TECHNOLOGICAL DEPENDENCE AS A SOURCE OF ECONOMIC VULNERABILITY: EVIDENCE AND POLICY OPTIONS FOR EMERGING ECONOMIES

Mamasoatov Najmiddin
Tashkent State University of Economics
najmiddinmamasoatov07@gmail.com
Scientific supervisor:
Nilufar Nabiyeva
https://doi.org/10.5281/zenodo.23898356

Abstract

Emerging economies increasingly depend on foreign technology for the layers of the digital economy that matter most: semiconductors, cloud infrastructure, software platforms and, most recently, artificial intelligence (AI) compute and models. This article asks whether such dependence is a distinct source of economic vulnerability and which policy options reduce it at acceptable cost. Using a structured narrative review of institutional reports and peer-reviewed studies, supplemented by three comparative cases (semiconductors, cloud services and AI), it assesses evidence across four channels: supply interruption, lock-in and rent extraction, jurisdictional exposure, and capability stagnation. The evidence indicates that dependence is most damaging where it is concentrated in few suppliers, hard to substitute and legally controlled abroad. It also shows that export controls tend to redirect supply chains rather than halt them, and that strict localisation can backfire on domestic firms. The findings point to a portfolio approach: procurement and contract reform, multi-vendor and open-standard architectures, pooled regional compute, and sustained investment in skills. The article concludes that the objective for emerging economies should be managed interdependence rather than technological autarky.

1. Introduction

Technology has become the main channel through which economies grow, trade and govern themselves. For most emerging economies, however, the technologies that carry this weight are designed, owned and controlled elsewhere. Chips are fabricated in a handful of locations, enterprise software and cloud services are supplied by a few multinational firms, and the most capable AI systems are trained on computing clusters concentrated in two countries. A mobile-money network, a tax portal or a hospital records system may therefore run on components that its own government can neither inspect nor easily replace.

This dependence is not new. Dependency theorists argued decades ago that peripheral economies were locked into positions set by the technological leaders. What is new is its scope and speed. Digital infrastructure is now embedded in public administration, finance and health, so a disruption in a foreign supply chain, a change in a vendor's pricing, or a decision by a foreign government can reach domestic economic activity within days. Recent shocks, from pandemic-era chip shortages to export controls on advanced semiconductors, have made this exposure visible to policymakers.

The debate remains polarised. One camp treats dependence as a vulnerability to be eliminated through "digital sovereignty" and import substitution. The other treats it as the ordinary price of access to global best practice and warns that self-sufficiency is unaffordable for small economies. Empirical evidence that could adjudicate between the two is scattered across trade economics, development studies, cloud policy and AI governance. However, little research has brought these strands together to ask which forms of

technological dependence create real economic vulnerability, and which policy responses have evidence behind them.

This article addresses that gap. It poses three research questions:

1. Through which channels does technological dependence translate into economic vulnerability in emerging economies?

2. What does the available evidence show about the size and persistence of these effects in semiconductors, cloud infrastructure and AI?

3. Which policy options reduce vulnerability at acceptable cost, and under what conditions?

The article hypothesises that vulnerability depends less on the amount of foreign technology used than on its concentration, substitutability and legal control. Its thesis is that emerging economies are best served by managing interdependence, through diversification, bargaining power and domestic absorptive capacity, rather than by pursuing technological autarky.

The paper proceeds as follows. Section 2 reviews the literature and identifies the gap. Section 3 explains the methodology. Section 4 presents the evidence, Section 5 interprets it and derives policy options, and Section 6 concludes.

2. Literature Review

The literature on technological dependence has developed in four overlapping strands. Read together, they explain why dependence matters but leave open how much, and for whom.

2.1 Structural dependency and the terms of trade

The earliest strand locates vulnerability in the structure of trade. Prebisch (1950) argued that economies specialised in primary commodities face deteriorating terms of trade against industrial exporters, while Hirschman (1945) showed how asymmetric trade relations hand bargaining power to the larger partner. Cardoso and Faletto (1979) extended the argument to technology, claiming that foreign control of productive know-how shapes domestic development paths. These works established the core intuition that dependence is a power relationship, not only a trade statistic. Their weakness is empirical: they offer little guidance on which dependencies are harmful, and the later rise of East Asian exporters showed that integration with foreign technology could coexist with rapid catch-up.

