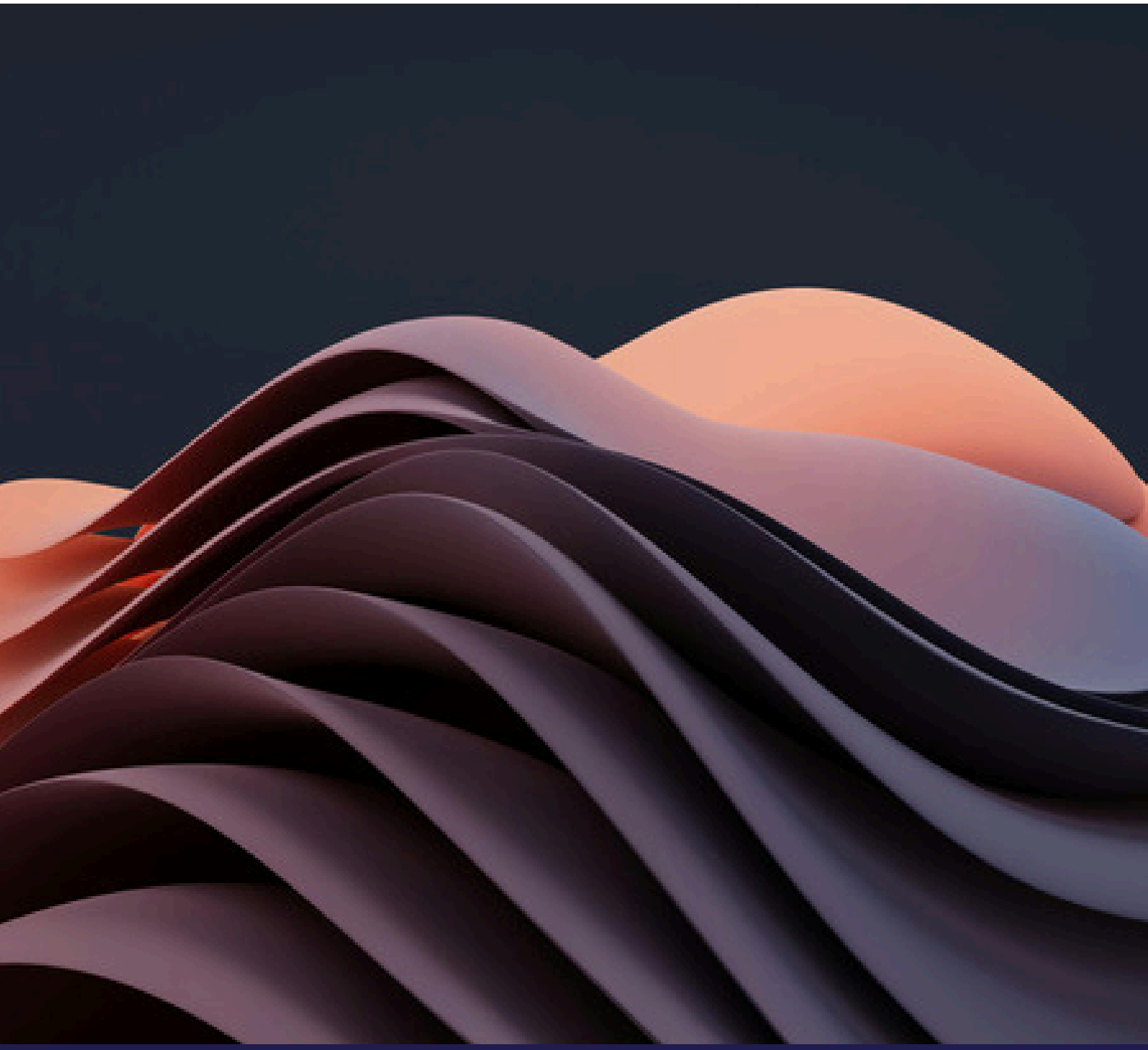
Southeast Asia Tech Stack Sovereignty

Paper 1: An Analytical Framework for Understanding Technology Sovereignty



April 2026

Southeast Asia
Public Policy Institute

Southeast Asia
Public Policy Institute

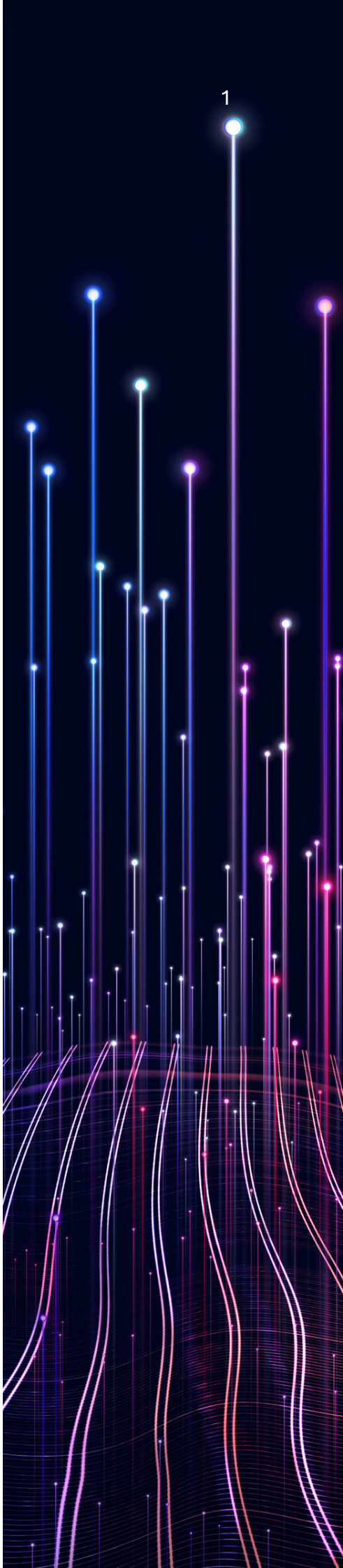
This report has been developed by the Southeast Asia Public Institute to support stakeholders' understanding of the concept of technology stack sovereignty in Southeast Asia. The views expressed are those of the authors and do not necessarily reflect the views of any affiliated organisations or partners. It is also not intended to be an exhaustive review of policy, legislation, or regulation and should be used with due caution and consideration of its scope and limitations

You can find out more about the Institute's work at seapublicpolicy.org

Table of Contents

Abstract

This paper introduces the concept of tech stack sovereignty as an analytical framework for assessing Southeast Asia's position in a fragmenting global technology order. It defines sovereignty not as autarky or self-sufficiency, but as the capacity to exercise control, maintain optionality, and ensure substitutability across interdependent technology systems. The framework identifies three analytical domains—access, capability, and governance—and situates Southeast Asia's technology challenges within the constraints faced by mid-sized, trade-dependent economies operating between competing global technology ecosystems.



1 Why Sovereignty is now a Technology Question

The global technology order is fragmenting. What was once assumed to be a stable regime of open markets, interoperable standards, and depoliticized supply chains has given way to strategic competition over the commanding heights of the digital economy. Technology is no longer simply an input to growth or a domain of commercial competition. It has become the primary terrain of geopolitical rivalry, the substrate of military capability, and the architecture of economic security. The shift from geopolitics to geoeconomics—and from geoeconomics to techno-economic statecraft—is now underway[1]. Traditional geopolitics centered on territory, alliances, and military positioning. Geoeconomics moved competition into trade policy, investment screening, and industrial subsidies. Techno-economic statecraft goes further: it uses control over semiconductor design software, advanced manufacturing equipment, cloud infrastructure, AI models, data flows, and technical standards as instruments of strategic leverage. States that cannot shape or substitute these systems face structural dependence.

