International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(23s) 2026 pp. 1394-1406
https://doi.org/10.70917/ijcisim-2026-5701
Article

Technology Decoupling and Strategic Tech: The National Security Implications of Restricting Chinese Digital Infrastructure and FDI in India

Dr. Vikram Mani Tiwari

Assistant Professor (Political Science), Department of Lifelong Learning and Extension, Chhatrapati Shahu Ji Maharaj University, Kanpur, India
vikrammanitiwari@csjmu.ac.in

Abstract: India's restrictions on Chinese digital infrastructure and foreign direct investment (FDI) represent a shift from a predominantly market-access logic toward a national-security logic in technology policy. This paper argues that the strategic issue is not whether Chinese technology is "safe" or "unsafe" in the abstract, but whether dependence is concentrated in parts of the digital stack were ownership, software control, privileged network access, standards, financing or supply-chain disruption could create coercive leverage. India's 2020 Press Note 3 moved Chinese-linked investment from the automatic route to government approval, while the telecommunications sector subsequently developed a trusted-source regime, critical-telecommunication-infrastructure rules and stronger cyber-security obligations. At the same time, India continues to depend on globalized supply chains for electronics, semiconductors, components and digital hardware, which means that blanket decoupling can raise costs without eliminating strategic exposure. Using the concept of weaponized interdependence and a layered digital-infrastructure framework, the paper examines FDI restrictions, telecom vendor controls, critical-infrastructure rules and their economic trade-offs. It finds that targeted restriction is strategically superior to indiscriminate decoupling: India should secure core networks, critical cloud and data infrastructure, sensitive procurement chains and ownership/control rights while preserving competitive access to non-critical technologies. The paper concludes that resilient "de-risking" requires diversification, domestic capability, security-by-design and auditable supply chains rather than a binary Chinese-versus-non-Chinese technology policy.
Keywords: India–China technology competition; digital infrastructure; foreign direct investment; national security; telecom security; de-risking; decoupling; strategic technology

1. Introduction

Digital infrastructure has become a form of national power because communications networks, cloud platforms, data centres, software dependencies and hardware supply chains underpin finance, transport, public administration, defence and economic production. India's security policy therefore increasingly treats the digital sector as critical infrastructure rather than a conventional commercial domain. The Department of Telecommunications now explicitly identifies the telecom sector as critical information infrastructure and points to the cascading effects that disruption could have across the economy and national security [3,4].

Against this background, India's restrictions on Chinese technology and investment should be understood as an attempt to manage network dependence. The policy challenge is difficult because the same Chinese firms that may create security concerns can also offer scale, low-cost components, manufacturing know-how, venture capital and rapid deployment. A security regime that eliminates one vendor while leaving downstream dependencies untouched may simply relocate risk rather than reduce it.

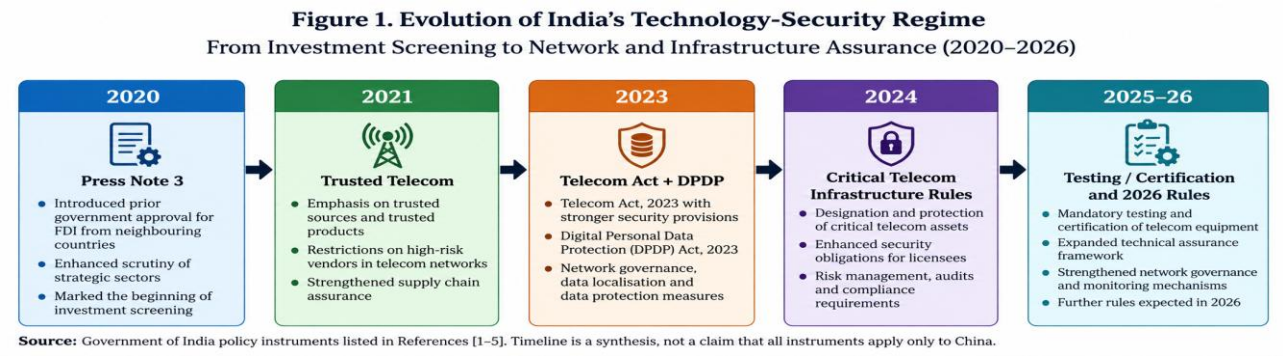

Figure 1. Evolution of India's technology-security policy, 2020–2026.

Source: Author's synthesis from Government of India policy instruments [1–5].

2. Research Questions and Method

The paper asks three questions: (1) what national-security risks arise when foreign firms from a strategic competitor occupy critical points in India's digital infrastructure; (2) how have India's FDI and telecom-security measures altered those risks; and (3) what economic and technological trade-offs follow from restricting Chinese participation?

The study uses qualitative policy analysis and structured comparison. Primary evidence comes from Indian government regulations, official FDI statistics and telecommunications policy documents; secondary evidence comes from peer-reviewed research on Chinese digital expansion, technology decoupling and network power. The analytical framework separates four layers—physical infrastructure, data, control/standards and capital—to avoid treating "technology" as a single category. This layered approach allows the study to distinguish a Chinese-branded smartphone from a foreign-controlled telecom core network or a strategically sensitive cloud platform.