2.2 Technological capabilities and catch-up

The second strand explains that contrast. Lall (1992) argued that what matters is not access to technology but the domestic capability to select, absorb and improve it. Kim (1997) documented how Korean firms moved from assembling imported designs to innovating on them. The UNCTAD (2021) Technology and Innovation Report applies this logic to frontier technologies: its readiness index covers 158 countries and shows that a few developing economies, notably India, perform far above what their income suggests, while most lag. Notably, the top overperformers rank lower on ICT connectivity and skills, a pattern that holds for developing countries as a group. This strand shifts attention from whether a country imports technology to what it can do with it. However, it pays limited attention to the political and legal control that suppliers retain after the technology is imported.

2.3 Global value chains and weaponised interdependence

The third strand addresses that control. Gereffi, Humphrey and Sturgeon (2005) showed that lead firms govern value chains and capture most of the gains, which constrains upgrading by suppliers. Rodrik (2018) argued that new technologies reduce the scope for labour-intensive, export-led industrialisation, narrowing a path that earlier developers used. Farrell and Newman (2019) added a security dimension:

states that host network hubs can turn interdependence into leverage, either by surveilling flows or by cutting off access. Empirical work on export controls tests this claim. Studies of the Japan–Korea dispute and of US controls on China suggest that restrictions often reroute supply rather than eliminate it (Bonnet et al., 2026; Makioka & Zhang, 2024), though costs can be large for specific products and firms (Kim & Cho, 2024). Most of this evidence concerns middle-income, capability-rich economies such as Korea and China, and it is less clear that it transfers to smaller, less capable economies.

2.4 Digital sovereignty, cloud and AI

The fourth and newest strand concerns digital infrastructure. The World Bank's work on cloud markets finds that these markets are largely located in high-income countries and that economies with limited access to affordable services will lag in harnessing machine learning and AI (Gelvanovska-Garcia et al., 2024). Its guidance for policymakers distinguishes a "resilience through hyperscale" model from a "digital sovereignty" model based on local control (World Bank, 2024). In AI, analysts describe a "compute divide", with a few countries hosting most specialised infrastructure, and warn of a new dependency in which strategic AI capabilities run on foreign clouds under foreign terms (Stimson Center, 2026). Much of this literature comes from policy institutes and reports rather than peer-reviewed studies. Its claims are plausible but often rest on figures that differ by source and definition.

2.5 The gap

Taken together, the strands agree that dependence is consequential but disagree on mechanisms and remedies. Structural theories stress power, capability theories stress absorption, and the export-control literature stresses substitution. Few studies compare the channels of vulnerability across several technology layers, and fewer still link them to policy options that small and middle-income economies can afford. This article contributes such a synthesis.

3. Methodology

3.1 Research design

The study is a qualitative, structured narrative review with a comparative case design. It does not collect primary data. Instead it synthesises published evidence on three technology layers, which serve as comparative cases: semiconductors (hardware), cloud and data infrastructure (platforms) and AI compute and models (the emerging layer). The cases were chosen because they differ in how easily a country can substitute away from foreign suppliers, which allows the hypothesis on concentration, substitutability and legal control to be examined.

3.2 Analytical framework

Vulnerability is analysed through four channels derived from the literature in Section 2:

1. **Supply interruption:** a supplier or government cuts or delays access to a critical input.
2. **Lock-in and rent extraction:** switching costs allow suppliers to raise prices or restrict flexibility.
3. **Jurisdictional exposure:** foreign law or foreign government action can reach domestic data and systems.
4. **Capability stagnation:** reliance on imported solutions weakens the domestic skills and firms needed to adapt technology.

3.3 Sources and sampling

Sources were identified through targeted web searches in October 2026 using terms related to technology dependence, export controls, cloud and data infrastructure, and AI compute in developing

countries. Purposive sampling favoured, in order of priority: peer-reviewed and working-paper studies, reports by multilateral institutions (UNCTAD, World Bank), reports by research institutes, and, only for recent developments, quality news coverage. The core evidence base comprises 12 sources, listed in the references. Classic theoretical works (Section 2) are cited from the established literature and were not re-verified for this article.

3.4 Data analysis

Each source was coded against the four channels, the technology layer, the type of evidence (causal estimate, descriptive statistic or expert judgement) and the income level of the economies studied. Findings were then compared across layers using thematic synthesis. Where sources reported different figures for the same phenomenon, both are reported and the difference is noted rather than reconciled.

