEAN related to AI.[43] Through its leadership, Singapore has strengthened ASEAN's capacity for governance of AI by developing the region's framework and creating the necessary supporting institutions for implementation.

However, Singapore has also looked beyond ASEAN for capacity building related to AI, particularly when it comes to governance. In 2022, Singapore launched the Digital Forum of Small States (Digital FOSS) initiative under the Forum of Small States which it helped establish in 1992 at the United Nations in New York as an informal and non-ideological grouping comprising more than 100 countries. Through Digital FOSS, Singapore partnered Rwanda to launch an AI Playbook for Small States[44] in September 2024 that promotes sharing of best practices contributed by FOSS countries on strategies to promote AI adoption and development, AI governance and safety, and on addressing the societal impact of AI.

A key policy recommendation for capacity building on AI is for Singapore to leverage its leadership position in the region to similarly advance dialogue on governance of military AI systems. In January 2025, the ASEAN Defence Ministers' Meeting (ADMM) released a joint statement on cooperation in military AI[45], which signalled that this issue is now on the ADMM agenda going forward, but it remains very broad in terms of its scope. Beyond coordinating with other ASEAN platforms addressing overlapping issues relevant to military AI, such as the ADMM-Plus Expert Working Group (EWG) on Cyber Security, any future work by the ADMM on military AI must navigate the evolving conversations taking place multilaterally, and the dynamics between the various ASEAN Dialogue Partners that have taken a wide range of positions on how best to approach military AI governance.

## International Partnerships and Collaboration

Given its desire to position itself as a globally relevant hub, international partnerships and collaboration are a key enabler for Singapore when it comes to both semiconductors and AI. Moreover, Singapore has consistently emphasised the importance of supporting multilateral institutions, participation in multilateral dialogue, and adherence to the norms and governance frameworks that have emerged from these institutions and the dialogue they have facilitated. The approach that Singapore takes for semiconductors versus AI is driven by the practical needs of each sector, and the needs of the companies within the domestically based ecosystem. It is also driven by the need to ensure access to and participation in global supply and value chains, given that Singapore often lacks the ability to integrate vertically due to its small size and resource constraints.

For semiconductors, Singapore's international partnerships and collaboration occur across several fronts. The most critical is investments by large global players, who are engaged by Singapore's Economic

Development Board (EDB) to locate their regional headquarters, R&D, advanced manufacturing, and other functions in Singapore with various incentives designed to facilitate their ease of doing business. But the EDB does not work alone—it collaborates with other government agencies across the full spectrum of potential business needs, such as land, energy, and manpower, to provide a holistically compelling case for investing and staying invested in Singapore.

Evidence of the EDB's success is seen in recent announcements of major new investments in Singapore's semiconductor sector. In June 2024, Taiwan-based Vanguard International and the Dutch giant NXP Semiconductor announced a joint venture for a wafer fabrication plant worth US$7.8 billion[46], while earlier in the year, Japan's Toppan Holdings broke ground on its first facility outside of Japan to manufacture substrates for semiconductor packaging.[47] Existing players have also expanded their investments—Micron broke ground on a new, US$7 billion high-bandwidth memory advanced packaging facility in January 2025, bringing its total investments in Singapore to more than US$30 billion since 1998.[48]

The other major front where Singapore has forged international partnerships and collaborations is in R&D. For example, Singapore's public sector R&D agency, the Agency for Science, Technology and Research (A*STAR) launched the 'Lab-in-Fab' initiative together with the Japanese industrial vacuum equipment supplier ULVAC and local player STMicroelectronics in 2020 to create a R&D line focused on piezoelectric microelectromechanical systems (piezoMEMS), which are used in robotics, medical diagnostic equipment, and certain consumer electronics.[49] In May 2025, a second phase of the 'Lab-in-Fab' initiative was announced, underscoring its longevity as a successful initiative, with additional research institutions participating in R&D efforts that are now being focused on developing more sustainable lead-free piezoMEMS.[50]

As with semiconductors, Singapore's international partnerships and collaborations for AI are focused on attracting investments by large global players. In 2025 alone, major tech companies such as Oracle, Alibaba, Microsoft, and Google announced that they will set up AI innovation and R&D labs in Singapore.[51] These announcements build on significant related commitments announced in recent years for cloud infrastructure, which underpins the delivery of AI-driven applications and services. For example, Amazon Web Services committed to investing US$9.3 billion in expanding its cloud infrastructure in Singapore between 2024 and 2028[52], while Google Cloud raised its total investment in Singapore to US$5 billion in the same year.[53]

In addition to attracting investments from large global players, Singapore's international partnerships and collaborations for AI are focused on promoting global governance. Singapore was an early mover in this area, leveraging the World Economic Forum to publicise its Model AI Governance Framework beginning in 2019. It was also part of the group of 29 countries that signed the Bletchley Declaration at the first Global AI Safety Summit organised by the United Kingdom in 2023.[54] This positioned Singapore as a key global player within a small club of countries at the forefront of addressing risks from the most advanced AI systems. At subsequent summits in 2024 and 2025, Singapore announced various initiatives to signal its active participation, such as the Global AI Assurance Pilot which is a testbed for technical testing of generative AI applications' adherence to assurance guidelines.[55]

Singapore also sought to carve out a leadership niche for itself in AI safety by initiating the Singapore Conference on AI (SCAI) in 2023. The inaugural SCAI was focused on harnessing the development of AI for the global good, in line with the vision outlined in the second iteration of Singapore's National AI Strategy, which is "AI for the public good, for Singapore and the world."[56] The second SCAI in 2025 led to the launch of the "Singapore Consensus on Global AI Safety Research Priorities" document, which aimed to build on the International AI Safety Report published in 2025 which was commissioned by the countries that signed the Bletchley Declaration in 2023.[57]

## Conclusion

Singapore's approach to the semiconductor and AI sectors across the dimensions of economic security, cybersecurity, AI and data governance, capacity building, and international partnerships and collaboration are anchored by a fundamental goal to sustain the city-state's position as a hub for global business, finance, and trade. Across the five dimensions, Singapore tends towards pragmatic approaches that prioritise the needs of industry. In some dimensions, such as cybersecurity and data governance, legal frameworks underpin the approach taken, whereas in others, such as AI governance, voluntary guidelines are preferred.