Table 1. Four-layer model of strategic technology dependence.

Layer	**Examples**	**Security concern**	**Preferred policy response**
Physical	RAN, routers, fiber, data-centre hardware	Supply-chain compromise; remote maintenance exposure	Trusted sourcing, certification, redundancy
Data	Cloud, platforms, data storage	Unauthorized access; cross-border transfer risk	Data governance, access controls, auditability
Control	Standards, software, firmware, network management	Hidden dependencies; vendor lock-in	Security-by-design, source review, update controls
Capital	FDI, venture funding, acquisitions	Ownership influence; access to sensitive firms	Risk-based FDI screening and beneficial-owner review

Source: Author's analytical framework based on Farrell and Newman (2019), Buzan et al. (1998), India's telecom-security framework, and literature on digital infrastructure governance. See References [3], [10], [11], [17].

3. Literature Review: From Interdependence to Technology Security

Farrell and Newman's concept of "weaponized interdependence" is central to understanding why infrastructure dependence can become geopolitical power. Their argument is that globally connected networks create chokepoints

through which information, transactions and supply chains flow. Actors that control or regulate such nodes can obtain information or deny access, thereby converting economic connectivity into strategic leverage [10].

Recent research extends this logic to digital infrastructure. Scholarship on China's digital expansion identifies a broad "technology stack" spanning telecommunications networks, undersea and terrestrial links, devices, cloud and data infrastructure, platforms and smart-city systems [11]. This matters because security risk can be cross-layer: a company may enter a market through relatively benign hardware and gradually become embedded in standards, financing, data services and maintenance relationships.

Shrivastava's analysis of India's ICT sector is particularly relevant because it finds that Chinese strategic footprints extend across e-commerce, consumer electronics, semiconductors and telecom, and therefore cannot be evaluated through telecom policy alone [9]. Other scholarship on cross-border data governance shows why national security concerns increasingly intersect with data localization and state access regimes [12]. The theoretical implication is that technology restriction is effective only when it addresses the architecture of dependence, not merely the nationality of the visible supplier.

4. India's FDI Screening Regime and the Chinese Investment Question

India's April 2020 Press Note No. 3 moved investment by entities incorporated in countries sharing a land border with India, or with beneficial owners located in such countries, from the automatic route to the government-approval route [1,2]. The measure was introduced during the COVID-19 period and formally framed around preventing opportunistic acquisitions, but in practice it became an important national-security gateway for Chinese capital.

The policy should not be interpreted as a prohibition on Chinese capital. It is an ex ante screening mechanism that shifts the burden from automatic market entry to governmental review. The distinction matters for strategic policy because it preserves the possibility of investment where the state judges the risks acceptable, while allowing review of ownership, sensitive-sector exposure and control rights.

