In whose tech we trust

Part I: Mapping Indo-Pacific security approaches to foreign owned, controlled or influenced technology

JUSTIN BASSI,
SIMEON GILDING,
ANGELA SURIYASENEE
AND JAMES CORERA

NOVEMBER 2025

Policy Brief

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

About the authors

Justin Bassi is the Executive Director at ASPI.

Simeon Gilding is a Senior Fellow at ASPI.

Angela Suriyasenee is a Researcher with ASPI's Cyber, Technology and Security Program.

James Corera is the Director of ASPI's Cyber, Technology and Security Program.

Acknowledgements

The authors would like to thank ASPI colleagues who helped work on or reviewed this report for their valuable review and feedback. We also wish to thank Tom Uren, Joonui Park, Manoj Harjani, Colonel KPM Das, Sameer Patil, Rijesh Panicker, Kazuto Suzuki, Ken Jimbo, Akira Igata and Takumi Kawasaki for their insights and contributions.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Cyber, Technology and Security Program

ASPI's Cyber, Technology and Security Program (CTS) analysts inform policy debates in the Indo-Pacific through original, rigorous and data-driven research. CTS is a leading voice in global debates on cyber, emerging and critical technologies, foreign interference and issues related to information operations and disinformation. CTS has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building and internet safety, satellite analysis, surveillance and China-related issues. To develop capability in Australia and across the Indo-Pacific region, CTS has a capacity-building team that conducts workshops, training programs and large-scale exercises for the public, private and civil-society sectors.

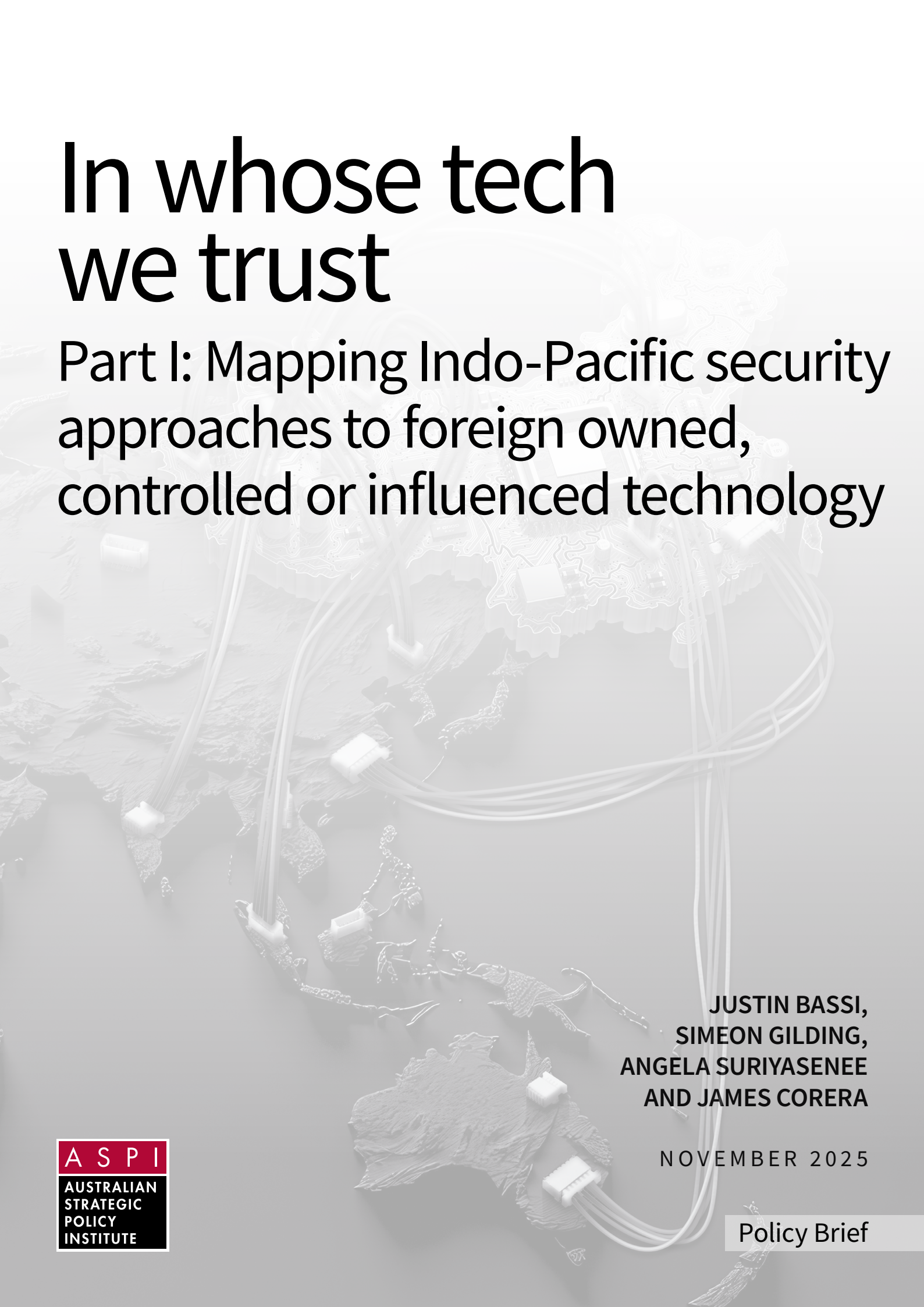
CTS enriches regional debate by collaborating with civil-society groups from around the world and by bringing leading global experts to Australia through our international fellowship program. We thank all of those who support and contribute to CTS with their time, intellect and passion for the topics we work on.

If you would like to support the work of the CTS, contact: ctspartnerships@aspi.org.au.

Cover image: Byron Illyes, ASPI.

In whose tech we trust

Part I: Mapping Indo-Pacific security approaches to foreign owned, controlled or influenced technology



JUSTIN BASSI,
SIMEON GILDING,
ANGELA SURIYASENEE
AND JAMES CORERA

NOVEMBER 2025

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Policy Brief

First published November 2025

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel Canberra + 61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au


Facebook.com/ASPI.org


@ASPI_org

Contents

Overview

While leading countries in the Indo-Pacific do fret about a hypertransactional Trump administration, they worry about another superpower when it comes to foreign ownership, control and influence (FOCI) of technology. As China has risen to dominate global manufacturing supply chains, it has flexed its growing national power to assert its interests at the expense of its neighbours, deploying force to press its territorial claims on India, Japan, Taiwan and the South China Sea, and backed up those efforts with economic coercion. But regulating Chinese technology is a tricky balance. As regional countries have become more concerned about China's strategic ambitions, they've also become more reliant for critical technologies on Chinese vendors that are subject to state direction. Reducing dependence on Chinese technology can't be achieved overnight without significant economic disruption. Therefore, managing the security and economic risks—whether by accepting or prohibiting Chinese technologies and identifying alternative options—requires special care. While China is uniquely positioned for reasons outlined in this report, and so is the focus here, China is not the only source of such risks.

This report provides a comparative analysis of how five Indo-Pacific countries—Australia, India, Japan, Singapore and South Korea—have sought to balance FOCI risks when assessing vendors. The report focuses on those five countries because they provide among the clearest and most mature policies, decisions and outcomes across sectors, which enables robust comparisons. Taken together, the five countries have developed well-documented guidance and enforcement mechanisms, making strong reference points from which the broader region can draw insights.

A separate ASPI report, Part II in this series and informed by this five-country comparative analysis, provides policy and governance options for governments and industry to mitigate risks and strengthen trusted technology ecosystems.

In settling their policies, all survey countries have needed to manage the tension between FOCI risks, economic costs and development objectives. Many of the most consequential steps have been quiet changes to procurement rules, licensing conditions, screening processes and technical standards. The pattern is consistent but not uniform. Where economic ties to China are deeper or political space is narrower, action has tended to be more circumspect. What's striking is not only that all five countries have taken action, but that the cumulative effect is stronger than is commonly recognised, precisely because much of it's happened out of the spotlight. That discretion has reduced political friction, but it's also meant that countries have often acted independently, and so there is an absence of shared best practice across the region.

The aim of this report is to explore which approaches represent best practice and might usefully inform other regional countries outside the scope of this report as they balance the benefits against FOCI risks. Few states have clear principles to guide decisions on FOCI technology vendors. Added to that is the reality that many Pacific (and some Southeast Asian) nations work with tight budgets, and Chinese digital technologies are widely available—often offering strong performance for price and sometimes paired with finance and delivery support. China has also shown it can move fast and respond proactively to requests from smaller Pacific governments, making offers attractive when capability or timelines are tight. For governments that rely on partners for digital transformation, affordability is understandably a primary filter that shapes incentives and can narrow feasible choices. In contrast, larger economies, like those that are the subject of this report, can draw on more established institutions, clearer legal mandates and deeper markets, allowing them to put greater weight on assurance and enforcement rather than on headline price.