For Southeast Asia, this shift poses an acute challenge. The region's economic model has been built on integration into global value chains and strategic ambiguity between competing powers. Southeast Asian countries have thrived by remaining non-aligned, attracting investment from multiple sources, and leveraging their position as manufacturing and logistics hubs in an interconnected world[2]. But the assumptions underlying this model are eroding. Rivalry between the US and China is driving a process of technology bifurcation, in which competing ecosystems—across hardware, software, platforms, standards, and governance regimes—are becoming less interoperable and more politically conditioned. While Southeast Asia has benefitted from the development of China+1 supply chains, the situation is become more challenging, especially concerning technology and export controls, sanctions, and technology transfer restrictions[3].

Three developments in the last five years have made this particularly urgent for Southeast Asia.

1. The COVID-19 pandemic exposed the fragility of single-supplier dependencies.

2. US-China decoupling accelerated. ASEAN states found themselves pressured to choose sides in domains ranging from cloud computing to artificial intelligence partnerships[4].

3. Internal coordination failed. Despite rhetorical commitments to ASEAN centrality, member states pursued divergent and often contradictory technology strategies. Singapore positioned itself as an AI hub through partnerships with American firms. Indonesia pursued aggressive data localization to assert sovereignty over the digital economy. Thailand launched electric vehicle industrial policies tied to Chinese battery supply chains. Malaysia sought semiconductor investment from both sides.

The result is a strategic dilemma. ASEAN states can no longer treat technology as a neutral import, assuming that market forces will deliver optimal outcomes. But it is also unrealistic to pursue autarkic self-sufficiency. The capital intensity, technical complexity, and scale requirements of modern technology systems make vertical integration effectively impossible for mid-sized economies. The question is not whether to engage with technology sovereignty, but how to exercise it without self-defeating isolationism.

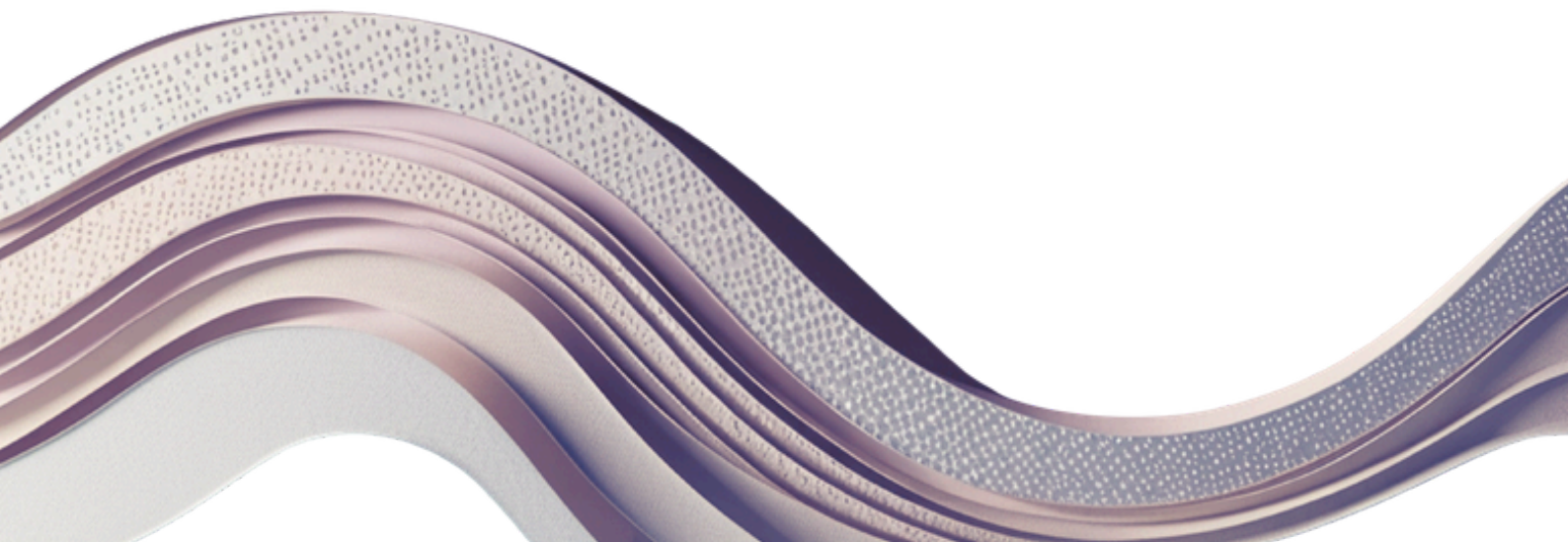
This paper introduces ‘tech stack sovereignty’ as a framework for navigating this dilemma. It rejects both passive dependence and self-sufficiency in favor of a third path: strategic coordination to maintain optionality and ensure substitutability. The goal is not to own every layer of every technology system, but to exercise meaningful control over the systems that matter most. Where individual capacity falls short, groupings such as ASEAN and the EU have the opportunity to act collectively to create shared sovereignty.