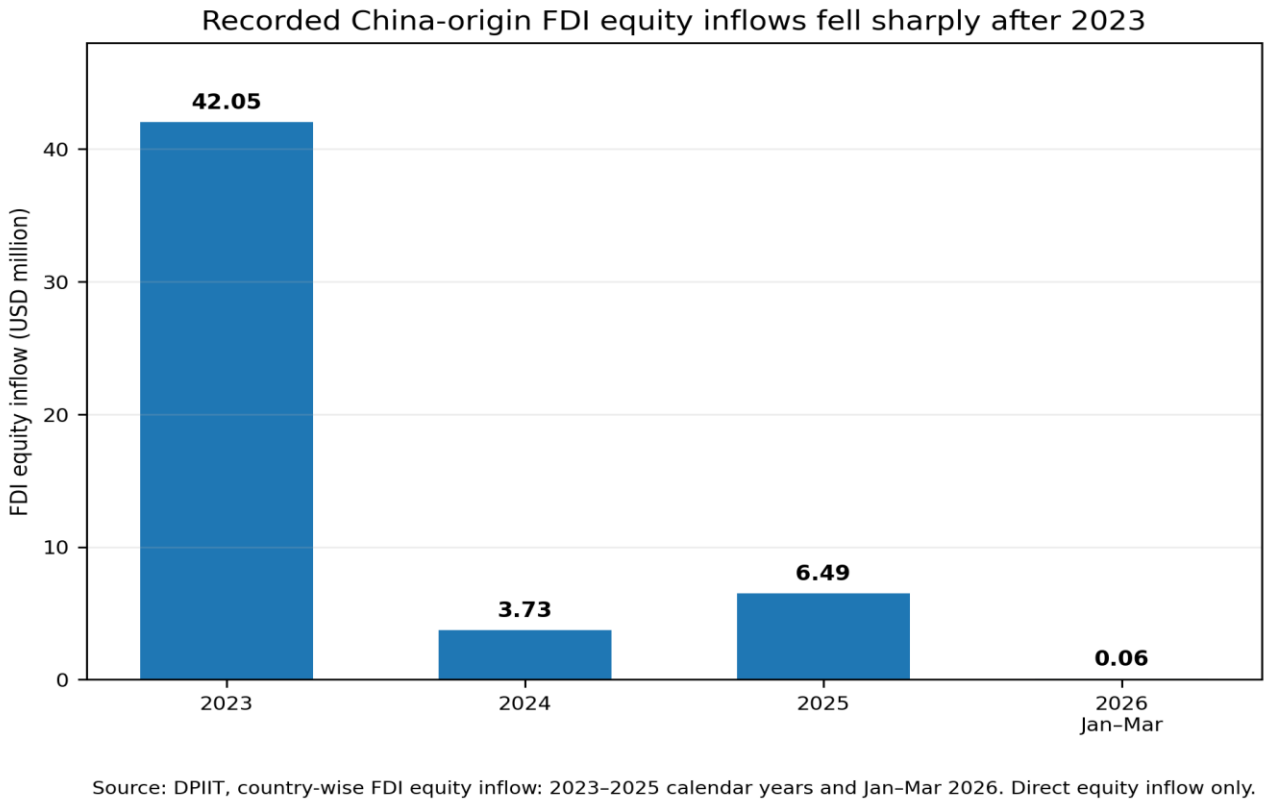

Figure 2. Recorded China-origin FDI equity inflows fell sharply after 2023 and remained near zero in Q1 2026.

Source: DPIIT country-wise FDI equity inflow statistics for calendar years 2023–2025 and January–March 2026 [8,22,23].

Table 2. Recorded China-origin FDI equity inflows into India, 2023–2026.

Year	**China-origin FDI equity inflow (USD million)**	**Interpretation**
2023	42.05	Post-2020 screening environment; inflow remains modest
2024	3.73	Sharp contraction in recorded equity inflow
2025	6.49	Still very low in absolute terms
2026 (Jan–Mar)	0.06	Near-zero first-quarter recorded inflow

Source: Department for Promotion of Industry and Internal Trade (DPIIT), country-wise FDI equity inflow statements. Values are USD million and refer to recorded equity inflows; they do not measure indirect ownership or Chinese content embedded in third-country investment. See References [8], [21], [22].

The data should be interpreted carefully. Country-wise FDI statistics capture recorded equity inflows by the relevant classification and do not exhaust all forms of Chinese capital exposure. Indirect ownership through third countries, venture structures, licensing, commercial credit, imports and supply-chain dependence may generate strategic exposure without appearing as direct China-origin FDI. That limitation is itself a security finding: ownership screening and supply-chain screening are different policy problems.

The updated DPIIT series also shows that China-origin recorded equity inflows remained extremely small in January–March 2026, at about USD 0.06 million, while total Indian FDI equity inflows in the same quarter were far larger. This gap suggests that the principal national-security challenge has shifted from direct Chinese ownership toward embedded dependencies in products, components, software and supply chains. Restricting capital can reduce ownership risk, but it cannot by itself remove technology risk [21,22].

5. Telecom Security: From Vendor Access to Trusted Networks

Telecommunications represent the clearest example of technology being treated as strategic infrastructure. India's National Security Directive on Telecom Sector created a trusted-source and trusted-product framework, and the Department of Telecommunications states that, from June 2021, service providers were required to connect only trusted products for new equipment under the framework [3]. The objective was not simply to exclude a single country but to improve supply-chain integrity and reduce the attack surface of the communications backbone.

The policy became especially consequential for Chinese equipment suppliers because Huawei and ZTE had established positions in telecom hardware markets globally. Importantly, the Indian framework was designed as a source/product assessment mechanism rather than a public blanket ban in its formal language. That distinction enables the government to securitize procurement through technical and institutional screening rather than nationality alone, even though the strategic environment makes Chinese vendors particularly salient [3,14].

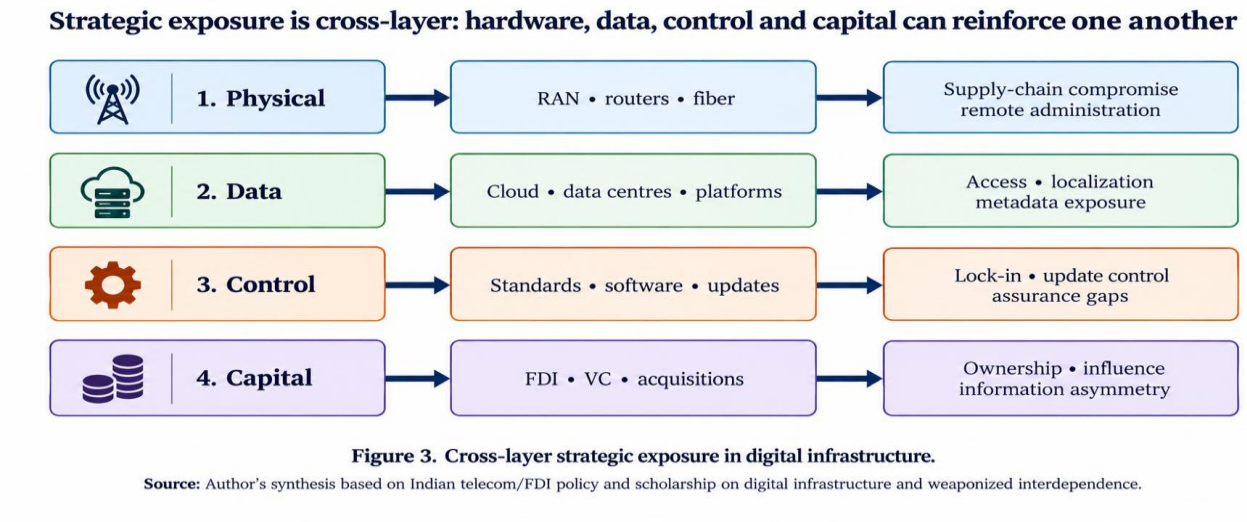

Figure 3. Digital-security risks emerge across interacting infrastructure layers.