While Australia's ability to manage high-risk technologies looks very different from that of other Pacific states, its strategic circumstances are similarly shaped by its simultaneous dependence on exports to China for economic growth and on the US for security. Until recently, Australia didn't feel it needed to choose between either country. However, sharpening strategic competition has made that balancing act increasingly difficult to sustain. This was made stark in China's response to Australia's decision to ban Chinese vendors from 5G networks, which made it plain that there are economic costs to technology decisions made on national-security grounds. Australia remains focused on the FOCI risks of technology vendors, but it now seeks to manage those risks in lower profile ways short of outright general bans. It's taken early and firm action to restrict the use of Chinese internet-connected technologies in government systems while calling

out particularly sensitive products such as TikTok and DeepSeek. More broadly, it's increased obligations on operators of critical technology to prepare, prevent and mitigate FOCI risks. And it's initiated government security reviews of foreign technology in sensitive areas to inform policy and technical guidance, issued voluntary guidance to public and private organisations on assessing and mitigating FOCI risk, and commenced detailed scrutiny of foreign investment proposals in critical infrastructure.

Recent Trump–Modi–Xi personal dynamics have obscured the decade-long hardening of Indian attitudes towards China and a commensurate effort to seek closer engagement with the US. That said, in the field of foreign technology policy, Indian efforts to reduce reliance on Chinese technology peaked in the wake of its border skirmish with China in 2020, when India took steps to exclude Chinese vendors from its 5G networks and began banning Chinese apps. Efforts since then to extend its 'trusted products from trusted sources' policy to other sectors have been hamstrung by India's dependence on China for industrial goods. In any case, the government's desire to substitute Chinese imports of those goods has been motivated as much by a longstanding Indian policy objective to develop local tech industries.

Japan's strategic posture has undergone an even more dramatic sea change in the years since a maritime territorial dispute with China in 2010 and a subsequent informal (and international law breaching) Chinese ban on rare earth exports to Japan. That shift has been reflected in Japan's foreign technology policy, where it's reframed economic and technological resilience as core components of national security. In 2018–19, Japan added opaque security requirements to public-sector and telecommunications procurement, resulting in Chinese vendors being excluded from all mobile networks. And, in 2022, it passed legislation empowering ministries to screen proposals for new facilities or changes to maintenance and management arrangements for existing facilities across a range of designated essential infrastructure service providers. If the government assesses that proposed plans have 'high risk of being misused as a means for actions taken from outside Japan to interfere with the stable provision of specified infrastructure services', the government can order the provider to 'take necessary measures to prevent disruptive actions'.[1]

Because Singapore is an open global business and financial hub, its economy and infrastructure are especially exposed to risks from foreign owned, controlled or influenced technology vendors whose products or services underpin critical systems. However, Singapore's lack of control over its external environment is offset by the government's tight grip on internal regulatory and policy levers. It's able to quietly take action to manage the threat of foreign vendors subject to direction from their government, should it judge the risk unacceptable. That happened with 5G.

South Korea frames Chinese technology vendors as a challenge to the resilience of its own high-tech manufacturing sector from intellectual-property predation and supply-chain disruption. The Korean Government has taken steps to protect designated advanced technologies through tax breaks to local companies and measures to prevent tech leaks and talent loss, and to secure supply chains by subsidising companies that diversify or reshore inputs. Authorities do have the capacity to restrict foreign technology in critical infrastructure, but their primary focus is on defending networks against malicious cyber actors from North Korea. In contrast to Japan, South Korea has been less concerned with the risk from foreign technology vendors. That divergence reflects differing economic exposure. Japan's commercial ties with China are significant but more diversified, giving Tokyo greater latitude to pursue a securitised approach, while South Korea remains deeply dependent on China for critical inputs, making it far more vulnerable to supply-chain disruptions. Alone among the five countries surveyed, South Korea imposed no restrictions on Chinese 5G vendors.

All five governments share concerns about China's growing military power and coercive economic behaviour. Two face contested borders, and four have experienced punitive economic actions. This explains the coherence of the response to 5G: all except South Korea acted decisively to mitigate the security risks posed by Chinese vendors, recognising the foundational role of telecommunications networks and the potential access vulnerabilities inherent in 5G systems. But, beyond 5G, the trade-off between security and economic pragmatism has to date proven more complex.

Across the country responses examined here, four themes that are relevant for future policy and strategy stand out.

1. Form matters: quiet moves, firm outcomes

Japan's opaque screening, India's 'trusted source' whitelist and Singapore's technical standards show how indirect measures can exclude FOCI vendors without overt bans. Those approaches work best in managed media environments, but like-minded coalitions such as the Five Eyes or Quad can help other societies coordinate and resist coercion.

2. Some exposures carry more risk: critical infrastructure demands proactive oversight

Japan and Australia offer two strong but distinct models. Japan's pre-procurement screening mitigates risk early but requires significant government control; Australia's operator-led regime is more flexible but depends on consistent implementation and can identify issues late. Both highlight the need to embed vendor risk management into everyday investment and operational decisions, and to treat critical infrastructure regimes as living instruments with scheduled reviews.

3. Government as market leader

Public procurement can set the tone for national standards. Rules on FOCI—such as in Australia's Protective Security Policy Framework and Japan's procurement rules—have created informal lists of trusted vendors and encouraged secure supply chains. Even limited exclusions, such as bans on specific apps for official devices, have shaped private-sector behaviour and signalled risk awareness.

4. Transparent principles, discreet choices

Clear, consistent and public principles have helped governments keep some operational decisions quiet. Transparency in intent has strengthened signalling to allies, adversaries and investors alike. Overflexibility has invited risk; pre-entry defaults and scheduled reviews have offered certainty and predictability.

Introduction

At a time of intensifying geostrategic competition, when borders are routinely contested and foreign interference operations are commonplace, internet-connected technologies that reach across national boundaries have become indispensable to the modern world. Those technologies lie at the heart of infrastructure that powers our cities, runs our transport networks, stocks our supermarkets, and communicates, stores and processes our data. More data is now generated every two days than in all human history up to the early 2000s, magnifying both the utility and the vulnerability of those systems.

There's a risk here, though. The technologies that reach across national borders can potentially be controlled or interfered with by their host nation. So, it's unsurprising that countries are paying more attention to who's building and maintaining the communication, industrial and consumer technologies upon which they rely. It's also predictable that Indo-Pacific countries have been at the forefront of those efforts. As China has risen to dominate global manufacturing supply chains and rival the US as a technology superpower, it has flexed its growing national power to assert its interests across the region, deploying force to press its territorial claims on India, Japan, Taiwan and the South China Sea, and backing up those efforts with economic coercion.

To be sure, regional countries fret about a hypertransactional Trump administration—and are examining each White House announcement for a guide on policy—but they also recognise that China is the only country that has:

- the industrial capacity and policy intent to outcompete other critical-technology providers
- legal and political instruments to direct technology vendors to support state intelligence objectives[2]
- a track record of hacking operations aggressively targeting other countries' digital critical infrastructure
- the proven willingness to use those tools in pursuit of its strategic interests.

Increased awareness of these issues means that governments have been looking for ways to control the risks of Chinese technologies embedded in the critical parts of their economies. But, as countries have become more concerned about China's strategic ambitions, they've also become more reliant on China for critical technologies—from telecommunications and 'internet of things' (IoT) equipment and semiconductors to cloud infrastructure and industrial control systems—such that Chinese technologies are structurally embedded in the region's economic and technological landscape. China is now not just a major manufacturer; it's a central node in global technology supply chains. For many countries, reducing dependence on Chinese technology can't be achieved overnight without creating significant economic disruption. Therefore, managing the risks (economic, diplomatic and security)—whether by accepting or prohibiting Chinese technologies and identifying alternative options—requires special care.

Report outline

This report examines how selected Indo-Pacific countries have assessed and managed advanced ICT vendors, evaluating the frameworks, criteria and practices used to permit or restrict vendors in their critical infrastructure sectors. The aim is to inform the evolution of technology risk frameworks, offering guidance for futureproofing policies that enable next-generation technologies while mitigating critical security risks.

A separate companion report from ASPI, partly informed by the comparative analysis here, provides policy and governance options for governments and industry to mitigate risks and strengthen trusted technology ecosystems.

Part 1 of this report explores the geostrategic context, outlining common drivers across all countries examined in the report: notably, the urge to increase digital security by reducing reliance on Chinese vendors, and the economic costs of those efforts. Those two considerations are factored into national judgements of 'trust' in foreign technology vendors, with differences in decisions depending on the comparative weightings given to them. That is, outcomes shift according to which set of factors dominate at the time a country makes a determination.

Part 2 examines five Indo-Pacific countries—Australia, India, Japan, Singapore and South Korea—as case studies of how these strategic, economic and technical realities have affected their respective national policy and regulatory frameworks. Those five were selected because they have overlapping but distinct national approaches to technological regulation, with diverse governance systems, strategic positions and economic scales factoring into their respective policies to manage exposure to China's technology ecosystem. The purpose of surveying each country's framework for managing FOCI risks is to assess which approaches represent best practice and might usefully inform other countries in balancing the benefits and risks of technological entanglement with China. In each case, analysis considered the following:

1. *Strategic context:* the geopolitical, economic and security factors shaping each country's perception of foreign technology risks.
2. *Policy framework:* the laws, regulations and institutional mechanisms designed to manage those risks.
3. *Implementation approach:* how governments translate policy into action, balancing national security, economic priorities and innovation objectives.