When considering the various policy recommendations outlined, it becomes clear that both the semiconductor and AI sectors require policymakers and regulators across multiple issue areas to work together. Given that it has aimed to operate across silos in a 'whole-of-government' fashion, Singapore is well placed to address future challenges associated with the semiconductor and

AI sectors. However, as highlighted in the introduction, much will depend on events that are largely out of Singapore's control. Singapore's long-standing support for the rules-based order, regional cooperation and integration, and international partnerships will hopefully serve it well in managing these concerns.

## Notes

[1] Ministry of Trade and Industry, Economic Survey of Singapore 2023 (Singapore: Ministry of Trade and Industry, 2023), [https://www.mti.gov.sg/-/media/MTI/Resources/Economic-Survey-of-Singapore/2023/Economic-Survey-of-Singapore-2023/FullReport_AES2023.pdf](https://www.mti.gov.sg/-/media/MTI/Resources/Economic-Survey-of-Singapore/2023/Economic-Survey-of-Singapore-2023/FullReport_AES2023.pdf), p. 52.

[2] Robyn Mak and Anshuman Daga, "Tiny Singapore's chip hub retains a big punch," Reuters, June 21, 2024, [https://www.reuters.com/breakingviews/tiny-singapores-chip-hub-retains-big-punch-2024-06-21/](https://www.reuters.com/breakingviews/tiny-singapores-chip-hub-retains-big-punch-2024-06-21/).

[3] The AI Preparedness Index compares 174 countries in terms of their digital infrastructure, human capital, technological innovation, and legal frameworks. See: [https://www.imf.org/external/datamapper/AI_PI@AIPI/ADVEC/EME/LIC/SSQ](https://www.imf.org/external/datamapper/AI_PI@AIPI/ADVEC/EME/LIC/SSQ)

[4] The Global AI Vibrancy Tool compares 36 countries across eight dimensions: R&D, responsible AI, economy, education, diversity, policy & governance, public opinion, and infrastructure. See: [https://hai.stanford.edu/news/global-ai-power-rankings-stanford-hai-tool-ranks-36-countries-ai](https://hai.stanford.edu/news/global-ai-power-rankings-stanford-hai-tool-ranks-36-countries-ai)

[5] "Singapore Economy 2023," Ministry of Trade and Industry, n.d., [https://www.mti.gov.sg/COS-2023/Committee-of-Supply-2023/Singapore-Economy-2030](https://www.mti.gov.sg/COS-2023/Committee-of-Supply-2023/Singapore-Economy-2030).

[6] "What makes Singapore a prime location for semiconductor companies driving innovation?" EDB Singapore, August 20, 2024, [https://www.edb.gov.sg/en/business-insights/insights/what-makes-singapore-a-prime-location-for-semiconductor-companies-driving-innovation.html](https://www.edb.gov.sg/en/business-insights/insights/what-makes-singapore-a-prime-location-for-semiconductor-companies-driving-innovation.html).

[7] NAIS 2.0: Singapore National AI Strategy (Singapore: Ministry of Communications and Information, 2023), [https://file.go.gov.sg/nais2023.pdf](https://file.go.gov.sg/nais2023.pdf), p. 9.

[8] Lawrence Wong, "S Rajaratnam Lecture 2025," (Lecture, MFA Diplomatic Academy, Singapore, April 16, 2025), [https://www.pmo.gov.sg/Newsroom/PM-Lawrence-Wong-at-the-S-Rajaratnam-Lecture-2025](https://www.pmo.gov.sg/Newsroom/PM-Lawrence-Wong-at-the-S-Rajaratnam-Lecture-2025).

[9] Ibid.

[10] See: [https://sso.agc.gov.sg/Act/SIRA2024](https://sso.agc.gov.sg/Act/SIRA2024).

[11] See: [https://www.osir.gov.sg/about-sira/overview-of-ownership-and-control-obligations/](https://www.

osir.gov.sg/about-sira/overview-of-ownership-and-control-obligations/).

12 Ibid.

13 Ibid.

14 See: [https://www.osir.gov.sg/designation/designated-entities/](https://www.osir.gov.sg/designation/designated-entities/).

15 See: [https://www.stengg.com/en/about-us/organisation-structure/](https://www.stengg.com/en/about-us/organisation-structure/) and [https://www.stengg.com/en/innovation/artificial-intelligence](https://www.stengg.com/en/innovation/artificial-intelligence).

16 Manoj Harjani, "Singapore and China-US chip rivalry: Steady in choppy waters for now," Counterpoint Southeast Asia 12 (September 2024), [https://lkyspp.nus.edu.sg/docs/default-source/default-document-library/csa12_manojharjani.pdf](https://lkyspp.nus.edu.sg/docs/default-source/default-document-library/csa12_manojharjani.pdf), pp. 14-15.

17 Lennart Heim and Leonie Koessler, "Training compute thresholds: Features and functions in AI regulation," arXiv, 2024, arXiv:2405.10799v2, [https://arxiv.org/pdf/2405.10799](https://arxiv.org/pdf/2405.10799), pp. 7-8.

18 Jai Vipra and Sarah Myers West, Computational Power and AI (New York, NY: AI Now Institute, 2023), [https://ainowinstitute.org/wp-content/uploads/2023/09/AI-Now_Computational-Power-an-AI.pdf](https://ainowinstitute.org/wp-content/uploads/2023/09/AI-Now_Computational-Power-an-AI.pdf), p. 4

19 Ibid., p. 11.

20 NAIS 2.0: Singapore National AI Strategy, p. 49

21 Osmond Chia, "Singapore to expand data centre capacity by at least one-third, pushes for green energy use," The Straits Times, May 30. 2024, [https://www.straitstimes.com/tech/s-pore-to-expand-data-centre-capacity-by-at-least-one-third-pushes-for-green-energy-use](https://www.straitstimes.com/tech/s-pore-to-expand-data-centre-capacity-by-at-least-one-third-pushes-for-green-energy-use).