Source: Author's synthesis based on India's telecom-security framework and literature on Chinese digital infrastructure [3,9,11].

Table 3. Major technology-security instruments relevant to Chinese-linked dependence.

Policy instrument	Primary target	Security rationale	Possible downside
Press Note 3 (2020)	Chinese-linked FDI	Ownership and control risk	Slower capital entry; screening uncertainty
Trusted telecom framework	Network equipment sources/products	Supply-chain and cyber risk	Potential vendor concentration / higher costs
Critical Telecom Infrastructure Rules	Critical network operators/assets	Resilience and national-security continuity	Compliance burden for operators

Telecom cyber-security rules	Operational security	Incident response and security governance	Higher fixed compliance costs
MTCTE / conformity assessment	Equipment market access	Baseline technical assurance	Can disadvantage smaller suppliers if compliance is costly

Source: Government of India, DPIIT Press Note 3 (2020), Department of Telecommunications rules and trusted-source framework, and related conformity/cyber-security instruments. See References [1]–[5], [15], [23], [24], [26], [27].

The policy architecture continued to evolve in 2025–26. The Department of Telecommunications lists the 2025 mandatory testing and certification rules and, in 2026, new telecommunications network rules. The direction of travel is significant: national-security controls are becoming institutionalized as technical assurance, certification, network authorization and operational-security requirements rather than remaining a one-off geopolitical response [24,25]. This creates a more durable regulatory model but also makes transparency, due process and periodic review increasingly important.

6. Why Blanket Decoupling Is Strategically Incomplete

The case for restricting high-risk Chinese participation is strongest where three conditions overlap: the infrastructure is difficult to replace after deployment; the vendor can obtain privileged technical access; and disruption would produce system-wide economic or security effects. Telecom core networks, sensitive government systems, selected cloud infrastructure and certain semiconductor or industrial-control supply chains can meet these conditions. By contrast, low-risk consumer products are generally more substitutable and less capable of generating systemic coercive leverage on their own.

A blanket decoupling strategy can also create a second-order vulnerability: supplier concentration among a smaller set of alternative foreign vendors. If Nokia, Ericsson, a U.S. cloud provider or another supplier becomes a de facto monopoly, India may trade one dependency for another. The security objective should therefore be diversity plus controllability, not merely exclusion.

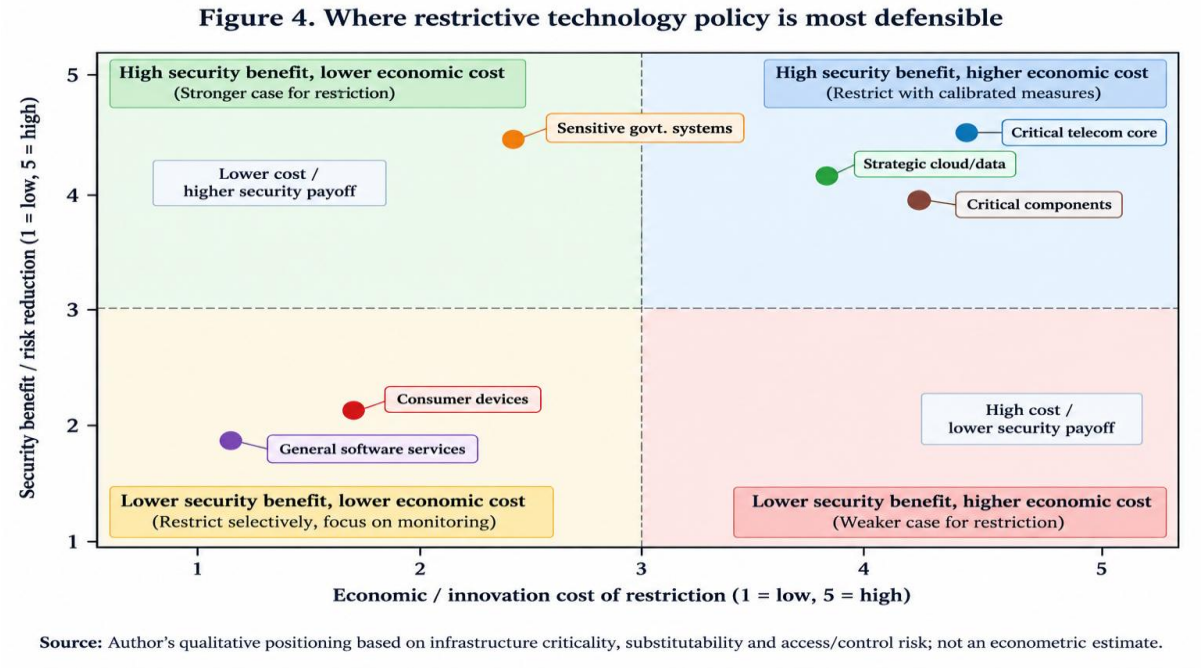

Figure 4. Restrictive technology policy produces simultaneous security gains and economic/innovation costs.