2 From Technology Markets to Technology Stacks

Traditional economic analysis treats technologies as discrete products or sectors. Semiconductors, software, electric vehicles, cloud computing—each is analyzed as a separable market with its own competitive dynamics, firm strategies, and policy instruments. This approach made sense in an era when technologies were relatively modular and market access was governed by stable multilateral rules.

This framework no longer captures how power operates in the digital economy. Modern technologies do not function as standalone products. They are interdependent systems organized vertically, where value, control, and dependency emerge across layers rather than within isolated sectors[5]. A smartphone is not just a device; it is a stack of advanced technologies that includes semiconductors, batteries, optical components, operating systems, app stores, cloud services, payment rails, data analytics, and increasingly AI—each layer controlled by different firms and governed by different rules. In each case, the unit of analysis is not the product but the system—the way components fit together, the points where control is exercised, and the dependencies that emerge between layers. Power in the digital age comes from the ability to shape or substitute entire systems, rather than dominance in isolated industries.

For Southeast Asia, this shift changes everything. ASEAN states may not out-invest the United States or China in semiconductor fabrication, cloud computing, or artificial intelligence research. But they do not need to. The question is not whether Southeast Asian countries can build every layer of every stack. The question is whether they can maintain optionality, and ensure substitutability in the layers that matter most. Thinking in stacks reveals where leverage exists, where coordination changes outcomes, and where dependence is structural versus where it is a policy choice.



3 Defining Tech Stack Sovereignty

What Tech Stack Sovereignty is (and is not)

Sovereignty is one of the most contested concepts in international relations, and its application to technology is particularly prone to ambiguity. In this series, tech stack sovereignty is not autarky. It is not the ability to produce every component of a technology system domestically and the vertical integration of supply chains within national borders without foreign inputs. For ASEAN member states—mid-sized, trade-dependent economies deeply integrated into global value chains—this would be structurally impossible. The capital intensity of semiconductor fabrication, the scale requirements of hyperscale cloud infrastructure, and the R&D budgets required for frontier AI research exceed the capacity of any individual ASEAN state and, in many cases, the region as a whole.

At the same time, sovereignty should not be conflated with closure. Openness to global technology ecosystems can materially enhance national capability. As highlighted in our *Opportunities at the Nexus of AI and Cybersecurity* report, AI-driven security is most effective when operating on consolidated cloud-based data estates, where large-scale telemetry improves threat detection and response[6]. Access to frontier AI models and hyperscale infrastructure can therefore strengthen resilience—provided governance, oversight, and substitutability are preserved. Managed openness, in this sense, can reinforce rather than weaken tech stack sovereignty.

Nor is sovereignty binary. States are not either sovereign or dependent; sovereignty exists as a gradient. A state can be highly sovereign in some layers of a stack and deeply dependent in others. It can exercise sovereignty in some technology domains while remaining exposed in others. Sovereignty is also not permanent. It must be actively maintained through investment, regulation, diplomatic coordination, and continuous adaptation to shifting technical and geopolitical realities.