22 Osmond Chia, "S'pore amends cyber-security law to boost oversight of national interests, essential services," The Straits Times, May 7, 2024, [https://www.straitstimes.com/singapore/politics/s-pore-amends-cybersecurity-law-to-better-secure-national-interests-essential-services](https://www.straitstimes.com/singapore/politics/s-pore-amends-cybersecurity-law-to-better-secure-national-interests-essential-services).

23 Irene Tham, "New law mooted to minimise digital service disruptions due to cloud, data centre outages," The Straits Times, March 1, 2024, [https://www.straitstimes.com/singapore/politics/new-law-mooted-to-minimise-digital-service-disruptions-due-to-cloud-data-centre-outages](https://www.straitstimes.com/singapore/politics/new-law-mooted-to-minimise-digital-service-disruptions-due-to-cloud-data-centre-outages).

24 See: [https://sso.agc.gov.sg/Act/FICA2021](https://sso.agc.gov.sg/Act/FICA2021).

25 See: [https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf](https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf).

26 See: [https://sso.agc.gov.sg/Acts-Supp/9-2018/](https://sso.agc.gov.sg/Acts-Supp/9-2018/).

27 See: [https://sso.agc.gov.sg/Act/CMA1993](https://sso.agc.gov.sg/Act/CMA1993).

28 See: [https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/

cybersecurity-certification-for-organisations/cyber-essentials](https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-certification-for-organisations/cyber-essentials).

[29] Singapore Cybersecurity Health Report 2023 (Singapore: Cybersecurity Agency of Singapore, 2023), [https://isomer-user-content.by.gov.sg/36/1051bace-6be7-4c59-934a-e43c952a32ed/csa-singapore-cybersecurity-health-report-2023.pdf](https://isomer-user-content.by.gov.sg/36/1051bace-6be7-4c59-934a-e43c952a32ed/csa-singapore-cybersecurity-health-report-2023.pdf), pp. 8-9.

[30] Arda Büyükkaya, "Chinese State-Sponsored Cyber Espionage Activity Targeting Semiconductor Industry in East Asia," EclecticIQ, October 5, 2023, [https://blog.eclecticiq.com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia](https://blog.eclecticiq.com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia).

[31] Samuel Devaraj, "Critical infrastructure in S'pore under attack by cyber espionage group: Shanmugam," The Straits Times, July 18, 2025.

[32] Manoj Harjani and Shantanu Sharma, "Adversarial attacks: An existential threat to AI," IDSS Papers, November 7, 2023, [https://rsis.edu.sg/rsis-publication/idss/ip23078-adversarial-attacks-an-existential-threat-to-ai/](https://rsis.edu.sg/rsis-publication/idss/ip23078-adversarial-attacks-an-existential-threat-to-ai/).

[33] See: [https://isomer-user-content.by.gov.sg/36/e05d8194-91c4-4314-87d4-0c0e013598fc/Guidelines%20on%20Securing%20AI%20Systems.pdf](https://isomer-user-content.by.gov.sg/36/e05d8194-91c4-4314-87d4-0c0e013598fc/Guidelines%20on%20Securing%20AI%20Systems.pdf).

[34] See: [https://isomer-user-content.by.gov.sg/36/3cfb3cd5-0228-4d27-a596-3860ef751708/Companion%20Guide%20on%20Securing%20AI%20Systems.pdf](https://isomer-user-content.by.gov.sg/36/3cfb3cd5-0228-4d27-a596-3860ef751708/Companion%20Guide%20on%20Securing%20AI%20Systems.pdf).

[35] See: [https://sso.agc.gov.sg/Act/PDPA2012](https://sso.agc.gov.sg/Act/PDPA2012).

[36] See: [https://sso.agc.gov.sg/Act/PSGA2018](https://sso.agc.gov.sg/Act/PSGA2018).

[37] See: [https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/data-governance-and-management-practices](https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/data-governance-and-management-practices).

[38] See: [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf).

[39] Jonathan Lee et al, "State of AI Safety in Singapore," Concordia AI, July 2025, [https://concordia-ai.com/wp-content/uploads/2025/07/State-of-AI-Safety-in-Singapore-2025.pdf](https://concordia-ai.com/wp-content/uploads/2025/07/State-of-AI-Safety-in-Singapore-2025.pdf), p. 6.

[40] "Singapore launches world's first AI testing framework and toolkit to promote transparency; Invites companies to pilot and contribute to international standards development," Infocomm Media Development Authority, May 25, 2022, [https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2022/sg-launches-worlds-first-ai-testing-framework-and-toolkit-to-promote-transparency](https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2022/sg-launches-worlds-first-ai-testing-framework-and-toolkit-to-promote-transparency).

[41] "Project Moonshot, powered by AI Verify, and AI

Collaborations," Infocomm Media Development Authority, May 31, 2024, [https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/project-moonshot](https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/project-moonshot).

42 See: [https://asean.org/book/asean-guide-on-ai-governance-and-ethics/](https://asean.org/book/asean-guide-on-ai-governance-and-ethics/).

43 "Singapore concludes fruitful chairmanship of the ASEAN Digital Ministers Meeting," Ministry of Digital Development and Information, January 17, 2025, [https://www.mddi.gov.sg/newsroom/singapore-concludes-fruitful-chairmanship-of-adgmin](https://www.mddi.gov.sg/newsroom/singapore-concludes-fruitful-chairmanship-of-adgmin).

44 See: [https://www.imda.gov.sg/-/media/imda/files/news-and-events/media-room/media-releases/2024/09/ai-playbook-for-small-states/imda-ai-playbook-for-small-states.pdf](https://www.imda.gov.sg/-/media/imda/files/news-and-events/media-room/media-releases/2024/09/ai-playbook-for-small-states/imda-ai-playbook-for-small-states.pdf).