Source: Author's analytical synthesis of policy and literature evidence; scores are not econometric estimates.

The Economic Survey has highlighted the importance of foreign investment for building manufacturing ecosystems and integrating India into global value chains, while also recognizing that the composition and strategic identity of investors matter [6,7]. This creates a central policy tension: India needs capital, technology transfer and global production networks at the same time that it wants to reduce strategic dependency. The appropriate response is therefore selective screening, not indiscriminate disengagement.

7. Security Implications of Chinese Digital Infrastructure

Confidentiality risk. Foreign-controlled network equipment or cloud services can create privileged technical access to metadata, network traffic or operational systems. The risk is greatest where the vendor also provides maintenance, software updates or orchestration tools.

Integrity risk. The more complex the software stack, the more difficult it is to verify that code and firmware behave exactly as expected. Supply-chain compromise can therefore be more consequential than traditional physical sabotage.

Availability risk. Dependence on a small number of suppliers creates a continuity problem if sanctions, geopolitical escalation, export controls or supplier refusal interrupt equipment replacement or software updates.

Information asymmetry. Governments and operators often lack the engineering transparency necessary to independently verify every component. Trusted-product regimes reduce this asymmetry by centralizing assurance, testing and procurement controls.

Coercion and bargaining power. A foreign firm embedded in critical systems can become a node of leverage even without actively exploiting a vulnerability. The mere possibility of dependency can affect policy choices during crisis. This is the core logic of weaponized interdependence [10].

8. Economic and Innovation Effects of Restriction

Technology restrictions have real opportunity costs. Chinese firms can contribute low-cost manufacturing, supplier networks and engineering expertise, particularly in electronics and hardware-intensive industries. The 2024 Economic Survey explicitly noted the potential for Chinese FDI to support supply-chain participation and exports, while the 2026 Economic Survey emphasizes the importance of attracting multinational production networks as anchors for exports, skills and industrial ecosystems [6,7].

At the same time, the experience of technology restrictions in other jurisdictions shows that security controls can create incentives for local substitution and new market entry. The relevant question is therefore not whether restrictions "hurt" the economy—some costs are unavoidable—but whether the security benefit exceeds the resulting cost and whether policy generates durable domestic capability instead of temporary protection.

India's trade data illustrate why strategic technology policy cannot be reduced to FDI. The 2025–26 Economic Survey reports that electronic-goods imports rose by 17.1 percent year-on-year during April–December 2025, while machinery and electrical imports rose 14.2 percent. At the same time, electronics exports grew strongly. This combination is evidence of increasing domestic production within globally sourced value chains: import substitution is real, but so is continued dependence on imported intermediates. A technology policy that blocks one supplier without building interoperable alternative sources may therefore reduce one form of vulnerability while preserving another [26].

Table 4. Security–economy trade-offs associated with selective technology restrictions.

Trade-off	Security benefit	Economic cost	Policy design to improve balance
Restrict Chinese telecom core gear	High	Potentially higher equipment / transition costs	Focus restrictions on critical layers; allow audited non-critical components
Tighten Chinese-linked FDI	Higher ownership screening	May reduce capital / expertise in selected sectors	Use risk-based thresholds and transparent approval criteria
Promote domestic telecom equipment	Supply-chain resilience	Scale-up costs and learning curve	Use procurement + standards + export support
Diversify cloud/data infrastructure	Reduces single-vendor exposure	Duplication and higher capex	Interoperability and portable architectures
Mandate security audits	Improves assurance	Recurring compliance costs	Risk-tier audits according to criticality

Source: Author's synthesis of the policy instruments and empirical literature cited in References [9]–[20], [25]–[28].

8.1 Measuring Strategic Technology Exposure

The key analytical weakness in broad 'decoupling' narratives is that they often treat all technology dependence as equivalent. A more useful approach is to distinguish between ordinary commercial substitutability and strategic dependence. A low-cost consumer device supplied by a globally diversified market is not equivalent to a core telecom component that can constrain a national network's update cycle, telemetry, authentication, or maintenance. Strategic exposure rises when four conditions coincide: high criticality, low substitutability, high concentration, and meaningful external control over software, data or maintenance pathways.

This distinction matters for China-linked investment because ownership is only one possible channel of leverage. An entity may create strategic dependence through market concentration, vendor lock-in, intellectual property control, software update authority, financing relationships, or privileged access to operational data even when the direct equity stake is small. Conversely, a Chinese-linked firm operating under Indian certification, data-localisation, audit and procurement controls may present a different risk profile from an uncontrolled supplier embedded in a critical network. Policy therefore needs to assess the architecture of dependence rather than use nationality as a proxy for risk.