Across all five countries, responses combine defensive measures—such as excluding high-risk vendors from critical networks—with adaptive strategies that enhance resilience, manage dependencies and safeguard technological innovation without unduly constraining economic opportunity.

Part 3 of this report examines how the introduction of fifth-generation (5G) telecommunications in the late 2010s provides an early test of these approaches.

Appendix 1 gives a detailed review of existing legislative and regulatory regimes of the five nations relevant to addressing FOCI risks. Understanding those regimes better enables policymakers to assess which risks need new legal or regulatory tools and where existing mechanisms could be applied more effectively or be adapted to ensure they're fit for purpose regardless of the technology and geostrategic environment.

Part 1: Common framing

Before looking at the comparative insights, best practices and lessons learned from each of the five case studies, it's useful to have an understanding of the shared drivers and contributing factors common to all. All five have needed to manage the natural tensions created by the simultaneous pursuit of digital security despite limited domestic or other alternative technologies and the need for economic security, which may require trade-offs between economic opportunity and digital security risk. It means that, as the jurisdictions have had to assess the extent to which they can 'trust' foreign technology vendors, decisions have been required to weigh up the following factors:

- *Digital security:* the extent of exposure to the legal, political and technical leverage a foreign state may be able to exert on their national vendors to enable operational control of targeted technologies, leaving them vulnerable to exploitation that enables foreign interference, disruption and sabotage.
- *Economic security:* the extent of dependency on geostrategic competitors, which increases their exposure to market control and requires consideration of supplier concentration, supply-chain dependency and the costs of switching suppliers.

While both factors are prevalent across the jurisdictions, what differs is the relative weight each government assigns to them. Outcomes shift according to which consideration dominates the decision-making process at a given time. That variation helps explain why countries with broadly similar threat assessments nonetheless arrive at different practical approaches to reducing dependence on FOCI technology.

Digital security: trustworthiness of the vendor/technology

Digital security is concerned with assured operator control and system trust. It's about exercising control over who can direct updates, access data, hold signing keys and exercise lawful or extraterritorial control over systems.

Relevant here is the country of origin—meaning the jurisdiction that ultimately has ownership and/or control of technology, rather than its place of assembly. This reflects the reality that technology is increasingly used as a vector for foreign interference by hostile states. Vendors can be shaped by the legal and political environment of their home state, including intelligence cooperation laws and party or state influence in corporate governance. The potential for coercion or exploitation is real and growing.

Underpinning country of origin as an assessment factor are technical considerations; specifically, hardware and software exploitability. How products and services operate determines exposure. Operational characteristics such as on-site maintenance, remote management, cloud connectivity and routing through foreign servers determine who can influence, access or disrupt the system. Standard operating practices often leave vendors with significant control over deployments. Remote updates, default cloud management, vendor-held signing keys, data collection[3] and vendor-run maintenance or managed services create exposure pathways that can reduce operator visibility and concentrate single points of failure.

China presents risks that are specific to its legal and political setting. Intelligence and national-security laws enable state direction of companies and extraterritorial orders. Chinese Communist Party (CCP) and state influence in governance, data and export rules, and vulnerability disclosure regimes,[4] can extend state leverage over vendors.[5] In combination, those factors aren't unique to China but are more salient, given Beijing's market share and strategic ambitions.[6] The law, however, is just a visible aspect of a demonstrated record of cyber operations and economic coercion that's resulted in a legal and operational environment in which Chinese vendors can't be assumed to operate solely as commercial actors.

Consistent with the case studies analysed in this report (notably India), governments are considering the balance between control-plane assurance now (strict update governance and in-country change control) and steadily second-sourcing and localising critical hardware where feasible. The imperative is increasingly clear: governance is needed to match the speed of software risk while laying the groundwork for hardware substitution.

The 'digital security' approach views FOCI technology, as a potential instrument of coercion by adversarial states. It emphasises risks of deliberate disruption, espionage or manipulation. Those threats typically manifest through:

- *state direction of vendors* embedded in essential networks
- *targeted cyber operations* against sensitive systems
- *foreign investment or influence* in strategic assets.

The focus is on assured access to essential systems during crises, transparent control of data and protection from extraterritorial interference. Specific technical risks include:

- *loss of guaranteed access* to critical systems if contractual obligations fail during emergencies
- *limited visibility and control* over operations, data flows, algorithms and information management
- *extraterritorial control* of software updates and remote management functions.

Economic security: dependence on geostrategic competitors

Here, the key considerations are the degree to which a country relies on technology, components or services controlled by a geostrategic competitor, the extent to which that poses a strategic vulnerability, and the time and cost to replace legacy technology, components or services.

Chinese technology is deeply embedded across Indo-Pacific supply chains, and China functions as a major manufacturer and central node in global technology networks.

Technological products and services are rarely confined to a single geography or a single supplier. Multinational vendors operate sprawling networks of suppliers, partners and subcontractors that may span dozens of countries. Even parts sourced from 'trusted' jurisdictions often incorporate materials, software or sub-assemblies from higher risk areas. Major networking and semiconductor makers depend on thousands of suppliers spread across regions, which increases complexity and can reduce visibility for regulators and buyers.[7] While many non-Chinese vendors use distributed, multinational supply chains that give customers and regulators more levers to manage and monitor risk, indirect exposure to China through deeper supplier tiers remains an issue.

By contrast, key Chinese vendors—most notably Huawei—retain the bulk of their research, development and manufacturing inside China. That high degree of vertical integration centralises decision-making and technical control within a jurisdiction where state direction is both legal and commonplace. Such consolidation limits external visibility on product decisions, supply-chain practices and software updates, making independent verification of security and reliability far more difficult. The result is greater dependence on Chinese vendors for maintenance and upgrades, higher switching costs for customers seeking to diversify, and increased exposure to geopolitical pressures. Those factors raise the risk that, in a crisis, Chinese vendors could be used as an arm of CCP state power.

Taken together, these dynamics point to three structural shifts:

- Technological change is accelerating, creating new capabilities and vulnerabilities faster than policy and regulatory frameworks can adapt.
- Supply chains have become deeply globalised but are increasingly bifurcating. Beijing's dual circulation[8] and 'secure-and-controllable' IT policies[9] are localising sensitive technology at home, while many non-Chinese vendors are increasingly reliant on China. That's altering risk profiles and reshaping supply-chain structure and governance.
- Geostrategic competition has intensified, and technology is now a central arena for statecraft, coercion and strategic influence.

The 'economic security' approach frames foreign technology in terms of market distortions and industrial resilience. The core risk is loss of control over critical inputs, markets and pricing power. It emphasises the need to protect domestic innovation capacity and strategic industries. Threats emerge through:

- unfair competition or state-subsidised market advantages
- displacement or hollowing out of formerly domestic critical industries
- concentrated supply chains and single-supplier dependence.

Huawei and 5G: balancing interference, autonomy and economics

In practice, the countries examined here have been motivated by both assessment factors. The case studies show that outcomes often depend on which factor dominates at the time of decision. In 5G, the potential for China to gain technical leverage (thereby enabling disruption and sabotage) was the dominant consideration for Australia, India, Japan and Singapore, while South Korea placed greater weight on economic considerations.

5G was an early example of how technology developed for civilian or commercial use could be repurposed for military or political objectives. Dual-use technologies such as cloud platforms, sensors, drones, artificial intelligence (AI) models and data services can increasingly be redirected with minimal modification. That dual-use risk affects both assessment factors: digital sovereignty through covert access or targeting, loss of assured control of updates, data and functionality; and economic security through strategic dependence that enables coercion.[10] The levers of repurposing are multifarious—they lie in who designs and maintains the software, who signs updates, where data is processed, and how exposed vendors are to foreign intelligence direction.[11] Real-world experience, including the rapid militarisation of commercial drones, AI and satellite services in Ukraine, underscores how quickly civilian technologies can be weaponised—and why policy should anticipate that trajectory (see box).[12]

Huawei and 5G as a case in point

The introduction of 5G telecommunications in the late 2010s provided an early test of these approaches. Part 3 of this report provides further details.

In response to security risks posed by Chinese vendors, the US Government launched nationwide 'rip and replace' programs to remove high-risk equipment from critical networks. The Secure and Trusted Communications Networks Act, enacted in 2020, established the Secure and Trusted Communications Networks Reimbursement Program, allocating US$1.9 billion to help smaller telecommunications providers replace equipment from companies such as Huawei and ZTE.[13] In 2024, an additional US$3 billion was authorised to cover escalating costs associated with the initiative.[14]

Similarly, the European Commission directed EU member states to adopt strategic and technical measures to mitigate supplier-related risks, including assessing risk profiles and applying restrictions or, where necessary, exclusions. In June 2025, the commission excluded Chinese companies from EU government purchases of medical devices priced at more than €5 million, marking the first application of the International Procurement Instrument to limit Chinese participation in public procurement. In parallel, in March–April 2025, Belgian prosecutors arrested and later charged several people in a bribery probe into alleged efforts by Huawei to influence European Parliament decisions. As a precaution, the parliament suspended access for Huawei lobbyists during the investigation. Huawei has denied wrongdoing and has pledged to cooperate.[15]

While Australia's outright ban was the first in 2018 and most direct, India, Japan and Singapore achieved comparable outcomes through less visible regulatory and industry measures, often supported by discreet government–operator cooperation:

- *Australia* formally assessed Huawei and ZTE as high-risk vendors and excluded them entirely from 5G networks.
- *India* introduced procurement rules requiring equipment from 'trusted sources', and Chinese vendors were absent from the whitelist.