45 See: [https://asean.org/wp-content/uploads/2025/02/JS-ON-COOPERATION-IN-THE-FIELD-OF-AI-IN-THE-DEFENCE-SECTOR.pdf](https://asean.org/wp-content/uploads/2025/02/JS-ON-COOPERATION-IN-THE-FIELD-OF-AI-IN-THE-DEFENCE-SECTOR.pdf).

46 "VIS and NXP to establish a joint venture to build and operate a 300mm fab," NXP, June 5, 2024, [https://www.nxp.com/company/about-nxp/newsroom/NW-VSMC](https://www.nxp.com/company/about-nxp/newsroom/NW-VSMC).

47 Ovais Subhani, "Japan's Toppan to build its first S'pore microchip materials plant, creating 350 new jobs," The Straits Times, March 14, 2024, [https://www.straitstimes.com/business/japan-s-toppan-to-build-its-first-s-pore-microchip-materials-plant-creating-350-new-jobs](https://www.straitstimes.com/business/japan-s-toppan-to-build-its-first-s-pore-microchip-materials-plant-creating-350-new-jobs).

48 Ovais Subhani, "Micron's $9.5b chip plant to give Singapore foothold in AI space; will create up to 3,000 jobs," The Straits Times, January 8, 2025, [https://www.straitstimes.com/business/microns-9-5bln-chip-plant-to-give-spore-foothold-in-ai-space-create-up-to-3000-jobs](https://www.straitstimes.com/business/microns-9-5bln-chip-plant-to-give-spore-foothold-in-ai-space-create-up-to-3000-jobs).

49 "STMicroelectronics establishes world's first "lab-in-fab" to advance adoption of piezoelectric MEMS in Singapore in partnership with A*STAR and ULVAC," STMicroelectronics, October 28, 2020, [https://newsroom.st.com/media-center/press-item.html/t4293.html](https://newsroom.st.com/media-center/press-item.html/t4293.html).

50 "A*STAR's inaugural 'Innovate Together' showcases Singapore's semiconductor ambitions on global stage" A*STAR News, May 22, 2025, [https://www.a-star.edu.sg/News/astarNews/news/press-releases/innovate-together-semiconductor-singapore-astar](https://www.a-star.edu.sg/News/astarNews/news/press-releases/innovate-together-semiconductor-singapore-astar).

51 "From Google to Alibaba: AI investments in Singapore over the last 12 months," The Straits Times, August 4, 2025, [https://www.straitstimes.com/singapore/ai-investments-in-singapore-over-the-last-12-months](https://www.straitstimes.com/singapore/ai-investments-in-singapore-over-the-last-12-months).

52 "AWS to invest an additional S$12 billion in Singapore by 2028, and announces flagship AI programme," Amazon, May 7, 2024, [https://press.aboutamazon.com/sg/aws/2024/5/aws-to-invest-an-additional-sg-12-billion-in-singapore-by-2028-and-announces-flagship-ai-programme](https://press.aboutamazon.com/sg/aws/2024/5/aws-to-invest-an-additional-sg-12-billion-in-singapore-by-2028-and-announces-flagship-ai-programme).

[53] Zhaki Abdullah, "Google's latest data centre raises its investment in Singapore to $6.7 billion," The Straits Times, June 3, 2024, [https://www.straitstimes.com/tech/tech-news/google-s-latest-data-centre-raises-its-investment-in-singapore-to-676-billion](https://www.straitstimes.com/tech/tech-news/google-s-latest-data-centre-raises-its-investment-in-singapore-to-676-billion).

[54] Aqil Hamzah, "Better global understanding, cooperation needed for safe, ethical AI development: PM Lee," The Straits Times, November 2, 2023, [https://www.straitstimes.com/singapore/better-global-understanding-cooperation-needed-for-safe-ethical-ai-development-pm-lee](https://www.straitstimes.com/singapore/better-global-understanding-cooperation-needed-for-safe-ethical-ai-development-pm-lee).

[55] "Singapore announces new AI safety initiatives at the global AI Action Summit in France," Infocomm Media Development Authority, February 11, 2025, [https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/singapore-ai-safety-initiatives-global-ai-summit-france](https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/singapore-ai-safety-initiatives-global-ai-summit-france).

[56] See: [https://www.smartnation.gov.sg/initiatives/national-ai-strategy](https://www.smartnation.gov.sg/initiatives/national-ai-strategy).

[57] See: [https://www.scai.gov.sg/2025/scai2025-report/](https://www.scai.gov.sg/2025/scai2025-report/).

# Positioning the Philippines' Competitive Edge: Semiconductors and Artificial Intelligence

Mark Bryan Manantan

## Key Points

- Once a key player in the global semiconductor industry, the Philippines has lost most of its market share and stagnated in the lower end of assembly, packaging, and testing. The Philippines' decline can be attributed to its lack of foresight and inability to adapt in the fast-changing manufacturing sector, lack of sound investment and industrial policy, and low research and development outputs.

- With its growing focus on AI adoption and innovation, the Philippines is currently consolidating its approach through the formulation of legal and regulatory frameworks, enhancing ethical, transparent guardrails, and improving educational curricula.

- As the government sets its sights on AI, the Philippines must remain committed to addressing structural challenges that continue to hinder digital transformation. Key issues, from lagging internet connectivity, poor workforce development opportunities, and increasing cybersecurity threats, can undermine the country's prospects.

## Policy Recommendations

- On semiconductors, the Philippines must increase its incentive approach towards export-oriented industries like manufacturing to regain its semiconductor market share. It should focus on improving its foreign trade and investment regime, as well as maintaining political stability, upgrading infrastructure, and investing more in human capital development and research and development, especially among promising local suppliers and enterprises.

- Similarly, on AI, improving digital infrastructure and connectivity, revisiting educational curriculum, as well as technical and vocational courses that are responsive to industry needs, are paramount. Conversely, adopting international technical standards and frameworks that promote cybersecurity and data privacy, and the ethical, safe, and transparent use of AI should be encouraged, if not mandatory.