A Functional Definition

In this research series, tech stack sovereignty is defined as **the capacity of a state or region to exercise meaningful control over technology systems relevant to economic security, policy autonomy, and strategic optionality.**

This definition emphasizes capacity rather than ownership, and influence rather than self-sufficiency. A state may lack the ability to build or own key technologies, yet still exercise sovereignty if it can determine how those technologies operate within its jurisdiction and economy.

The Three Functions of Tech Stack Sovereignty

To operationalize this definition, sovereignty is assessed using three criteria: control, optionality, and substitutability. These criteria do not describe technology systems themselves. Rather, they are evaluative tests applied to any part of a technology stack to determine the degree of sovereignty exercised over it.

1. Control

Control refers to the ability to set rules, enforce standards, and shape outcomes within technology systems, even when not owning all components. A state exercises control when it can regulate how data flows across borders, audit models, require interoperability, or mandate transparency. Control does not require ownership. It requires regulatory capacity, technical expertise, and the geopolitical leverage to enforce compliance.

2. Optionality

Optionality refers to the ability to choose between providers, architectures, or regulatory frameworks without coercion. A state has optionality when it can select a variety of American, Chinese, or European cloud providers based on cost, performance, and alignment with domestic priorities—not because it has been sanctioned, cut off, or forced into an exclusive partnership. Optionality means that no single external actor can impose unacceptable terms by threatening to withdraw access.

3. Substitutability

Substitutability refers to the ability to switch providers or layers without catastrophic economic, security, or operational disruption. A state achieves substitutability when its systems are designed for portability, when workloads can migrate between clouds, when data formats are standardized and open, and when dependencies on any single vendor are limited. Substitutability is the practical expression of optionality. Without it, choice is theoretical.

These criteria are mutually reinforcing. Control without optionality is brittle; optionality without substitutability is hollow; substitutability without control is passive. Together, they provide a practical lens for assessing sovereignty across complex, interdependent systems.

Strategic Sovereignty in the Southeast Asian Context

For Southeast Asia, sovereignty will not be achieved through total and extensive ownership of frontier technologies, but through strategic participation, governance capacity, system design, and coordination. Control, optionality, and substitutability are therefore the relevant measures of sovereignty in a region characterized by openness, integration into global value chains, and structural exposure to external technological power.

These criteria will be applied consistently across the series to assess where Southeast Asian countries' dependence is structural, where it is a policy choice, and where individual states' actions and regional coordination can materially shift outcomes.

4 The Three Layers of Tech Stack Sovereignty

The sovereignty criteria defined above—control, optionality, and substitutability—describe how sovereignty is exercised. The framework introduced here addresses a different question: where, within modern technology systems, sovereignty is exercised or constrained.

Overview of the Three Domains

Modern technologies operate as vertically integrated systems rather than standalone products. Value creation, control, and dependency emerge across distinct functional domains that interact and reinforce one another. This framework distinguishes three sovereignty domains that locate where power, control, and vulnerability reside within a technology stack.

Access Sovereignty

Control over entry, use, and movement of critical inputs
(jurisdiction, storage, access, cross-border flows)

Capability Sovereignty

Control over system logic and decision making
(algorithms, AI models, production and execution logic)

Governance Sovereignty

Control over rules, standards, and enforcement
(market access, compliance, coordination power)

These domains are not evenly distributed across the global economy. In particular, capability sovereignty is structurally concentrated in a small number of economies and will likely remain so for the foreseeable future. The purpose of this framework is not to imply that all states can attain equal control across domains, but to clarify how sovereignty is exercised under conditions of persistent capability dependence—through control over access, through governance of how systems operate, and through the management of lock-in, optionality, and reversibility.