3.5 Ethical considerations

The study uses only published material and involves no human participants, so institutional review board approval and informed consent were not required. All sources are attributed, and direct quotation is avoided in favour of paraphrase.

4. Results

This section reports what the sources show, layer by layer, without interpretation. Table 1 summarises the pattern; the subsections give the detail.

Table 1. Evidence by technology layer

Layer	Concentration of supply	Strongest evidence on channels	Type of evidence
Semiconductors	One Taiwanese firm makes over 90% of the most advanced chips (Stimson Center, 2026)	Supply interruption; rerouting of supply	Causal trade studies
Cloud and data infrastructure	Cloud markets largely located in high-income countries (Gelvanovska-Garcia et al., 2024)	Lock-in; jurisdictional exposure	Institutional reports
AI compute and models	US and China host 86% of data-centre capacity (Stimson Center, 2026)	Capability stagnation; lock-in; jurisdictional exposure	Think-tank reports, expert judgement

4.1 Semiconductors

Five studies examine export controls on chips. Makioka and Zhang (2024) studied Japan's 2019 restrictions on three chemical inputs to South Korea. Exports of one input, hydrogen fluoride, fell sharply, but exports of the other two did not. Japanese hydrogen fluoride exports to the United States rose, so Japanese production of semiconductor-related goods did not fall. South Korea shifted sourcing to Belgium, the United States and Taiwan, and domestic production by Korean firms and Japanese affiliates in Korea increased.

Bonnet et al. (2026) examine unilateral US controls on chip exports to China. US chip exports declined significantly, while exports of manufacturing equipment from the EU, Japan and Singapore increased significantly. The authors conclude that the controls redirected supply chains. Kim and Cho (2024) report a 14% fall in South Korean semiconductor exports after US controls on China, concentrated in advanced and memory products. Chen and Sun (2024) find that the controls reduced China's own supply chain vulnerability in controlled manufacturing products and stimulated independent innovation, with

limited damage to industry development. Crosignani et al. (2024) study how supply chains reconfigure after controls, but their abstract reports no headline estimate.

4.2 Cloud and data infrastructure

The World Bank and IFC report that cloud and data infrastructure markets are largely located in high-income countries, and that countries with limited access to affordable services will lag in using machine learning and AI at scale (Gelvanovska-Garcia et al., 2024). The World Bank's guide for developing-country policymakers describes two adoption models: "resilience through hyperscale", and "digital sovereignty" through private or community clouds that reduce exposure to foreign jurisdictional conflicts (World Bank, 2024, as summarised by Devdiscourse).

For Africa, press coverage of World Bank warnings reports that heavy reliance on imported proprietary software risks ceding control of digital systems to foreign vendors, that vendor lock-in limits flexibility, and that institutions turn to open-source alternatives mainly when proprietary platforms become too expensive or rigid (Njaaga, 2026). The same report cites an estimate of US$62–79 billion needed to build the foundations of a continent-wide digital economy.

4.3 AI compute and models

The Stimson Center (2026) reports that the US and China host 86% of global data-centre capacity, that 150 countries lack AI infrastructure, and that only 32 nations have data centres capable of AI computing. It also reports US private AI investment of US$109.1 billion in 2024 against US$9.3 billion for China, with Africa receiving under 1% of global funding. ORF Middle East (2026) finds that capital-intensive layers (frontier research, compute and investment) are increasingly concentrated, while deployment is the least concentrated layer and the one where the Global South's weight is visible. It cites India's IndiaAI Mission (US$1.25 billion over five years, approved in 2024) and US$803 million in cumulative African AI startup funding since 2019, and calls the capital gap structural.

Interview-based research by New America (2026) finds that most Global South organisations do not train frontier models but fine-tune open-source models or run inference on models built elsewhere. It documents organisations legally barred from foreign cloud providers yet lacking local compute, and reports that data-localisation laws can disadvantage domestic start-ups because larger, often foreign, firms are better placed to run local facilities. It also reports that proprietary models trained mainly on English-language and Global North data fit local contexts poorly. Under IndiaAI, more than 38,000 GPUs have been made available to nonprofits and start-ups at subsidised rates, and public-compute initiatives exist in Morocco, Brazil and Senegal.

4.4 Capability and readiness

UNCTAD (2021) scores 158 countries on frontier-technology readiness using ICT deployment, skills, R&D, industry activity and access to finance. India's actual rank was 43 against 108 predicted from income, an overperformance of 65 places. The five top developing-country overperformers rank lower on ICT connectivity and skills, as do developing countries as a group. The report finds that innovation systems in most developing countries are weak and prone to systemic failures.