- The Philippines must maximize its existing partnerships among Quad or ASEAN member countries to learn best practices, exchange information, attract investments, and leverage capacity-building opportunities to enhance its prospects in building a sound and innovative tech environment with a focus on AI and semiconductors.

## Context

In its ongoing digital transformation journey, the Philippines recognizes the growing importance of AI and semiconductors. Semiconductors remain a strong export for the country's electronics industry, while AI use-case applications are accelerating, especially in key sectors, ranging from Business Process Outsourcing, mining, manufacturing, and healthcare, to agriculture. The Marcos administration is formulating legal and regulatory frameworks, enhancing research and development as well as human capital development to ensure that the Philippines is well-positioned to attract foreign direct investments (FDI) and stimulate local innovation to upgrade in the global value chain. This paper examines the opportunities and challenges in semiconductors and AI and reflects on the potential prospects of the Philippines in tapping into international partnerships among the Quad and Southeast Asian countries to upgrade its competitive edge in critical and emerging technologies.

## Semiconductors

The upheaval in the US-China strategic competition has sparked a reconfiguration of the highly integrated Global Manufacturing Value Chain (GMVC). Under the guise of decoupling away from China, the US is challenging the fundamental premise of global economic interdependence marked by a rapid shift from supply chain integration to fragmentation and reindustrialization, and the remaking of trade rules and regulations. Both the Trump and Biden administrations had expanded the US export control regime and tightened investment screening mechanisms to undermine China's access to advanced chips and halt its further advancement in artificial intelligence (AI). But despite the uncertainty in the GMVC landscape, many countries in Southeast Asia, including the Philippines, see the upside of Washington's desires to decouple or derisk from Beijing. What is viewed as a major disruption can be an opportunity for the Philippines to reposition itself as a viable production alternative to China, and hopefully, a means to upgrade in the value chain of integrated chips.

## A lost opportunity

Once a promising player, the Philippines' semiconductor exports have been in sharp decline in recent decades. Its share of the global semiconductor market has been dwindling since the 2000s with 7.7. percent to 4.2 percent in 2005, and 2.5 percent in 2012. External and internal factors have contributed to the Philippines' underwhelming performance. First is its heavy reliance on foreign capital, mainly from the US and Japan. As the US and Japan's share in the global semiconductor market started to decline beginning in the 2000s, the Philippines' overdependence on both markets left it highly exposed. The resulting economic downturn that began in 2001, which eventually culminated in the global financial and economic crisis in 2008-2009, further impacted the Philippines' growth trajectory due to the significant downturn in the demand for electronics and semiconductors. The Philippines' slow recovery in the aftermath of the global financial crisis further diminished its prospects to regain its momentum, while other countries like China, Hong Kong, Taiwan, South Korea, and Singapore continued to achieve an uptick in exports in 2008. Furthermore, while Singapore and Malaysia began to expand their international semiconductor production networks with China and Taiwan, the Philippines failed to diversify and remained tied to the US and Japan, whose shares have sharply diminished. From 2012 to 2021, the Philippines' semiconductor industry continued to have slower growth, where invested capital flows have remained stagnant at 4 percent from 2022 to 2023.

China's rise as the dominant semiconductor powerhouse was a major factor in slowing down growth in the Philippine semiconductor industry. As China became a major recipient of Foreign Direct Investments in the early 2000s, the Philippines lost a significant market share. This was compounded by the fact that the Philippines failed to tap into China's growing semiconductor market. While Chinese semiconductor exports and imports grew steadily in Singapore and Malaysia, the Philippines experienced a marked decline in exports and imports to China since 2008.

Internally, the Philippines' weak incentives towards its manufacturing sector curtailed the rise of export-oriented local enterprises that could facilitate local semiconductor innovation and product development. Additionally, the Philippines' unpredictable investment climate, political instability, outdated foreign and trade regimes, lack of infrastructure, and the burdensome lack of ease of doing business also impacted its successful participation in global semiconductor production in recent decades. Finally, the Philippines continues to rank low in research and product development in chip design. Unlike Singapore, Malaysia, and Thailand, the Philippines continues to underinvest in research and development (R&D), which limits the country to the lower-tier end of the assembly and packaging in the semiconductor value chain. It is also slow in upgrading its semiconductor manufacturing equipment for the front-end and back-end of manufacturing to produce more sophisticated chips.

## Reviving the PH Chip Industry

Indeed, the ongoing recalibration of GMVC, particularly on semiconductors, serves as the reset button for the Philippines, whose performance in the highly competitive chip industry has faltered in the last two decades. With increasing labor costs in China  and the unpredictable headwinds from the ensuing US-China strategic rivalry, there is an opportunity for the Philippines to revitalize its performance in the global production networks, especially in semiconductors. The Philippines' renewed interest in revitalizing its semiconductor market is warranted. In December 2023, electronics still accounted for 58.4 percent of the country's merchandise export, where semiconductors made up approximately 70 percent.  In April 2023, cumulative electronic exports reached US$12.90 billion or 59.28 percent of the Philippines' total exports.  Of this share, the semiconductor manufacturing services accounted for 73 percent. Both the semiconductor and electronics industry account for 28 percent of the Philippines' Gross Domestic Product.  Specifically, hard disk drives under electronic data processing for the US climbed to 24.74 percent, while integrated circuits bound for Taiwan declined by 23.92 percent.  Key export destinations include Hong Kong, the USA, China, Singapore, and Japan, respectively.   There is also a growing domestic semiconductor industry comprising local firms that can support supply-chain gaps, reducing lead-times for semiconductor manufacturing as well as sourcing of local raw materials.