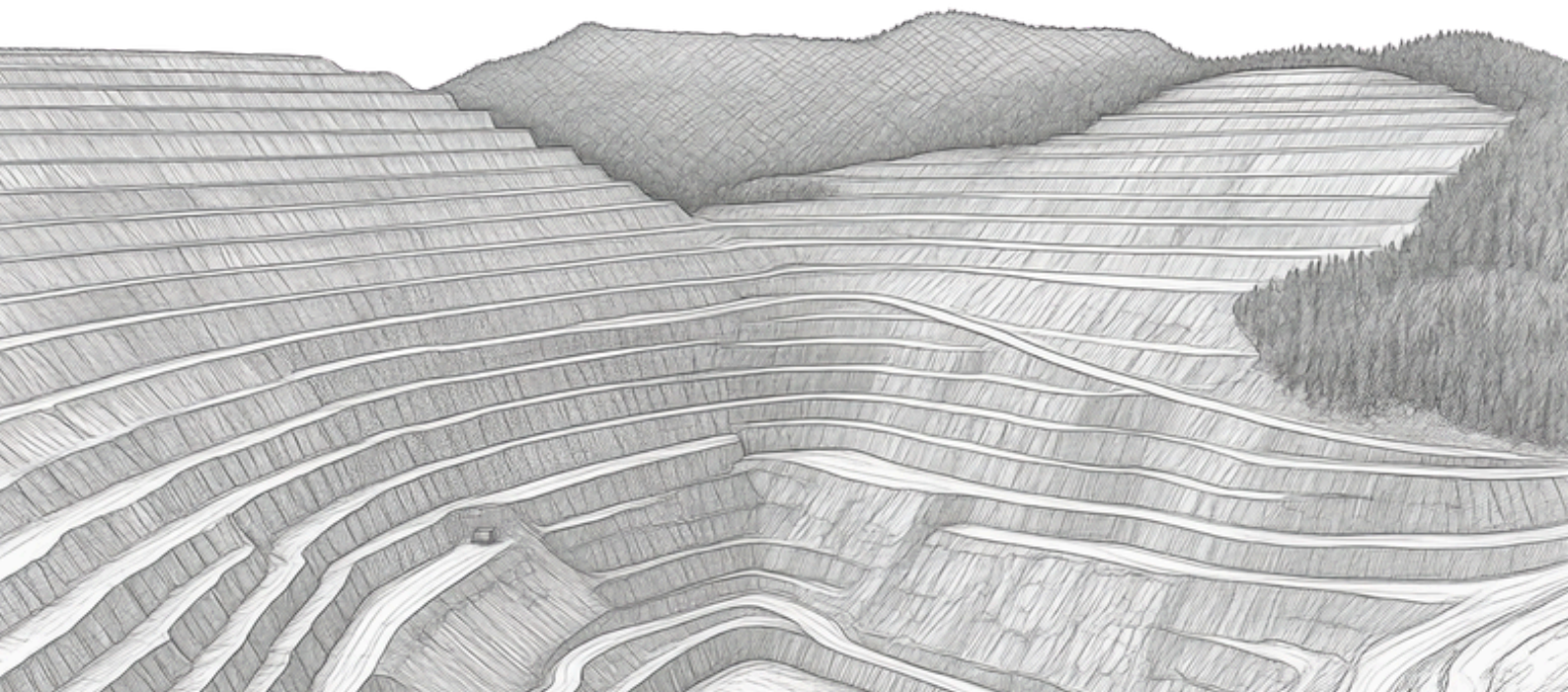
Domain 1: Access Sovereignty

Control over the resources that enter technology systems

"Who controls access to essential inputs? Can supply be diversified or substituted? Can value be captured from input provision rather than simply extracted and exported?"

These inputs include natural resources (critical minerals, rare earths, energy), data generated within a jurisdiction, skilled labor, and critical components such as semiconductors or batteries. Control at this stage creates boundary leverage: the ability to shape downstream behavior by granting or withholding access, attaching conditions, or influencing pricing and availability.