- *Japan* tightened public-sector procurement rules and imposed broad telecom security requirements, prompting operators to avoid Chinese suppliers.
- *Singapore* established performance, security and resilience standards that led licensees to select non-Chinese vendors for national core networks.
- *South Korea* imposed no formal restrictions, and one of its three major carriers chose a Chinese supplier.

In most cases, those national positions on 5G have influenced how countries manage broader technology risks beyond telecoms and across foreign owned, controlled or influenced technology suppliers more broadly. Australia has complemented sector-specific actions with a cross-cutting Technology Vendor Review Framework[16] that can examine specific technologies or classes of technology and advise on proportionate controls, while India has tended to extend measures through sector pathways reflecting both security and industry policy priorities. Together, those approaches have informed responses beyond telecommunications, including for cameras, cloud services and social media platforms.

Part 2: Indo-Pacific country profiles

This part examines how Australia, India, Japan, Singapore and South Korea, as five Indo-Pacific countries, have responded to FOCI risks. While their approaches overlap, they also diverge in important ways, shaped by differences in governance systems, strategic positioning and economic scale. The survey highlights how those governments manage exposure to China's technology ecosystem, particularly the risks posed by vendors subject to state direction. The purpose is to draw out best practices and lessons that can guide others in balancing the opportunities and risks of technological entanglement with foreign technology vendors.

Part 2.1: Australia's approach to managing FOCI risks

Key takeaways

Australia's approach to FOCI risk combines:

- *public exclusion* of Chinese vendors Huawei and ZTE from the National Broadband Network and 5G networks, based on concerns about extrajudicial obligations to foreign governments that conflict with Australian law
- *formal, broader risk-assessment frameworks* that apply to all technology vendors regardless of country of origin to assess FOCI risks or exposure to foreign jurisdictions that could conflict with Australia's security interests, including the Technology Vendor Review Framework, and voluntary guidance to public and private organisations on assessing and mitigating FOCI risk
- *a government procurement framework* that assesses and excludes any vendor with foreign ownership, control or influence, or exposure to foreign jurisdictions; such exclusions aren't blanket bans on vendors from China but reflect a country-specific outcome based on risk assessments—as seen with prohibitions and guidance from federal agencies on internet-facing technologies with FOCI risks
- *regulatory requirements* for critical infrastructure operators to identify and mitigate risks, with powers to compel remediation
- *rigorous foreign investment screening* for critical infrastructure and other sensitive sectors.

Strategic context

Australia's strategic circumstances are shaped by the nation's simultaneous dependence on exports to China for economic growth and on the US for security. Little more than a decade ago, balancing new economic interests with China and traditional security ties with the US was considered in Australia's interest, and former Prime Minister John Howard argued that there was 'no need to choose' between the two countries.[17] Rising strategic competition between those powers, and a greater focus on Australia's own sovereignty, have made that balancing act increasingly complex and difficult to sustain.

The 'balancing' approach saw policy initiatives that were each self-evidently sensible but contained inherent contradictions, including the 2009 Defence White Paper expressing concern about the 'pace and scope of China's military modernisation' in the same year that China became Australia's largest export market (driven by natural-resources exports).[18] In 2012, the Australian Government excluded Huawei from its National Broadband Network (an initiative to replace the country's ageing copper network with fibre) while simultaneously negotiating a free trade agreement with China that would be signed in 2015. Just a year later, a new Defence White paper would be shaped by China's military modernisation. By the time Australia excluded Chinese vendors from 5G networks in 2018, any attempt to 'balance' had been replaced by a definitive choice of Australian sovereignty. In other words, decisions on 5G vendor risk, foreign interference and rejection of the Belt and Road Initiative were taken on sovereignty grounds, and Australia accepted the cost of potential economic coercion.

Yet it remains the case that Australia's business and national-security communities hold starkly different views of China's rise. National-security agencies continue to highlight the risks posed by China's expanding military and technological capabilities, while Australia's business community sees China as a source of vast, unproblematic market opportunity. Those divergent perspectives continue to influence policy responses, including measures to manage risks associated with foreign owned, controlled or influenced technology vendors. It means that, despite Australia's strategic alignment with the US, Australia's approach to address those security risks has been more cautious since its 5G exclusion strategy. Australia is seeking to return to a policy of 'not choosing' between China and the US—a difficult trick at a time when both superpowers see no difference between national and economic security and readily punish 'two-faced' countries[19] that seek to 'butter both sides of [their] bread at the same time'.[20]

Policy framework and implementation approach

Australia has established two mechanisms to manage geostrategic threats relating to critical infrastructure and critical technologies.

First, the Foreign Investment Review Board (FIRB) offers a mature, constantly evolving process to examine proposed investments and make recommendations to the Treasurer. Where investments raise national-security concerns, the FIRB applies a national-security test to assess 'the extent to which the investment will affect Australia's ability to protect its strategic and security interests'.[21]

Second, Australia evaluates ICT vendor risks through the lens of foreign influence and disruption. The country was an early adopter of that perspective, recognising China's covert and coercive methods of interference. That lens has informed the government's latest guidance on third-party supply-chain risk management, which introduces the concept of FOCI.[22] FOCI analysis considers geopolitical tensions, national-security requirements, export-control regulations and the protection of critical assets, assessing how those factors affect suppliers, products, customers or broader supply chains.

As an overarching framework, Australia's Protective Security Policy Framework (PSPF) complements those mechanisms by setting government procurement standards to safeguard people, information and assets. It provides a unifying basis for vetting suppliers, securing sensitive systems and limiting high-risk vendor involvement across critical government and infrastructure supply chains. That's largely unique to Australia when compared to the other countries examined.

Together, those mechanisms illustrate how Australia seeks to combine regulatory oversight and economic pragmatism to manage the complex risks posed by foreign owned, controlled or influenced technology vendors.

Following its realisation of the risks inherent in 5G technology choices, Australia strengthened requirements for owners and operators of critical infrastructure to identify and mitigate operational risks. The *Security of Critical Infrastructure Act 2018* (SOCI Act) mandates reporting on cyber incidents affecting essential services, operational and ownership information, and a written risk-management program.[23] The Critical Infrastructure Risk Management Program, introduced in 2023, obliges owners to account for all hazards, including supply-chain disruptions intentionally aimed at compromising critical infrastructure.[24] A subset of 168 'systems of national significance' across energy, communications, transport, financial services and data sectors face additional obligations, including cyber incident response planning, vulnerability assessments, and near-real-time reporting to the government.[25]

In 2023–24, the government rolled out a framework to identify, manage and report risks of FOCI in technology assets across federal executive agencies. That included legally binding directions under the PSPF to nearly 100 departments and agencies, representing best practice for an additional approximately 90 Commonwealth corporate entities and wholly owned companies.[26] The directions restrict the use of Chinese and other untrustworthy internet-connected technologies while calling out particularly sensitive products such as TikTok and DeepSeek.[27] In short, the government recognised the FOCI risk and took early, firm and repeated actions to manage it within executive agencies. The action taken on TikTok and DeepSeek didn't involve the nationwide ban taken in relation to Chinese suppliers of 5G services, but rather prohibitions limited to government personnel.

In late 2024, SOCI Act reforms extended obligations to all business-critical data systems and introduced a directions power enabling 'regulators to compel a critical infrastructure entity to remedy a seriously deficient risk management program where there is a risk to national security, the defence of, or the social or economic stability of Australia'.[28]

Recommending the amending legislation to parliament, the Minister for Home Affairs, Tony Burke, drew attention to the heightened geopolitical and cyberthreats facing the country, which meant that 'the risk to our sovereignty, defence, and security has never been more present, especially for the critical infrastructure providing essential services crucial to our way of life.'[29] In support of that, he quoted the observation by the Director-General of the Australian Security Intelligence Organisation (ASIO) that 'malign foreign powers will consider using sabotage to coerce, disrupt or retaliate during times of escalating geopolitical tensions. Pre-positioning malicious code in Australia's critical infrastructure is the most likely means.'[30]

The intent of those reforms is different from Australia's ban on Chinese 5G vendors. That decision was enabled by powers to compel telecommunication companies not to use equipment that the Minister for Home Affairs (on advice from ASIO) considers 'prejudicial to security'.[31] In contrast, the SOCI Act reforms are about driving critical infrastructure to become match fit for an increasingly hostile world. Minister Burke also emphasised that those reforms are designed to embed preparation, prevention and mitigation into routine operations of critical infrastructure assets.[32]

Further measures to manage FOCI technology in the broader economy have been in that same spirit, including the December 2024 Technology Vendor Review Framework, which evaluates risks posed by vendors owned, controlled or influenced by foreign governments with interests conflicting with Australia's.[33] Interagency security reviews of foreign technologies deployed in sensitive areas inform future policies and technical guidance but, unlike government systems, the use of foreign vendors in the private sector will not be banned outright.[34]

In March 2025, Home Affairs took a further step, issuing guidance to help public- and private-sector organisations assess and mitigate a vendor's exposure to FOCI risks when they're procuring technology products or services.[35] Again, the guidance is voluntary, with no regulatory or reporting requirements.[36] The guidance contains sensible, realistic advice. It warns that Australian companies and organisations may have to spend more on products and services delivered by secure and verifiable technologies and vendors. But an 'up-front investment in a more secure product can reduce disruption and result in significant savings in the longer term.' It recommends that risk treatments might include technical controls to treat the specific access and control risks, the imposition of contractual obligations on a vendor, or managing the risk by diversifying to reduce reliance upon a single-source jurisdiction. And, if the risk can't be effectively treated by other means, it recommends restricting access to the vendor in procurement processes or replacing the product or service if procurement has already occurred. In certain circumstances, government security agencies can assist with the provision of treatment advice.