In response to the ongoing shifts in GMVC, particularly in semiconductors, the Philippines has outlined national policies, strategies, an institutional framework, as well as key incentives to increase growth and attract more foreign investments. Under the Philippine Development Plan (2023 to 2028), the National Economic Development Authority aims to focus on industrial modernization to further advance R&D from knowledge creation to commercializing R&D products and cultivating an innovation-centered entrepreneurial ecosystem. The Philippine government also enacted the Republic Act No. 11293, or the Philippine Innovation Act, in 2019, which mandates the establishment of the National Innovation Council to achieve a whole-of-government approach in facilitating cooperation among key government departments and agencies to drive science, technology, and innovation, especially in the semiconductor industry. Moreover, the Innovation Startup Act calls on the Department of Trade and Industry, Department of Science and Technology, and the Department of Information and Communications Technology to develop and launch various initiatives, such as the Start-up Venture Fund, the Grants-Aid Program subsidies, and the Start-Up Investment Development Plan to empower local startup communities.

To increase FDI, the Strategic Investment Priority Plan provides incentives for key sectors in critical investment areas such as income tax holidays, enhanced deductions, and a preferential five percent special corporate income tax rate. Under the CREATE Act in 2021, the corporate income tax rate shall also be reduced from 30 percent to 20 percent for domestic, micro, small, and medium-sized enterprises, and lowered tax rate up to 25 percent for all other companies. Despite the Philippines' lackluster performance in the last two decades, there remains ample room to upgrade in the design and fabrication of semiconductors. While challenges are underway, the Marcos Jr. administration's creation of an advisory council in April 2025 can make positive inroads to addressing the prevailing gaps in the semiconductor industry. Three areas stand out that the Philippines can leverage to increase its competitiveness over the short-to-medium term: (1) improving human capital development, (2) strengthening cybersecurity standards to protect valuable Intellectual Property and sensitive data, and (3) forging international partnerships with key partners to share best practices in enhancing the business environment.

## Capacity-building

Workforce development remains a key plank in ensuring a competitive edge in the semiconductor industry. The Philippine Board of Investments announced plans to produce 128,000 semiconductor engineers by 2028. To be realistic, achieving the said target will require skills mapping and establishing labor market information for data verification.

Yet the country needs to go beyond simply reaching the target quota—it must also revisit existing vocational and tertiary curricula to ensure that graduates are responsive to the market needs. The current program on academe-industry matching that aligns academic education and industry needs from basic to higher education, as well as technical and vocational training, should be integrated well within the country's long-term vision for the semiconductor industry.

Another pathway to ensure that the semiconductor industry cements a strong pipeline of industry-ready graduates is for the Philippine government to formally institutionalize collaboration between universities and semiconductor firms. At present, most arrangements are ad hoc, and no existing system is in place to ensure the sustainable provision of internships and training opportunities, as well as scholarships. In formalizing industry and academia collaborations through an institutional framework, it becomes feasible to achieve the required number of graduates, but also facilitate closer knowledge-creation, increase R&D, and commercialization of product development outputs.

## Cybersecurity

Considered as one of the most strategically valuable technologies in the modern era that powers up AI-enabled platforms, selfdriving vehicles, and the Internet of Things, semiconductors are increasingly becoming vulnerable to cybersecurity risks. Threat actors can launch cyberattacks at any stage of the chip lifecycle, from design to packaging and testing, which can disrupt production and even steal valuable IP of advanced chips. Thus, robust cybersecurity standards are becoming mandatory given the highly intricate nature of the semiconductor supply chain, dispersed at vertical and horizontal lines of production. As the Philippine courts encourage more FDIs to inject capital flows in the local semiconductor industry and set up R&D and manufacturing facilities, the establishment and adoption of international cybersecurity standards and protocols are paramount to assessing and mitigating risks throughout the chip cycle. This positions the country as a haven for protecting valuable information in technological innovation.

## International Collaboration

The Philippines must capitalize on its international networks of partners. As the current figures have shown, the US, Japan, and Singapore are key destinations for the country's exports, while India is emerging as an R&D hub. And with the current geopolitical climate, the US and Japan will only continue to invest heavily in the country's semiconductor sector.  With its positive relationships among the four countries, whether through bilateral or plurilateral formats, the Philippines must harness such linkages to meet the demands of its semiconductor industry. The Philippine government can learn from the lessons and best practices while forging strategic alliances among key educational institutions to spur R&D collaboration. Many Filipino professionals also work in such geographies. Tapping into such networks of skilled Filipino diaspora workers will be beneficial for the Philippines' semiconductor industry to encourage more dialogue and exchange of ideas. Conversely, the Philippines has also entered into formal and informal cybersecurity cooperative agreements with the US, Japan, Australia, and ASEAN. Focusing on the salient issue of strengthening and harmonizing cybersecurity standards to enhance the resilience of semiconductor supply chains should be pursued in future dialogues and exercises.

Evidently, the Philippines has a long way to go in regaining its place in the semiconductor industry. The Philippines must implement economic and regulatory reforms and perhaps, even pursue an industrial policy to match its aspirations of becoming a vibrant semiconductor hub in Southeast Asia. Further, building credible infrastructure for logistics, access to affordable and sustainable electricity, and enacting legislation to ease the flow of capital and investments are equally critical challenges for the country to overcome in the years to come. But this should not hinder the Philippines in pursuing short-to-medium term objectives such as improving human capital development, raising cybersecurity standards, and forging international partnerships as it undergoes a massive overhaul to kickstart the Philippines' resurgence in the increasingly technologically driven industries.

## Artificial Intelligence

The Philippines is actively consolidating its approach towards artificial intelligence governance. While discussions on AI ethics are known and prevalent, economic imperatives still weigh heavily in driving the current Marcos Jr. administration's efforts in enacting new legislation and regulations, supporting local innovation, and encouraging more foreign investments in the country's data center infrastructures.

Despite its rosy prospects, the Philippines must also contend with the implications of AI. Key issues surrounding AI adoption include widening digital inequities, job displacements, cybersecurity threats and risks, and data privacy. While these concerns are not unique to the Philippines, the country must redouble its efforts in addressing fundamental factors to ensure the safe, ethical, and transparent deployment of AI technologies towards its economy and society.