Access sovereignty does not determine how inputs are processed or integrated once they move further down the technology stack. A state may therefore exercise strong access sovereignty while remaining dependent elsewhere in the system. Indonesia's nickel endowment illustrates this distinction. Control over reserves and export licensing provides leverage at the point of supply, but the economic and strategic outcomes of that leverage depend on how downstream refining, battery production, and vehicle integration are organized; questions that fall under capability and governance sovereignty rather than access sovereignty itself.



Domain 2: Capability Sovereignty

Control over how technology systems operate, evolve, and reconfigure

"Who builds the systems? Who controls the operational logic? Can systems be modified, substituted, or operated independently of providers?"

Capabilities include production processes (manufacturing technologies, fabrication methods), software and algorithms (operating systems, AI models, vehicle control software), operational architectures (cloud platforms, telecommunications networks, grid management), and the capacity to integrate, maintain, and upgrade these systems over time. This is where operational intelligence, adaptability, and day-to-day control are concentrated.

A state exercises capability sovereignty when it can meaningfully influence how systems function rather than just deploy them. This depends on whether system design and core intellectual property are accessible, whether system behavior can be inspected or audited, and whether dependence on any single provider can be reduced through substitution or migration. Where systems are proprietary, opaque, and tightly integrated, states may operate advanced technologies while remaining structurally dependent on external actors.

Capability sovereignty is typically the most difficult domain to secure. It requires sustained investment in research and development, skilled human capital, and the accumulation of tacit knowledge embedded in engineering teams, manufacturing processes, and operational practice. Yet it is not all-or-nothing. Partial capability sovereignty can be achieved through targeted industrial policy, technology-transfer arrangements, co-development requirements, and regional collaboration. A state does not need to train frontier AI models to exercise influence over how models are used, audited, or adapted to local contexts; nor does it need to build hyperscale cloud infrastructure capabilities to reduce lock-in by requiring interoperability, portability, and multi-vendor architectures.

Domain 3: Governance Sovereignty

Control over the rules, standards, enforcement mechanisms, and coordination frameworks that shape technology systems

"Who sets the standards? Who defines compliance? Can a state or region shape global rule-making, or only adapt to rules written elsewhere?"

Governance operates as a meta-domain. It determines what is legal, what is required, what is possible. It operates at multiple scales—national laws, regional harmonization, international standards, extraterritorial enforcement. Governance sovereignty is the ability to regulate technology systems even when lacking technical or economic dominance.

A state exercises governance sovereignty when it can do more than adapt to rules written elsewhere—when it can credibly impose obligations, enforce compliance, and influence how markets are structured. This depends not only on formal rule-making authority, but on regulatory capacity, institutional credibility, and the ability to withstand lobbying or retaliation.

Governance sovereignty is also where coordination matters most. Individually, states may impose compliance costs without altering firm behavior. Collectively, harmonized rules and aligned enforcement can create regulatory markets large enough to shape global practices. For regions such as ASEAN, coordination can transform limited national leverage into collective bargaining power, enabling standards, certifications, and procurement rules to influence how external technologies operate.

Strong governance sovereignty has a force-multiplier effect across the technology stack. It can partially compensate for weak capability sovereignty by mandating transparency, auditability, interoperability, and portability. It can strengthen access sovereignty by attaching conditions to market entry, requiring local value creation, or shaping investment incentives. The European Union illustrates this logic: despite lacking dominant cloud platforms or frontier AI developers, it exercises meaningful sovereignty through regulatory frameworks and procurement rules that external firms must comply with to access its market.

5 Southeast Asia's Structural Position and the Logic of the Series

Southeast Asia occupies a constrained but consequential position in the global technology order. ASEAN member states are not technology superpowers or global leaders in areas such as semiconductor design and artificial intelligence research. But at the same time, they are not peripheral. The ASEAN-6 economies—Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam—are mid-sized, rapidly growing, and deeply integrated into global value chains. Collectively, ASEAN-10 is a $3.6 trillion economy with 680 million people, comparable in scale to the European Union. The region is a critical node in global manufacturing networks, a fast-growing market for digital services, and a major generator of economic and social data.