The government has also tightened foreign investment rules with China in mind.[37] In May 2024, it announced that investments in critical infrastructure, critical minerals or critical technology and those in proximity to sensitive Australian Government facilities or involving sensitive data would face greater scrutiny to protect the national interest.[38] In justification, the government noted the risk of potential access and control over sensitive organisations and assets such as critical infrastructure assets, which 'may provide opportunities for espionage, sabotage or other activities contrary to Australia's national security interests'.

Part 2.2: India's approach to managing FOCI risks

Key takeaways

India's approach to FOCI risk combines:

- *restrictions* on Chinese investment, requiring government approval for proposals
- *effective exclusion* of Chinese companies from government procurement
- *a de facto ban* on Chinese vendors in telecommunications networks through a rigorous 'trusted products from trusted sources' framework, emphasising opaque but credible technical assessments
- *ad hoc extension* of the trusted sources approach to products such as surveillance cameras and solar panels, driven by both security concerns and industrial policy objectives
- *aspirations* to expand trusted sources assessments to other critical sectors (such as power generation), constrained by China's dominance of high-tech and industrial supply chains
- *opaque processes* enabling exclusion of Chinese vendors while limiting diplomatic and commercial blowback.

Strategic context

Obscured by the drama of the recent personal dynamics between President Trump, Prime Minister Modi and President Xi, India's strategic posture evolved markedly over recent years. Previously styling itself as a non-aligned leader of the global South, India has become more pragmatic and willing to engage transactionally with an eye to strategic opportunities and risks—a country that can buy both Russian oil and US military equipment, and be a member of the BRICS as well as the Quad. Underpinning that approach is a hardening of attitudes towards China and a growing openness to deeper cooperation with the US. As External Affairs Minister Subrahmanyam Jaishankar noted in early 2025, the instinctive caution that had previously 'consciously limited' cooperation with the US has shifted towards an 'intersection of interests … substantial enough to serve as a foundation for a high-quality strategic partnership'.[39]

At the same time, recent high-level diplomatic engagements, such as the Chinese Foreign Minister's visit to New Delhi in early 2025, signal that India is also seeking to stabilise relations and avoid uncontrolled escalation with Beijing, even as structural competition endures. In early September 2025, Prime Minister Modi visited China to attend the Shanghai Cooperation Organisation Summit and met President Xi, and both parties framed the meeting as part of efforts to stabilise ties.[40] Uncertainties remain, including current tensions with the US flowing from tariff impositions to wean India off Russian oil and Pakistan policies under the Trump administration. But India is repositioning itself to become a counterbalance to China in a 'multi-polar Asia' and a trusted alternative in global supply chains.[41]

India has recognised the central role of technology in the protection of national security and pursuit of global influence; Jaishankar has noted that technology is 'now a structural feature of contemporary times'. India has sought to limit China's ability to influence the public via technologies that may be used as 'expressions of China's growing capabilities … that impinge directly on our interests [and require] mitigating dependence in sensitive domains'.[42] Those assessments and the fighting between unarmed Indian and Chinese troops in the Galwan Valley on the disputed border between the two countries in June 2020 were a key waypoint in India's recognition of its neighbour as a strategic competitor and security threat. The development of more sovereign critical technologies, therefore, is vital and requires 'analysing and prioritising partners': 'those who share traits of pluralism, democracy, market economy and rule of law have a natural convergence with us' but 'geo-political factors [and] historical experiences will also be part of our calculus. India may be non-West, but its strategic interests ensure that it is not anti-West.'[43] Policies subsequently restricted Chinese participation in government procurement and infrastructure projects. In May 2020, Prime Minister Modi launched the Atmanirbhar Bharat (self-reliant India) program to strengthen domestic production capacities (an elaboration of 2014's Make in India policy),[44] specifically targeting sectors in which dependence on China was highest.[45]

That said, India's dependence on China for industrial goods—ranging from machinery and electronics to chemicals—has raised concerns about supply-chain and cyber vulnerabilities. China's leadership in AI, semiconductors and green technologies accentuates those structural dependencies, particularly in energy, telecommunications and electronics. Chinese investment in Indian digital start-ups has also been perceived as a potential strategic vulnerability.

Policy framework and implementation approach

India's economic dependency on China and the Galwan incident provide the context for its efforts to restrict Chinese technology.

A fortnight after Galwan, India banned 59 Chinese apps deemed 'prejudicial to [the] sovereignty and integrity of India, defence of India, security of state and public order' (including TikTok, Shein, WeChat and Weibo). The government's press release accused 'elements hostile to national security' of stealing and exfiltrating user data to 'locations outside of India' for data mining and profiling.[46] The Minister for Information Technology characterised the decision as a 'digital airstrike'.[47] Successive orders, most recently in February 2025, have led to the banning of well over 600 Chinese apps or those with links to developers in China or Hong Kong.

India's big muscle movement on Chinese technology came with the announcement of the National Security Directive on the Telecommunication Sector in December 2020. How that unfolded is referenced in Part 3 of this report, but it's worth examining the 'trusted products from trusted sources' approach that underpinned the effective exclusion of Chinese vendors from India's 5G networks, because that has provided the model for Indian efforts to exclude Chinese vendors in other areas. That approach sits alongside India's other technical conformity regimes for telecom equipment. The trusted products / trusted sources regulation involves a thorough process for vetting telecoms equipment. Vendors must apply for equipment approval on a Trusted Telecom Portal, providing details on the products, vendors and security practices (set out in multiple detailed requirements). Assessment focuses on vendor and component source trustworthiness through the portal, and determinations are made by the National Cyber Security Coordinator as the designated authority and approved by the National Security Committee on Telecom. Post-deployment, the government conducts field inspections to verify continued compliance; if a certified product is later found with unexplained deviations, certification can be revoked and the product removed from networks. The trusted products / trusted sources mechanism determines what licensed operators may connect to their networks, and it focuses on vendor provenance and trust in addition to general technical conformity.

Another element of evaluation is carried out in hardware and software testing through the Telecommunication Engineering Centre's (TEC's) Mandatory Testing and Certification of Telecom Equipment (MTCTE) program, which was introduced in 2019.[48] The MTCTE is a separate mechanism run by the TEC that verifies a device against essential technical requirements for sale and import across certain categories but doesn't assess vendor geopolitical risk. The program tests products for both technical and security parameters by government-designated laboratories against TEC 'essential requirements' and is a prerequisite for sales or imports in covered categories. In practice, the way those two processes would interact is that vendors typically obtain MTCTE certification for a product first, and if/when a telecom operator wants to deploy or integrate a product, it must also meet the 'trusted product' checks. A device could in theory pass the MTCTE and still be refused connection to national networks; for example, if it isn't designated as 'trusted'. In that way, the two equipment vetting regimes create a dual gate to carefully vet out high-risk ICT vendors.

The certification process is focused on hardware components as well as the software (firmware) that governs devices. Reportedly, conditional approval for the use of foreign vendors is subject to them reducing reliance on Chinese components.[49] Given that up to 80% of the components are made in China, this seems unrealistic and may be unnecessary. The most undetectable and scalable vector for an adversary-controlled vendor to manipulate a target device is through firmware updates. Regardless, that broad focus on components as well as software characterises India's approach to the certification of foreign technology in other areas.

The rigour of the certification process is matched by the lack of transparency in the decisions that emerge from it. Decisions aren't made public; they're communicated directly to applicants through the Trusted Telecom Portal. But thoroughness and opacity are the innovative features of the policy, the former providing credibility, the latter masking

the *de facto* blacklist of Chinese vendors.[50] Used this way, opacity has enabled India to mitigate against Chinese suppliers while limiting overt retaliation. At the same time, India has demonstrated pragmatism by allowing flexibility in certain high-priority infrastructure sectors in which alternatives are limited, such as in metro transportation, and where the need to sustain project timelines and economic development can be prioritised over strict exclusions. A comparable experience occurred in the UK's telecommunications sector from 2010, when a Huawei-funded evaluation centre staffed by UK nationals was established to scrutinise the company's hardware and software, end-to-end. The exercise demonstrated that technical oversight could mitigate immediate risks but neither guarantee long-term security nor shape strategic outcomes. Ultimately, while technical measures mitigated existing vulnerabilities, only a policy decision to exclude could address future risks stemming from potential shifts in the intent of the Chinese Government, which had control over Huawei (the UK made that policy decision in 2020, excluding Huawei from its 5G networks).