### Emerging Legal and Regulatory Frameworks, Strategies, and Roadmaps

Currently, three government agencies are tasked to lead the Philippines' AI journey: The Department of Trade and Industry (DTI), the Department of Science and Technology (DOST), and the Department of Information and Communications Technology (DICT). Leveraging each department's distinct mandate, the three leading departments are charged with shepherding the Philippines' goal of enhancing its R&D, adopting AI to spur new growth areas to achieve upper middle-income status, and guaranteeing that AI technologies and systems are deployed in a secure, safe, and ethical manner.

In July 2024, the DTI launched the National AI Strategy Roadmap (NAISR) 2.0. which builds on the previous strategy released in 2021. The new iteration emphasized the new challenges posed by Generative AI, while still stressing the importance of improving internet connectivity, data access, workforce development, research and development, and ethics. The National Innovation Council, a policy advisory group that guides and evaluates the country's overall innovation goals and priorities, will lead the implementation of NAISR 2.0, while the Center for AI Research was tasked to manage collaboration with regional partners like AI Singapore and industry.

Conversely, the DOST rolled out its AI National Roadmap in June 2021 that focuses on key strategic areas: Facilities and Services, Human Resources, and R&D technologies. In collaboration with various universities across the country, DOST has embarked on various AI initiatives to explore the use-case applications in health and education, mobility, environment, disaster risk reduction, autonomous vehicles, quantum, and generative AI.

For its part, DICT is focused on AI policymaking primarily through the ethical development and development of AI, capacity-building activities, and international partnerships. As AI adoption occurs at varying paces across sectors, DICT drafted the Principles for the Ethical and Responsible Use and Development of AI in Government based on the ASEAN AI Guidelines. On capacity-building, it has co-developed the Philippines Skills Framework for Analytics and AI in collaboration with the Analytics Association of the Philippines. DICT also represents the Philippines in various international forums like the AI Seoul Summit, AI Safety Summit, and supports the adoption of the ASEAN AI Guidelines and OECD AI Principles.

On the regulatory dimensions of AI, several pieces of legislation are currently tabled in the Philippine Congress that tackle the comprehensive adoption, deployment, and evaluation of AI in public and private sectors. Current legislations center on the ethical use of AI (House Bill 1777), development of AI regulations for government agencies and departments (House Bill 10751), the creation of the Philippine Council on AI (House Bill 7913 and 10944), penalizing malicious use of deepfakes (House Bill 9425), and the enhancing accountability and transparency especially on deepfakes (House Bull 10567). Because such legislations are still pending, the Philippines currently relies on existing legal and regulatory frameworks to fill the gaps in regulating AI-enabled tools such as the Cybercrime Act of 2012, Data Privacy Act of 2012, and the Innovation Start-up Act, among others.

To its credit, the Philippines' efforts towards the consolidation of its legal and regulatory frameworks on AI, investments in R&D, and desire to foster international cooperation are bearing positive results. According to the 2024 Government AI Readiness Index that measures a country's capacity to utilize and implement AI solutions in public services across three categories: Government, Technology, Data and Infrastructure, the Philippines was ranked 56th out of 188 countries, where it garnered a score of 58.51 out of 100—a figure slightly higher than the global average of 47.59.

## Addressing Structural Issues

Amid the Philippines' proactive approach to AI innovation and development, the country must not lose sight of addressing prevailing structural issues that are fundamental to its digital transformation journey.

### Inclusive Capacity-building

With AI's rapid integration in the Business Process Outsourcing and manufacturing sectors, fears of unemployment abound. If the two main sources of the country's overall revenue are adversely impacted by significant job displacements, the Philippines' economic growth will shrink. The lack of investment to improve the country's infrastructure is also deepening digital inequities, as the means for citizens to meaningfully participate in the internet economy remains desolate. For instance, inadequate access to reliable and affordable internet remains a stumbling block for more students to enroll in digital opportunities, such as e-commerce, as well as reskilling or upskilling opportunities via virtual platforms.

As AI reshapes the global economy, human capital development should be prioritized and backed by sustained investment and policy attention. In recent years, the Philippines has been on a downward spiral in fundamental skills required in business, technology, and data science. UNESCAP also found that almost 90 percent of Filipinos lack basic Information and Communications Technology Skills. In addressing such issues, the Philippine Department of Education and Commission on Higher Education are actively reviewing the basic and tertiary education curriculum to improve the country's poor performance and produce graduates who are responsive to the industry's needs.

### AI Ethics

The evolving cybersecurity-related threats and risks, such as data leakages, surveillance, ransomware, scams, disinformation and deepfakes, may inflame existing socio-political and economic divisions, cultivate extremist views and behavior, and contribute to further breakdown of trust towards institutions. With the introduction of GenAI and agentic AI, the threat surface has further expanded, while malicious actors are given new tools to exploit in launching more sophisticated spear-phishing emails, engage in various forms of online scams, as well as create deepfakes.

With AI's development at a breakneck speed, Filipino policymakers must continue to foster dialogue and exchange with the private sector to seize the opportunities of AI while mindful of its ill effects both to society and the economy. As legislation and regulatory guidelines are underway, the Philippine government must gain oversight to guarantee enforcement. Encouraging a risk-based rather than adopting a blanket approach to AI regulation provides more flexibility to encourage innovation while still implementing clear guidelines to mitigate negative impacts. As the currency of data becomes even more important in developing new frontier models, revisiting, and possibly revising existing laws in cybersecurity and data privacy and protection that reflect consent, and algorithmic transparency should be considered.

**Multistakeholder and International Collaboration**

Achieving concrete breakthroughs in these areas demands greater public-private partnerships. From promoting AI ethics to forging closer collaboration in curriculum development, the role of a multistakeholder collaboration that involves key players from government, industry, academia, and civil society cannot be further emphasized. By establishing a robust cross-sectoral approach to AI innovation and development, the Philippine government can avoid blind spots in its policymaking, while promoting or breaking down silos across public and private sector actors.