5. Discussion

5.1 Interpretation

The evidence supports the hypothesis in part. Technological dependence creates economic vulnerability through all four channels, but its severity varies by layer. In semiconductors, the dominant

finding is that supply interruptions are real yet often temporary: sourcing shifted and production adjusted after the Japan–Korea and US–China restrictions (Makioka & Zhang, 2024; Bonnet et al., 2026). The harm was greatest where substitutes were scarce, as with hydrogen fluoride, the one restricted input whose exports to Korea fell sharply, and with advanced and memory products (Kim & Cho, 2024). Substitutability, not the mere presence of imports, therefore determines exposure.

In cloud and AI, the evidence points to a different mix of channels. Here the main risks are lock-in, jurisdictional exposure and capability stagnation rather than sudden shortage. These risks are slower and harder to see, which may explain why they are argued mostly in policy reports. The question of whether such reports overstate the problem remains open, because few causal estimates exist for these layers.

The New America findings show that a naive sovereignty response can worsen the problem. Rules that bar foreign cloud use without building local compute leave organisations stranded, and localisation can favour large foreign operators over domestic start-ups. Vulnerability is therefore shaped as much by policy design as by the technology itself.

5.2 Comparison with the literature

The findings are consistent with capability theory (Lall, 1992; UNCTAD, 2021): the economies studied most closely, Korea and China, both had strong domestic industrial bases and adjusted to restrictions. They complicate the older dependency argument, since integration with foreign technology did not by itself entrench subordination. They also qualify the weaponised-interdependence thesis (Farrell & Newman, 2019): leverage exists, but controls can stimulate substitution and benefit third-country suppliers (Bonnet et al., 2026; Chen & Sun, 2024). The AI findings echo the value-chain literature, since the capital-intensive layers are concentrated while deployment is dispersed (ORF Middle East, 2026), a pattern in which the lead firms capture most of the gains (Gereffi et al., 2005).

5.3 Policy options

The synthesis suggests five options, ordered from low cost to high cost.

1. **Reform procurement and contracts.** Governments are large buyers of digital services. Standard clauses on data portability, exit rights, audit access and jurisdiction can reduce lock-in without building new infrastructure. Shared clauses across several countries would strengthen bargaining power.
2. **Design for substitutability.** Prefer open standards, open-source components and multi-vendor architectures for critical public systems, so that no single supplier or jurisdiction controls them (Njaaga, 2026).
3. **Match sovereignty to the risk.** Reserve local or community cloud for the most sensitive workloads, and use hyperscale providers elsewhere, rather than imposing blanket localisation (World Bank, 2024).
4. **Pool compute regionally.** Public or shared GPU capacity for fine-tuning and inference, as in India, Morocco, Brazil and Senegal, fits the way most organisations actually use AI better than attempts at frontier training.
5. **Invest in absorptive capacity.** Skills, connectivity, R&D financing and innovation-system reform address capability stagnation directly and make every other option work (UNCTAD, 2021).

For smaller economies, the combination of options 1 to 3 is the most affordable starting point. Options 4 and 5 need regional cooperation and sustained finance.

5.4 Limitations

The study relies on published secondary evidence and does not generate new data. Evidence on cloud and AI is thinner and less causal than on semiconductors, and part of it comes from policy institutes and

press summaries of reports rather than from peer review. Some figures differ across sources and are not harmonised. The strongest causal studies concern capability-rich economies such as Korea and China, which limits generalisation to low-income countries. The review used a purposive rather than systematic search, so relevant studies may have been missed. The policy options are inferred from the evidence and have not been tested.

5.5 Avenues for future research

Future work should estimate the economic cost of lock-in and cloud outages using firm-level or public-sector data, test whether localisation rules affect start-up entry, compare procurement reforms across countries, and track how AI compute pooling performs against its stated goals.

6. Conclusion

This article set out to establish when technological dependence becomes economic vulnerability and what emerging economies can do about it. The evidence shows that dependence is not uniformly harmful. It becomes dangerous where supply is concentrated, substitutes are scarce and foreign actors hold legal or commercial control, conditions that are increasingly met in cloud infrastructure and AI compute. Where substitutes exist, as in much of the semiconductor trade, restrictions have tended to redirect supply chains rather than break them.