The Indian certification process (as was seen in the UK's instance again) is resource intensive for telcos, vendors and government alike. And it's broader than 5G kit, ostensibly capturing all new equipment connected to networks (although claims by domestic manufacturers that 40% of networking equipment continues to be supplied by Chinese companies suggest that the government's focus is on core telco network kit).[51]

The Indian Government has hinted about extending the 'trusted products from trusted sources' policy beyond the telecommunications sector, but efforts to date have been patchy.[52] For example, officials have highlighted the risks of Chinese-dominated IoT modules, citing that over 80% of India's IoT market is served by Chinese firms including Quectel and Neoway, and indicated that similar trust-based requirements would be applied to IoT devices and other vital sectors, such as energy.[53]

Another example is CCTV cameras. Those supplied to government agencies have been undergoing testing since June 2024 and, since April 2025, manufacturers are being required to submit internet-connected surveillance cameras for testing at government laboratories to be certified for sale in India.[54] However, efforts to implement that policy outside the telecom sector have encountered several challenges, leading to inconsistent application. In the IoT sector, for example, while the government has highlighted security risks from dominant Chinese vendors, a complete exclusion can't be enforced, mainly because India's domestic IoT manufacturing remains nascent and is not yet competitive enough to replace imports. Likewise in the solar energy sector, in which attempts to apply trust-based procurement have been stop–start. Initial introductions were followed by delays as local producers struggled to meet the quality and scale requirements. Those sectoral differences mean the 'trusted sources' approach has so far been rolled out in a gradual and interrupted manner, driven by the need to balance security imperatives with industrial readiness. As such, while the policy appears to be motivated by security concerns about Chinese companies,[55] it also has its origins in the government's 'Make in India' industrial policy.[56] No Chinese models have been certified, and they appear to be facing additional hurdles.[57]

Further, in early 2024, the government announced that solar panels procured in government-funded projects would be limited to those on an approved list of models and manufacturers.[58] The purpose of the policy was to exclude Chinese vendors. Most recently, in early 2025, India's National Cyber Security Coordinator flagged that the government was working on trusted-source product rules for equipment used in the power sector,[59] but India is heavily dependent on Chinese generators and turbines. Between 2006 and 2019, Chinese companies won US$16 billion worth of projects in the sector—mainly coal-fired power plants, which generate three-quarters of India's electricity.[60] China's intelligence services also have form in this sector: multiple intrusions into electrical infrastructure were reported in 2021–22 following the Galwan Valley incident.

Despite import-substitution efforts, India has struggled[61] to reduce its dependence on China due to the latter's dominance of supply chains and the lack of local alternatives and industrial capacity.[62] Therefore, India's dependence on China for technology to develop its industrial capacity is both a driver for and a restraint on further technology regulation.

Complementing those measures, India has also been a potential beneficiary of the 'China+1' diversification strategies that other countries have adopted to mitigate reliance on China.[63] While that role has yet to translate into large-scale supply-chain shifts, it's increasingly seen as a geo-economic priority, and the Minister of Commerce is

under pressure to define measurable targets that would convert India's position into tangible gains. In that context, managing high-risk vendors complements the push for domestic innovation by creating clearer guardrails for trusted technology partnerships.

India's silent, or at least opaque, approach to banning Chinese and other suppliers of concern has reduced system vulnerabilities and prevented potential foreign control over many of its systems while avoiding retaliation.

Part 2.3: Japan's approach to managing FOCI risks

Key takeaways

Japan's approach to FOCI risk combines:

- *close monitoring* of foreign direct investment (FDI) to prevent the acquisition of sensitive technologies by foreign or state-controlled entities
- *telecommunications protection*: effective exclusion of Chinese vendors from private 5G networks through government procurement rules, later formalised via broad security obligations for telcos
- *de facto exclusion* of high-risk vendors from central government IT procurement and cloud services via supply-chain screening
- *issuance* of best-practice cybersecurity frameworks to highlight and mitigate risks from potentially compromised foreign vendors
- *discreet oversight* of essential infrastructure using structured, confidential processes (leveraging close government–industry relationships) to screen vendors across 15 critical sectors, balancing security with operational continuity.

Strategic context

Japan is an island nation with few natural resources and in close proximity to China, North Korea and Russia. Its postwar economic miracle was enabled by US security guarantees underwriting maritime trade routes and a stable multilateral trading system that provided predictable access to global markets.

Japan's vulnerability to Chinese supply chains became evident when China imposed an informal ban on exports of rare earths following the 2010 arrest of the crew of a Chinese trawler that rammed two Japan Coast Guard vessels in the contested Senkaku Islands in the East China Sea. At the time, Japan relied on China for four-fifths of its requirements for those minerals, which are essential for high-tech manufacturing.

The 2010 incident intensified Japan's security debate. In late 2013, the Abe government established the National Security Council and Secretariat (to serve as the 'control tower center for Japan's foreign policy and national security policy')[64] and released the country's first National Security Strategy (NSS).[65] At its centre was the assessment that 'Japan cannot protect its day-to-day peace and security unless it actively contributes to regional and global stability and security in cooperation with the international community.' The 2013 framing foreshadowed constitutional reinterpretations that enabled Japan's armed forces to support an ally under attack. Nearly a decade later, the updated 2022 NSS[66] described China as Japan's most significant regional security challenge and committed to strengthening the Japan Self-Defense Forces.

The late 2010s saw a further evolution in Japanese strategy—a reframing of economic and technological resilience as core components of national security. Japan's official policy position towards high-risk vendors is country- and vendor-agnostic. It has sought to apply risk-based criteria on a case-by-case basis to protect its critical infrastructure and stabilise essential services. Amid the Covid-19-related supply-chain shocks, the ruling Liberal Democratic Party turned its mind to the development of an economic security strategy,[67] releasing multiple proposals in 2020. Over the same period, economic-security divisions were created in the ministries responsible for economic, trade and industry, and foreign affairs, as well as in the National Security Secretariat. And, in 2020, the government increased scrutiny of foreign investment to protect sensitive technologies from foreign acquisition.[68]

In August 2022, the Kishida government appointed a Minister of State for Economic Security. Later that year, the 2022 NSS expanded the concept of national security to include the economic domain, citing supply-chain vulnerabilities, cyberattacks, threats to critical infrastructure and competition over advanced technologies as major security challenges.[69] It called for defensive economic measures against coercion and espionage, highlighting attempts by certain states to expand influence by restricting critical exports and engaging in intellectual property (IP) theft of sensitive technological information.

In line with that paradigm shift, Japan was one of the first to enact a comprehensive Economic Security Promotion Act (ESPA) in 2022, aimed at ensuring the 'stable provision of specified essential infrastructure services' through regulation to strengthen supply-chain resilience, safeguard critical infrastructure and protect emerging technologies.[70] Through the ESPA, ministries use country-agnostic criteria to screen new critical-infrastructure projects and block vendors and vendor activity that could compromise national systems. That enables Japan to manage FOCI technology risks without issuing overt country- or vendor-specific bans.

Japan's policy emphasises technical trustworthiness and vendor risk assessment over overtly politicised restrictions. Its regulatory lattice allows authorities to deter high-risk vendors while maintaining a rules-based posture that aligns with its G7 partners. Close coordination with allies reinforces that stance—for example, Japan has worked with the US and others to promote secure 5G supply chains and open network architecture, although US commitment to investment in Open Radio Access Network architecture is now in question. In parallel, Japan is investing heavily in domestic capabilities in semiconductors, AI and quantum computing to reduce reliance on foreign suppliers. The Ministry of Economy, Trade and Industry (METI) has also recognised the inseparability of cybersecurity and physical security, introducing the Cyber/Physical Security Framework to ensure trust at three levels: the integrity of providers, the security of cyber–physical interfaces and the trustworthiness of data itself.[71]

Policy framework and implementation approach

Japan frames the high-risk vendor issue as technical and operational vulnerabilities in ICT supply chains, particularly for products and services that underpin critical infrastructure. Concerns include hidden backdoors, sabotage capabilities, unauthorised access and state-linked espionage. The government's focus is on verifiable security practices and supplier diversity, and ministries urge both public and private operators to scrutinise third-party vendors for red flags such as opaque ownership, weak security track records and links to foreign intelligence agencies.

While officially vendor-agnostic, Japan's stringent evaluation criteria set a high benchmark and have, in practice, steered major operators away from higher risk suppliers in critical roles while avoiding unnecessary diplomatic escalation.

Japan began implementing structured regulatory measures in 2018 with the Agreement on National IT Procurement Policy, which introduced supply-chain security checks for government IT procurement. Agencies must now assess potential risks—such as backdoor vulnerabilities or undue foreign control—before purchasing IT equipment or services. This involves requests for information to collect detailed vendor and product data and avoiding procurement from vendors where security risks can't be mitigated.[72] Where security risks can't be adequately mitigated, agencies are expected to take the necessary measures, which may include not proceeding with procurement.