India's post-2020 experience also shows that industrial policy can partially offset the trade-offs created by security restrictions. Government data indicate large gains in domestic electronics production and mobile-phone exports, while domestic value addition remains materially lower than the headline production numbers. The strategic lesson is that assembly scale is an important resilience milestone, but it should not be mistaken for full supply-chain autonomy. Components, capital equipment, advanced semiconductors, network software and specialised manufacturing inputs remain relevant bottlenecks.

8.2 Strategic Exposure Matrix for Chinese-Linked Technology

Table 5. Strategic exposure matrix for Chinese-linked technology dependencies.

Technology layer	**Criticality**	**Replaceability**	**Main control point**	**Recommended posture**
Core telecom / network control	Very high	Low–moderate	Software, firmware, remote maintenance, network management	Strongest sourcing and audit controls; trusted products; restricted remote access
Critical cloud / data infrastructure	Very high	Moderate	Data access, admin privileges, concentration, jurisdiction	Diversification, portability, local governance, continuous assurance
Enterprise hardware / edge devices	Moderate–high	High	Supply chain, update mechanisms, telemetry	Security certification and supplier diversity rather than blanket exclusion
Consumer platforms / apps	Variable	High–very high	Data collection, algorithmic control, platform dependency	Targeted restrictions where evidence of harm or strategic leverage exists
Strategic semiconductor equipment / components	Very high	Low	Export controls, manufacturing bottlenecks, IP and tooling	Domestic capability, multiple foreign suppliers, strategic stockpiles where justified
Technology-company FDI	Variable	Variable	Beneficial ownership, board control, access to sensitive assets	Case-by-case government screening tied to criticality and control rights

Source: Author's analytical matrix based on Farrell and Newman (2019), Shrivastava (2024), India's telecom-security rules, CERT-In software/hardware bill-of-materials guidance, and DPIIT FDI policy. Ratings are qualitative and designed for comparative policy analysis, not statistical risk probabilities. See References [1], [3], [9], [10], [16], [23], [25]–[28].

9. Policy Model: From Decoupling to Managed Strategic Dependence

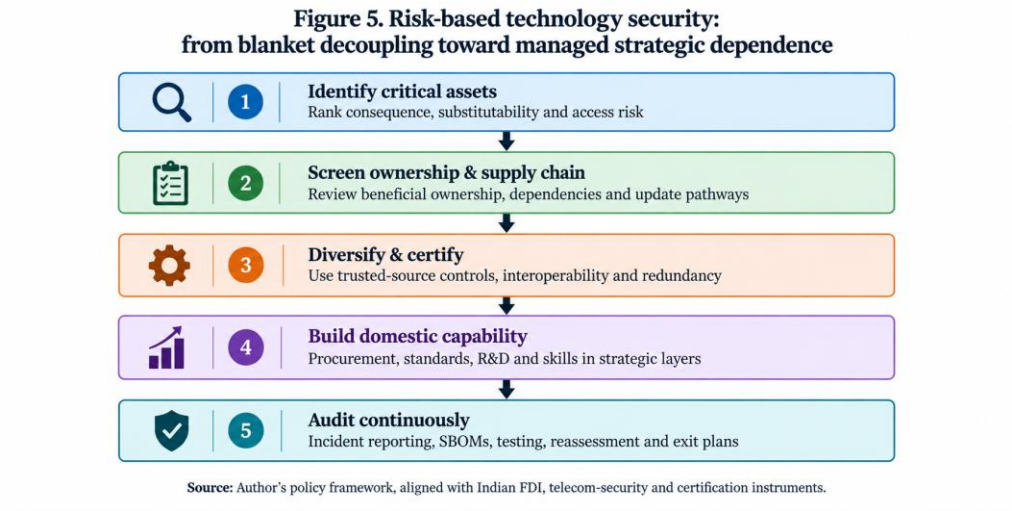

Figure 5. A risk-based policy model prioritizes targeted controls and resilience over blanket decoupling.

Source: Author's qualitative policy framework.

The evidence supports a four-part policy model. First, India should protect critical layers through targeted exclusion or stringent certification where the consequence of compromise is systemic. Second, it should diversify suppliers and maintain interoperability so that no foreign actor becomes indispensable. Third, domestic industrial policy should focus on capabilities that are genuinely strategic—telecom equipment, semiconductors, secure cloud infrastructure, cybersecurity tooling and critical components—rather than attempting autarky across the entire technology economy. Fourth, security must be continuous: software bills of materials, firmware validation, incident reporting, red-team testing and supplier reassessment should continue after procurement [15].

Table 6. Recommended strategic posture by technology layer.

Strategic layer	Preferred Indian posture	Reason
Core telecom and CII	High assurance / controlled sourcing	Potential system-wide impact
Sensitive government and defence digital systems	Strongest restrictions and sovereign control	Direct national-security consequences
Cloud/data-centre services	Diversified, interoperable, auditable	Concentration risk can create systemic dependence
Consumer devices	Open competition with security certification	Greater substitutability; avoid unnecessary market concentration
FDI into technology firms	Risk-based government screening	Ownership matters most where control confers strategic access

Source: Author's policy framework derived from risk-based security principles, Indian telecom regulation, FDI screening practice, and the technology-dependence literature. See References [1], [3], [4], [9]–[13], [16], [17].