These findings support the thesis that managed interdependence serves emerging economies better than autarky. Self-sufficiency is unaffordable for most, and blanket sovereignty rules can harm the domestic firms they aim to protect. The more promising path combines better contracts, substitutable architectures, risk-matched localisation, pooled regional compute and sustained investment in the skills and institutions that let a country use foreign technology on its own terms. The article thus addresses the gap identified at the outset: a comparison of vulnerability channels across technology layers, tied to affordable policy choices.

The broader lesson is that the question for policymakers is not whether to depend on foreign technology, but on whom, for what, and with what exit. Economies that can answer those three questions for their critical systems will bear the risks of a fragmenting technology order far better than those that cannot.

References

1. Bonnet, P., Ciani, A., & Zaurino, E. (2026). Throwing sand on the chips: The unintended effects of U.S. export controls on the semiconductor supply chain. European Commission, Joint Research Centre. https://publications.jrc.ec.europa.eu/repository/handle/JRC147129
2. Cardoso, F. H., & Faletto, E. (1979). Dependency and development in Latin America. University of California Press.
3. Chen, W., & Sun, Y. (2024). Export controls, innovation, and the development of the semiconductor industry. EconPapers. https://econpapers.repec.org/RePEc:spr:advbcp:978-94-6463-408-2_19
4. Crosignani, M., Han, L., Macchiavelli, M., & Silva, A. (2024, April 12). The anatomy of export controls. Liberty Street Economics, Federal Reserve Bank of New York. https://econpapers.repec.org/paper/fipfednls/98060.htm
5. Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42–79.

6. Gelvanovska-Garcia, N., Mačiulė, V., & Rossotto, C. M. (2024). Advancing cloud and data infrastructure markets: Strategic directions for low- and middle-income countries. World Bank. https://doi.org/10.1596/978-1-4648-2065-6
7. Gereffi, G., Humphrey, J., & Sturgeon, T. (2005). The governance of global value chains. Review of International Political Economy, 12(1), 78–104.
8. Hirschman, A. O. (1945). National power and the structure of foreign trade. University of California Press.
9. Kim, H., & Cho, J. (2024). The impact of US export controls on Korean semiconductor exports. KDI Journal of Economic Policy, 46(3), 1–23. https://dx.doi.org/10.23895/kdijep.2024.46.3.1
10. Kim, L. (1997). Imitation to innovation: The dynamics of Korea's technological learning. Harvard Business School Press.
11. Lall, S. (1992). Technological capabilities and industrialization. World Development, 20(2), 165–186.
12. Makioka, R., & Zhang, H. (2024). The impact of export controls on international trade: Evidence from the Japan–Korea trade dispute in the semiconductor industry. Journal of the Japanese and International Economies, 74, Article 101336. https://www.sciencedirect.com/science/article/pii/S0889158324000327
13. New America. (2026). Technical barriers and solutions. In Closing the adoption gap. https://www.newamerica.org/insights/closing-the-adoption-gap/technical-barriers-and-solutions/
14. Njaaga, D. (2026, April 28). World Bank: Why Africa does not own its digital future. The Standard (Kenya). https://www.standardmedia.co.ke/business/amp/sci-tech/article/2001546530/world-bank-why-africa-does-not-own-its-digital-future
15. ORF Middle East. (2026). Global AI: A story of fragmentation. https://orfme.org/expert-speak/global-ai-a-story-of-fragmentation/
16. Prebisch, R. (1950). The economic development of Latin America and its principal problems. United Nations.
17. Rodrik, D. (2018). New technologies, global value chains, and developing economies (NBER Working Paper No. 25164). National Bureau of Economic Research.
18. Stimson Center. (2026). Technology, talent, and trust: Three pillars for AI that serve the Global South. https://www.stimson.org/2026/technology-talent-and-trust-three-pillars-for-ai-that-serve-the-global-south/
19. UNCTAD. (2021). Technology and innovation report 2021: Catching technological waves—Innovation with equity. United Nations Conference on Trade and Development. https://unctad.org/news/few-developing-countries-overperform-frontier-technologies-most-lag-behind
20. World Bank. (2024). Unpacking cloud cybersecurity: A guide for policymakers in developing countries. Summarised in Devdiscourse. https://www.devdiscourse.com/article/technology/3205123-from-vulnerabilities-to-vitality-cloud-cybersecurity-in-developing-nations