Around the same time, regulators deepened engagement with critical infrastructure operators directly on vendor risks. The then National Center of Incident Readiness and Strategy for Cybersecurity (now the National Cybersecurity Office),[73] the Ministry of Internal Affairs and Communications and other agencies issued voluntary (but effectively binding) guidelines that require planning for worst-case scenarios, including the compromise of foreign vendors providing system maintenance. Ministries could use those review processes to block or raise concerns about high-risk suppliers.

Amendments to the Foreign Exchange and Foreign Trade Act in 2019–2020 strengthened FDI screening for sensitive firms; a very low prenotification threshold enables conditions, blocks or divestment where foreign state influence is a concern.[74] This closes potential pathways for foreign owned, controlled or influenced technology providers to gain influence indirectly via equity stakes.

In 2020, the government launched the Information System Security Management and Assessment Program, which sets a baseline for cloud service providers seeking to serve the central government.[75] To be government certified, providers must submit to an audit against security standards, including an assessment of 'the risk of unintentional access to or processing of information managed by the procuring ministry/agency etc., as a result of the application of laws and regulations other than domestic laws for information handled by the cloud service'.[76]

Those initiatives portended the essential service provider obligations legislated in the 2022 ESPA, and now cover 15 sectors, including energy, water, telecommunications, postal, transport, broadcasting, financial services and credit card providers. Under Chapter III of the ESPA, 'specified essential infrastructure providers' must notify the government in advance of major system changes, technology procurements or outsourcing of critical maintenance, triggering time-bound reviews.[77] The Cabinet Office's Economic Security Secretariat, together with relevant ministries, reviews those notifications for risks such as foreign ownership ties or excessive dependency on single suppliers against country-agnostic criteria (such as exposure to foreign legal compulsion, ownership or control, transparency and operational assurance). Ministries can order modifications or block projects if concerns arise. Although the ESPA is relatively new, it largely formalises existing government–industry coordination, shaping operator expectations about which proposals are likely to satisfy the screening criteria.

The Act on Protection of Important Economic Security Information[78] was also introduced alongside the ESPA in 2024, establishing Japan's first formal security clearance system for private-sector personnel handling sensitive designated economic-security information. Those developments aim to improve how risk information is shared between trusted corporate counterparts and government and further support public–private collaborations.[79]

Since May 2024, the government has required designated essential infrastructure service providers across those 15 sectors (so far over 250 in July 2025)[80] to seek prior approval for new facilities or changes to maintenance and management arrangements for existing facilities. Electricity, gas, water, telecommunications, financial services and credit card providers, as part of this process, need to provide details of suppliers of facility components. The focus for the screening is primarily information-processing systems used in the provision of essential infrastructure such as operating systems, middleware and business applications.[81] Contractors and subcontractors carrying out maintenance, management or operations at the facilities are also scrutinised. If the government assesses that proposed plans have 'high risk of being misused as a means for actions taken from outside Japan to interfere with the stable provision of specified infrastructure services', the government can order the provider to 'take necessary measures to prevent disruptive actions' (that is, to change or discontinue the plan or take risk-reduction measures).[82]

While the scheme is country-agnostic, the intent in relation to foreign vendors is clear. Providers are expected to confirm that their suppliers will report breaches 'that may result from the legislation of a foreign country or an external entity's instructions (including both explicit and tacit ones)'. And they're expected to provide 'information that helps determine whether and to what extent it is under foreign influence'.[83]

As with 5G vendor screening, decision-making on foreign vendors is opaque. It's surprising that critical infrastructure providers appear to be accepting of those onerous obligations, which reduce the field of eligible suppliers and probably raise costs. While the scheme has been in operation for only a short time, there appear to be no reports of companies denying orders, nor of government issuing them. A few considerations may explain that, including that underpinning these interactions is a strong culture of close relationships between the bureaucracy and large firms (and a revolving door between the two)—a legacy of Japan's postwar approach to industrial policy. All of this enables frank private conversations in which officials can be explicit about their vendor concerns, so that when proposals are formally submitted for review they take account of those sensitivities.[84] Over time, this process can help operators learn which suppliers will pass review and which will raise red flags.[85]

Part 2.4: Singapore's approach to managing FOCI risks

Key takeaways

Singapore's approach to FOCI risk combines:

- *de facto exclusion* through performance, security, and resilience standards that effectively bar high-risk vendors from national mobile networks
- *legal capacity to act* across essential services with stringent cybersecurity and operational resilience requirements, enabling the removal of vendors that are vulnerable to foreign interference
- *authority to exclude* such vendors from government contracts on national-security grounds to ensure procurement safeguards
- *neutral public framing* with a consistent policy of describing supply-chain risks without naming countries, avoiding public attribution to foreign state direction.

Strategic context

Singapore is a multi-ethnic, trade-dependent city-state with neither strategic hinterland nor natural resources, but a prime location at the crossroads of regional trade routes.

The city-state is a business and financial services hub heavily dependent on trade flows valued at more than three times its GDP (it's the world's largest transhipment hub).[86] To an unusual degree, Singapore's prosperity relies on open economic policy settings to attract business (it markets itself as a stable, reliable and trusted partner), backstopped by geopolitical stability and predictable multilateral rules-based economic arrangements. Singapore's 'friend to all, enemy to none' foreign policy seeks to balance relations between the two superpowers. It hosts a logistics hub for US naval forces but also assiduously cultivates strong relations with China. Given its size, Singapore relies on a technologically advanced military and a concept of 'total defence' to mobilise all sectors in support of national resilience.[87]

Because Singapore is a global business and financial hub, its economy and infrastructure are deeply integrated into global technology supply chains, making it especially exposed to risks from foreign owned, controlled or influenced technology vendors whose products or services underpin critical systems—but it has worked hard to address that vulnerability. While Singapore's domestic market is relatively small, the government has strategically leveraged government-linked companies[88] to maintain control over critical sectors, simultaneously fostering partnerships with vendors to enhance scale, innovation and technological development.

Acutely aware of its exposure to geopolitical shocks and systemic technology risks, Singapore avoids overt geopolitical signalling while quietly implementing a pragmatic, layered and sector-specific approach to technology security. Traditionally, this has been Singapore's style. However, under Prime Minister Lawrence Wong, there are early indications of a shift towards more explicit signalling in technology policy, including officials who are more willing to acknowledge geopolitical drivers alongside technical and operational framing.[89] Currently, and much like India and Japan, Singapore's model effectively screens out high-risk vendors without explicitly naming countries or companies, balancing the imperatives of safeguarding critical infrastructure with maintaining its status as a global technology hub. Rather than imposing blanket bans, Singapore enforces stringent performance, operational resilience and cybersecurity standards—particularly for vendors supporting critical information infrastructure and essential digital services. That framework rests on security-by-design principles, continuous oversight and risk-based evaluation, allowing authorities to manage foreign technology risks discreetly and flexibly.

Singapore's procurement rules allow for the exclusion of suppliers on national-security grounds. In March 2025, when asked about possible restrictions on DeepSeek, the Minister for Digital Development and Information wouldn't comment directly but repeatedly emphasised 'security' and confirmed that technology suitability is regularly reviewed against performance, resilience and security criteria.

Policy framework and implementation approach

Singapore's legal powers allow decisive action against vendors suspected of enabling foreign interference in critical infrastructure. However, it defines cybersecurity threats in country-agnostic terms, framing them as the work of 'malicious actors' rather than attributing them to specific states. In contrast to Japan, India and Australia, there have been few hints about the risks posed by vendors from hostile states. That would be inconsistent with Singapore's efforts to attract tech talent and capital from all comers. The recent public attribution of a major cyber incident to a state-linked actor marked a significant departure from that longstanding neutrality; even though Singapore identified a Chinese-linked 'advanced persistent threat' actor, it declined to explicitly say where it was from. While this is only one data point and not yet evidence of a broader trend, it suggests that Singapore may be incrementally open to naming risks where the evidence is overwhelming.[90]

The country's regulatory architecture is a tiered governance system built on 'Zero Trust'[91] principles, delegating operational oversight to sectoral regulators while maintaining strong central coordination through the Cyber Security Agency of Singapore. Accountability sits firmly with operators—especially critical information infrastructure owners and essential service providers—who are legally responsible for managing third-party vendor risks under three interlinked principles:

- *pre-engagement:* formal designation, risk classification and due diligence
- *contractual controls:* audit rights, breach notification and termination clauses
- *post-approval monitoring:* reassessment after threat changes, ownership shifts or technology upgrades.

The Cybersecurity Act 2018 established the legal foundation for designating and regulating critical information infrastructure, which was reinforced in 2019 when 'Digital Defence' became the sixth pillar of 'Total Defence'.[92] The Covid-19 pandemic then accelerated digitisation, increasing reliance on external providers and revealing hidden interdependencies. The 2023 Equinix data centre outage—caused during routine third-party maintenance and disrupting banking operations—underscored how even inadvertent vendor failures can trigger systemic consequences.[93] Some observers draw two lessons. First, Singapore can mobilise and recover quickly. Second, the episode tests whether the regulatory settings are sufficiently preventive, and not just reactive. Judging that requires sector-specific benchmarking against international best practices.