This position creates hard constraints on sovereignty, but also actionable opportunities. No single ASEAN state can match the R&D budgets, market scale, or capital intensity of the United States, China, or the European Union, and capability-intensive layers of modern technology stacks—such as frontier AI models or advanced semiconductor design and production—will likely remain concentrated. National strategies that seek to replicate these capabilities domestically are expensive and time-intensive. Governments in the region have invested billions of dollars in digital infrastructure and sector-specific capabilities such as EV production. As a result, ASEAN states compete with one another for the same foreign capital. A stack sovereignty view may help individual economies, and ASEAN as a whole, act and invest more strategically.

Capability sovereignty is therefore likely to be selective and negotiated rather than comprehensive. The strategic question is not how to replicate frontier capabilities wholesale, but how to limit lock-in, preserve optionality, and shape deployment terms. Sovereignty is often exercised less through direct control than through governance — standards-setting, interoperability requirements, procurement rules, and coordinated enforcement.

Regional coordination changes the sovereignty equation. Acting collectively, Southeast Asia constitutes a market large enough to set baseline standards, demand interoperability, and negotiate terms that individual states cannot. Shared procurement, infrastructure investment, and coordinated regulatory enforcement could create bargaining power that directs external actors to engage with the region as a whole rather than cherry-picking accommodating jurisdictions.

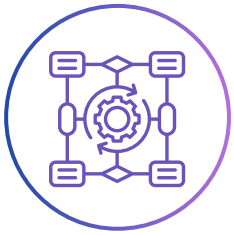
This does not require uniformity. Member states have different priorities and geopolitical exposures. Coordination requires alignment on minimum common denominators like interoperability standards, mutual recognition of certifications, reciprocal data flows, and coordinated positions in multilateral forums.

Thinking in stacks reveals where power operates, where dependency emerges, and where coordination changes the game — shifting focus from sectors to systems, from ownership to control, from national champions to regional leverage.

The remainder of this series applies the three-layer framework to the most strategically consequential technology stacks for Southeast Asia. Each paper maps a specific domain, assesses ASEAN's position across the four layers, and identifies where regional coordination can shift outcomes. The objective is not to eliminate dependence, but to govern it—preserving agency and room to maneuver in an increasingly fragmented global technology order.

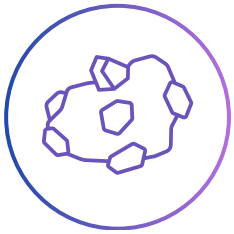
How to Read This Series

Paper 1
Framework



What is tech stack sovereignty and why does it matter for Southeast Asia?

Paper 2
Critical Mineral Stack

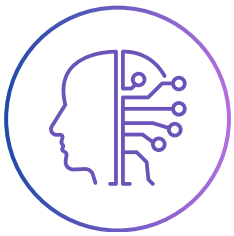


Can Southeast Asia move from resource extraction to value capture?

Paper 3
Electric Tech Stack

Can Southeast Asia build electric tech stack capabilities to move beyond assembly hub status?

Paper 4
Artificial Intelligence Stack



Can Southeast Asia translate growing AI adoption into its own AI ecosystem and capabilities?

Endnotes

[1] Roberts, A., Choerorsky, H., & Polk, N. (2019). The Geoeconomic World Order.
[2] Kurlantzick, J. (2023). Southeast Asia's Dilemma. Council on Foreign Relations.
[3] U.S. Department of Commerce (2022). Implementation of Additional Export Controls on Certain Advanced Computing and Semiconductor Manufacturing Items.
[4] Ghiasy, R., & Krishnamurthy, R. (2021). China's Digital Silk Road and Southeast Asia.
[5] Bratton, B. H. (2016). The Stack: On Software and Sovereignty. MIT Press.
[6] SEAPPI (2025), Opportunities at the Nexus of AI and Cybersecurity.

www.seapublicpolicy.org