Finally, the Philippines can benefit well from international partnerships seeking to cultivate robust cybersecurity standards and promote human-centric governance of data and AI. It should continue leveraging its existing engagements with UNESCO, ASEAN, and OECD while seeking to expand with other initiatives like the Hiroshima AI principles supported by the US, Japan, and other Southeast Asian countries like Singapore.

## Conclusion

The Philippines' ambition to compete regionally and globally in the ongoing technological race, be it in semiconductors or AI, demands more than just releasing strategies, roadmaps, or forming advisory councils. It should reflect the lessons of the last three decades, where the lack of sustained and holistic government policies and investments towards upgrading infrastructure, workforce capacity, and R&D has left the country's digital innovation in a downward spiral. With renewed optimism under the current Marcos Jr. Administration, and the steady improvement in the country's economic outlook post-COVID, the Philippines must seize the current momentum in reclaiming its spot in technological innovation. This can be done through internal policy reforms that address longstanding structural impediments to economic development and digital transformation, while simultaneously forging international partnerships through the Quad and ASEAN.

## Notes

[1] Cabegin, Emily Christi A. The Challenge of China and the Role of Deepening ASEAN Integration for the Philippine Semiconductor Industry. ERIA Discussion Paper Series, April 2015. https://www.eria.org/ERIA-DP-2015-31.pdf

[2] Cabegin, Emily Christi A. The Challenge of China and the Role of Deepening ASEAN Integration for the Philippine Semiconductor Industry. ERIA Discussion Paper Series, April 2015. https://www.eria.org/ERIA-DP-2015-31.pdf

[3] Cabegin, Emily Christi A. The Challenge of China and the Role of Deepening ASEAN Integration for the Philippine Semiconductor Industry. ERIA Discussion Paper Series, April 2015. https://www.eria.org/ERIA-DP-2015-31.pdf

[4] OECD (2024), Promoting the Growth of the Semiconductor Ecosystem in the Philippines, OECD Publishing, Paris, https://doi.org/10.1787/01497fea-en

[5] OECD (2024), Promoting the Growth of the Semiconductor Ecosystem in the Philippines, OECD Publishing, Paris, https://doi.org/10.1787/01497fea-en

[6] Cabegin, Emily Christi A. The Challenge of China and the Role of Deepening ASEAN Integration for the Philippine Semiconductor Industry. ERIA Discussion Paper Series, April 2015. https://www.eria.org/ERIA-DP-2015-31.pdf

[7] Athukorala, Prema-chandra. The Philippines in global manufacturing value chains: A tale of arrested growth. Australian National University, Working Papers in Trade and Development No. 2021/2022. September 2021. https://crawford.anu.edu.au/sites/default/files/2025-02/acde_athukorala_2021_22.pdf

[8] OECD (2024), Promoting the Growth of the Semiconductor Ecosystem in the Philippines, OECD Publishing, Paris, https://doi.org/10.1787/01497fea-en

[9] Cabegin, Emily Christi A. The Challenge of China and the Role of Deepening ASEAN Integration for the Philippine Semiconductor Industry. ERIA Discussion Paper Series, April 2015. https://www.eria.org/ERIA-DP-2015-31.pdf

[10] Athukorala, Prema-chandra. The Philippines in global manufacturing value chains: A tale of arrested growth. Australian National University, Working Papers in Trade and Development No. 2021/2022. September 2021. https://crawford.anu.edu.au/sites/default/files/2025-02/acde_athukorala_2021_22.pdf

[11] https://seipi.org.ph/about-the-industry/#:~:text=The%20Philippine%20Electronics%20Industry%20is,destination%20of%20the%20electronics%20sector.&text=a.,Northern/Central%20Luzon%20and%20Cebu.

[12] SEIPI website (2025), About the industry. https://seipi.org.ph/about-the-industry/#:~:text=The%20Philippine%20Electronics%20Industry%20is,destination%20of%20the%20electronics%20sector.&text=a.,Northern/Central%20Luzon%20and%20Cebu.

[13] SEIPI website (2025), Philippine Electronics Export Performance 2025. https://seipi.org.ph/philippine-electronics-export-performance-june-2025/

[14] SEIPI website (2025), Philippine Electronics Export Performance 2025. https://seipi.org.ph/philippine-electronics-export-performance-june-2025/

[15] OECD (2024), Promoting the Growth of the Semiconductor Ecosystem in the Philippines, OECD Publishing, Paris, https://doi.org/10.1787/01497fea-en

[16] OECD (2024), Promoting the Growth of the Semiconductor Ecosystem in the Philippines, OECD Publishing, Paris, https://doi.org/10.1787/01497fea-en

[17] World Bank. 2024. Better Internet for All Filipinos: Reforms Promoting Competition and Increasing Investment for Broadband Infrastructure - A Policy Note. © World Bank. http://hdl.handle.net/10986/40924 License: CC BY-NC 3.0 IGO

[18] Bhandari, Ritu. Bridging the skills gap: Fuelling careers and the economy in Australia. Economist Impact. June 15 2023. https://impact.economist.com/new-globalisation/bridging-skills-gap-fuelling-careers-and-economy-australia

CONVERGE
INDO-PAC
CRITICA
FORU
PACIFIC FORUM INTERNATIONAL
INDO-PACIFIC CRITICAL TECH FORUM 2024
Maria Monica W

CONVERGE
INDO-PACIFIC CRITICAL TECH FORUM 2024
ESRP
Daniele Cave
Hisashi Riko

CONVERGE
INDO-PACIFIC CRITICAL TECH FORUM 2024
acific Forum International
esearch Center for Advanced Science and Technology
niversity of Tokyo, Japan
ctober 10-11, 2024
CONVERGE
INDO-PACIFIC CRITICAL TECH FORUM 2024
Konark Bhandari

ESRP
東大先端研
Danielle Cave

PACIFIC FORUM
INTERNATIONAL

converge.pacforum.org | pacificforum@pacforum.org