10. Discussion

The national-security question should therefore be reframed from "Should India decouple from China?" to "Where does Chinese-linked dependence create asymmetric and hard-to-replace strategic leverage?" This reframing is important because full decoupling is not technically or economically feasible in a deeply integrated global

technology system. India imports components, tools, machinery and intermediate goods through complex international supply chains, and Chinese-origin content may enter indirectly even when a final supplier is based elsewhere.

The practical implication is that provenance should be only one element of risk assessment. India should increasingly evaluate ownership, governance, data access, maintenance rights, software-update pathways, supply concentration, substitutability and geopolitical jurisdiction. Such an approach is more defensible in international economic policy because it can be justified by infrastructure criticality and risk rather than by generalized nationality-based exclusion.

The strategy also has a geopolitical dimension. Technology controls can become part of a wider signaling contest with China, but excessive securitization can reduce the room for economic engagement and increase incentives for reciprocal restrictions. Managed interdependence therefore supports both resilience and diplomatic flexibility: India can retain market relationships while preventing strategic vulnerabilities from becoming structurally embedded.

10.1 Policy Sequencing for 2026–2030

Table 7. Policy sequencing for 2026–2030: assurance, diversification, capability and selective openness.

Policy phase	**Priority actions**	**Security objective**	**Economic/innovation safeguard**
Phase I: Assurance	Map critical dependencies; strengthen supplier, SBOM and remote-access controls	Make hidden dependencies visible	Avoid unnecessary exclusion where risk can be audited and contained
Phase II: Diversification	Dual-source critical telecom, cloud and infrastructure components	Reduce single-vendor coercive leverage	Use interoperability and performance standards to preserve competition
Phase III: Capability	Scale domestic components, telecom equipment, semiconductor packaging and security R&D	Raise domestic substitutability	Tie support to measurable technology transfer and productivity
Phase IV: Selective openness	Permit lower-risk Chinese-linked activity under proportionate controls	Preserve economic connectivity where strategic risk is low	Transparent criteria reduce policy uncertainty and rent-seeking
Phase V: Stress testing	Run procurement, cyber, supply and geopolitical disruption scenarios	Test resilience before crisis	Use evidence to recalibrate restrictions and avoid over-securitization

Source: Author's policy sequencing synthesized from India's 2020 FDI screening framework, telecom security rules, CERT-In assurance guidance, current electronics-manufacturing outcomes, and the strategic-dependence literature. See References [1]–[5], [9], [10], [16], [25]–[28].

A stronger strategic technology policy should therefore sequence restrictions, capability-building and market opening rather than treating them as mutually exclusive. The proposed sequence below emphasizes immediate security assurance while using industrial policy to reduce the number of sectors in which exclusion creates high switching costs.

11. Conclusion

India's technology-security regime is evolving from an investment-screening response toward a broader architecture of digital resilience. Press Note 3 established a cross-sectoral gate for Chinese-linked investment; telecom

trusted-source rules moved security into procurement and network architecture; and the Telecommunications Act and Critical Telecommunication Infrastructure Rules have strengthened the concept of critical digital infrastructure as a national-security concern [1–5].

The evidence does not support a simple conclusion that Chinese technology is inherently insecure or that technological decoupling is costless. It does support a more precise conclusion: dependence becomes strategically dangerous when it is concentrated in infrastructure that is difficult to replace, difficult to audit and capable of transmitting disruption across multiple sectors. The optimal response is therefore selective exclusion, diversification, domestic capability and continuous assurance.

India should consequently aim for "managed strategic dependence" rather than technological autarky. The objective is not zero exposure to Chinese technology; it is to ensure that no external supplier, investor or state can obtain a decisive coercive lever over critical Indian digital systems. Achieving that objective will require the integration of FDI screening, telecom security, industrial policy, cybersecurity standards and supply-chain intelligence into one coherent national-security strategy.

12. Study Limitations

Official FDI statistics understate total strategic exposure because capital can move through indirect structures and because supply-chain dependencies are distinct from ownership. Vendor security assessments are also partly classified, making it difficult to measure the precise probability of espionage or sabotage. The paper therefore focuses on structural vulnerabilities and policy design rather than attempting to quantify an exact probability of compromise.

REFERENCES

1. Government of India, Department for Promotion of Industry and Internal Trade. (2020). Press Note No. 3 (2020 Series), 17 April 2020. https://www.dpiit.gov.in/static/uploads/2025/07/e6c4b62b2af92e19a3ffd3092dd2902b.pdf
2. Government of India, Ministry of Commerce & Industry, Press Information Bureau. (2020). Government amends the extant FDI policy for curbing opportunistic takeovers/acquisitions. https://www.pib.gov.in/newsite/PrintRelease.aspx?lang=2&reg=48&relid=202359
3. Government of India, Department of Telecommunications. (2021). Final Induction Note: National Security Directive / Trusted Telecom framework. https://dot.gov.in/sites/default/files/FINAL-INDUCTION-NOTE.pdf
4. Government of India, Department of Telecommunications. (2024). Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024. https://www.dot.gov.in/static/uploads/2025/07/cb09cb6c3cc53f27a4d37397067e18bf.pdf
5. Government of India, Department of Telecommunications. (2026). Act & Policies portal, listing Telecommunications Network Rules, 2026 and related security regulations. https://eservices.dot.gov.in/act-and-rules
6. Government of India, Ministry of Finance. (2025). Economic Survey 2024–25, external sector chapter. https://www.indiabudget.gov.in/budget2025-26/economicsurvey/doc/echapter.pdf
7. Government of India, Ministry of Finance. (2026). Economic Survey 2025–26. https://www.indiabudget.gov.in/economicsurvey/doc/eschapter/echap16-1.pdf
8. DPIIT. (2026). Country-wise FDI equity inflows, January 2000–March 2026. https://www.dpiit.gov.in/static/uploads/2026/06/2cc182ef8c744244238af5ee1a847f35.pdf
9. Shrivastava, M. (2024). The strategic challenge of decoupling from China: The case of India's ICT sector. India Quarterly, 80(3). https://doi.org/10.1177/09749284241264045
10. Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351
11. Gong, Y., & Li, J. (2024). China's digital expansion in the Global South: Systematic literature review and future research agenda. The Information Society. https://doi.org/10.1080/01972243.2024.2315875
12. "Chinese digital platform companies' expansion in the Belt and Road countries." (2024). The Information Society, 40(2). https://doi.org/10.1080/01972243.2024.2317058
13. Tan, W. (2024). National security as the trump card: Assessing China's legal regime on cross-border data transfer. Information & Communications Technology Law, 33(3), 368–383. https://doi.org/10.1080/13600834.2024.2375125
14. Thornton, A., & colleagues. (2025). Authoritarian collaboration and repression in the digital age: Balancing foreign direct investment and control in internet infrastructure. Democratization, 33(1). https://doi.org/10.1080/13510347.2024.2442377
15. TRAI. (2022). Recommendations / consultation materials on trusted telecom products and preferential market access. https://trai.gov.in/sites/default/files/CP_11022022.pdf
16. CERT-In. (2025). Technical Guidelines on SBOM, QBOM & CBOM, AIBOM and HBOM, Version 2.0. https://www.cert-in.org.in/PDF/TechnicalGuidelines-on-SBOM,QBOM&CBOM,AIBOM_and_HBOM_ver2.0.pdf

17. Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A New Framework for Analysis. Lynne Rienner.
18. Brundage, C. (2023). The US–China semiconductor power-security dilemma: Decoupling the security and power struggles. International Journal. https://doi.org/10.1177/00207020231213612
19. Peng, D., Wang, Z., Kong, Q., & Cai, M. (2024). Evaluating the impact of OFDI on the growth quality of industrial firms. International Review of Economics & Finance, 92, 1616–1627. https://doi.org/10.1016/j.iref.2024.01.029
20. Xiao, L., Zhao, L., & Zhu, Q. (2024). Host country economic policy uncertainty, trade openness and Chinese enterprise overseas investment. International Review of Economics & Finance, 103566. https://doi.org/10.1016/j.iref.2024.103566
21. DPIIT. (2026). Country-wise FDI equity inflow during calendar year 2026, January–March 2026. https://www.dpiit.gov.in/static/uploads/2026/06/d1705d83523c9a29ccb1b827c46cfa9b.pdf
22. DPIIT. (2026). Country-wise FDI equity inflow, January 2000–December 2025. https://www.dpiit.gov.in/static/uploads/2026/04/efbfcc1b6ebb398f153c2374b32e960a.pdf
23. Government of India, Department of Telecommunications. (2025). Telecommunications (Framework to Notify Standards, Conformity Assessment and Certification) Rules, 2025. https://www.eservices.dot.gov.in/mtcte/about-mtcte
24. Government of India, Department of Telecommunications. (2026). Act & Policies portal: Telecommunications Network Rules, 2026. https://eservices.dot.gov.in/act-and-rules?page=1
25. Government of India, Ministry of Electronics & Information Technology. (2026). Domestic value addition in electronics manufacturing has improved significantly; currently at 18%–20%. Press Information Bureau, 1 April 2026. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2247771&lang=2&reg=48
26. Department of Telecommunications, Government of India. (2026). Act & Policies: Telecommunications Network Rules, 2026. https://eservices.dot.gov.in/act-and-rules
27. Department of Telecommunications, Government of India. (2024). Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024. https://eservices.dot.gov.in/sites/default/files/circular-notifications/Critical%20Telecommunication%20Infrastructure%20Rules%2C%202024_0.pdf
28. Indian Computer Emergency Response Team (CERT-In). (2025). Technical Guidelines on SBOM, QBOM & CBOM, AIBOM and HBOM, Version 2.0, 9 July 2025. https://www.cert-in.org.in/PDF/TechnicalGuidelines-on-SBOM%2CQBOM%26CBOM%2CAIBOM_and_HBOM_ver2.0.pdf