In response, the Cybersecurity Act was amended in 2024 to expand its scope to cover third-party infrastructure, including offshore and cloud-based systems, and to introduce new obligations for 'foundational digital infrastructure' providers and 'entities of special cybersecurity interest'.[94] Critical information infrastructure operators must now embed audit rights, real-time incident reporting and termination clauses into vendor contracts, and the Cyber Security Agency of Singapore is empowered to order the discontinuation of systems posing unresolved national-security risks.[95] Complementing that, the Critical Information Infrastructure Supply Chain Programme mandates structured risk assessments, covering vendor interdependencies, privileged access and potential impacts of compromise.[96] Singapore's Significant Investments Review Act, which came into force in 2024, also established an investment screening regime that allows the government to designate critical entities and require approvals for ownership and review of substantial transactions that may pose a national-security risk to Singapore.[97]

Sector-specific regulators add further layers:

- *Financial sector:* Singapore's role as a global financial hub means that protecting the banking and finance sector is a top priority. The Monetary Authority of Singapore (MAS) enforces stringent controls through its Technology Risk Management Guidelines,[98] outsourcing notices[99] and Third-Party Risk Management Guidelines. Regulated entities must assess vendor criticality, geopolitical exposure, cybersecurity history and jurisdictional legal environments. Contracts must allow MAS audits, require breach reporting, ensure data sovereignty and include life-cycle governance. MAS conducts active audits, issues remediation orders and can suspend vendor services.

- *Telecommunications:* The Infocomm Media Development Authority operates the Equipment Registration and Approval Scheme, requiring technical and security documentation before type-approval. The authority can revoke approval for insecure or noncompliant products—an effective but discreet filter against high-risk vendors, demonstrated by Singapore's 5G rollout.[100]

So, the government has strong powers to address vendors suspected of being vectors for foreign interference in Singapore's critical infrastructure. The government has the capacity to take action to quietly manage the threat of foreign vendors that are subject to direction from their government, should it judge the risk unacceptable. That seems to have happened with 5G. Singapore may be a 'sampan in a typhoon' of geopolitical rivalry, but the government runs a tight ship and chooses not to broadcast every course correction. Interventions are implemented quietly, avoiding the public naming of entities, allowing Singapore to neutralise risks from FOCI technology vendors while safeguarding its geopolitical neutrality and economic competitiveness. Much like the other countries examined here, the opacity of enforcement makes it difficult to assess the application of those practices and their outcomes.

Looking ahead, the forthcoming Digital Infrastructure Act, led by the Ministry of Digital Development and Information, will elevate existing advisory guidelines for infrastructure providers into binding regulations.[101] Together, those measures reflect Singapore's view that digital resilience is not only a technological necessity but a core pillar of national and economic security.

Part 2.5: South Korea's approach to managing FOCI risks

Key takeaways

South Korea's approach to FOCI risk combines the following factors:

- There are *no explicit regulatory restrictions* on foreign 5G vendors, although only the country's third-largest mobile operator selected Huawei equipment.
- Authorities have the *capacity to restrict* foreign technology in critical infrastructure, but the primary focus is on defending networks against malicious cyber actors—particularly North Korea—rather than on risks from vendors under foreign government influence.
- *China-related risks* are framed in terms of supply-chain disruption and the potential loss of advanced Korean technologies, and extensive measures are in place to mitigate those threats.
- *Public-sector procurement* rules impose high compliance hurdles for all foreign vendors and, apart from specific cases like DeepSeek, are applied in a country-agnostic manner.

Strategic context

The Republic of Korea (ROK) is an export-driven economy with limited natural resources.[102] Trade as a share of GDP is just short of 90%[103] and is powered by a high-tech manufacturing sector (accounting for around a quarter of GDP) that's heavily exposed to supply-chain disruption. A short distance north of the capital, Seoul, is an aggressive and unpredictable nuclear-armed North Korea, which is assessed 'as the biggest threat to ROK cybersecurity'.[104] The new Lee Jae-myung administration, inaugurated in 2025, inherits those security challenges but has signalled an interest in easing inter-Korean tensions through calibrated confidence-building while retaining a strong defence posture and alliance commitments with the US.[105]

Policies change when governments change. We can see this in both South Korea and Australia—the two countries in our survey that have switched ruling parties over the past decade. Under the centre-left government of Moon Jae-in from 2017 to 2022, South Korea was more sensitive to Chinese views (as seen in the 5G decision). The country swung closer to the US under Moon's conservative successor, Yoon Suk-yeol, and South Korea became more aligned[106] with the US on emerging technologies.[107] The Lee government has so far sought a more flexible and pragmatic balance between the two major

powers.[108] While emphasising that the US remains South Korea's only treaty ally, Lee has emphasised 'strategic autonomy' in economic and technology policy, attempting to restore limited and careful working-level engagement with Beijing on supply-chain stability without undermining Seoul's alliance commitments.[109]

South Korea frames Chinese technology vendors as a challenge to the resilience of its own high-tech sector against IP predation and Chinese economic coercion. Its strategic posture is often described as 'economy with China, security with the United States'—a formula that, for decades after the 1992 normalisation of relations with Beijing, rested on complementary economic and security arrangements.[110] China's entry into the World Trade Organization in 2001 accelerated integration, making it Seoul's largest trading partner, while Korean firms shifted manufacturing to low-cost Chinese facilities. That trajectory deepened further with the 2015 China – South Korea Free Trade Agreement, which entrenched cross-border supply chains and economic interdependence. The security pillar remains anchored in the US–ROK Mutual Defence Treaty, under which 28,500 American troops are stationed in South Korea, including at the largest overseas US military base.[111]

Together, China (including Hong Kong) and the US account for over 45% of Korean exports, and the ROK continues to source over a fifth of its imports from China.[112] That leaves its firms exposed to the shifting decisions of regulators and policymakers in both Beijing and Washington. At the same time, Korean companies must compete globally against increasingly competitive, low-cost Chinese high-tech producers.

Maintaining such a balance between the major powers has proven challenging in practice. Beijing's economic retaliation against Seoul's 2016 decision to deploy the US THAAD missile defence system shook Korean confidence in China as a stable partner,[113] prompting corporate hedging and supply-chain diversification. China's coercion of South Korea was akin to its coercion of Japan from 2010 to 2014 over rare earths. Meanwhile, Chinese industrial upgrading has turned the two economies into competitors in advanced technology sectors, while US export controls on China have threatened Korean semiconductor sales.

In response, South Korea has sought to arm itself with economic security measures to strengthen the resilience of its supply chains as well as to protect its high-tech sector. Both the Moon and Yoon administrations had also passed a plethora of legislation to protect designated advanced technologies through tax breaks to local companies and measures to prevent tech leaks, end talent loss and secure supply chains by subsidising companies that diversify or reshore inputs.[114] Some of that legislation has strengthened restrictions on foreign investment in strategic sectors to prevent the loss of IP in advanced technologies in which local firms have an edge.[115] While those laws are country-agnostic, in practice, they've been used to target Chinese investment.[116] Under President Lee, South Korea's industrial policy has been backed up by financial firepower, including a 50 trillion won (US$34 billion) fund for strategic sectors[117] and a planned 100 trillion won (US$71 billion) investment in AI,[118] signalling a move towards production-based semiconductor tax credits and logistics upgrades.

Rather than naming countries or imposing blanket bans, Seoul relies on a layered regime of regulatory scrutiny, technical standards and investment controls that function as indirect filters in critical infrastructure. Laws such as the Telecommunications Business Act[119] and Critical Information Infrastructure Protection Act[120] empower authorities to scrutinise and, if necessary, restrict foreign technology in networks and essential systems—prioritising integrity, trustworthiness and resilience rather than only country of origin.

Policy framework and implementation approach

South Korea's economic security measures mirror much of Japan's Economic Security Promotion Act, but without Japan's explicit emphasis on the 'stable provision of specified essential infrastructure services', or its focus on potential compromise arising from foreign legislation or external directives. Seoul concentrates on protecting the competitiveness of its high-tech manufactures and preventing any leakage of critical technologies to foreign competitors, rather than the risk from foreign technology vendors embedded in its critical infrastructure. That divergence reflects differing economic exposure. Japan's commercial ties with China are significant but more diversified, giving Tokyo greater latitude to

pursue a securitised approach, while South Korea remains deeply dependent on China for critical inputs—especially in semiconductors, raw materials and intermediate goods—making it far more vulnerable to supply-chain disruptions.

South Korea manages the risk of foreign owned, controlled or influenced technology vendors through a multilayered framework that prioritises integrity, resilience and trustworthiness rather than explicitly naming countries. Legislative instruments such as the Telecommunications Business Act and the Critical Information Infrastructure Protection Act[121] empower authorities to scrutinise and, where necessary, restrict technology in critical network layers and essential systems. Regulators are empowered to designate critical information infrastructure in sectors associated with national security and vital public services and, where designated, operators must submit annual security plans, conduct vulnerability assessments, implement robust access controls and address regulatory remediation requests.

That said, the Critical Information Infrastructure Protection Act appears to be focused on ensuring that vendor equipment used by designated critical information infrastructure meets international cybersecurity standards designed to mitigate 'network intrusions'. And those kinds of certifications can't predict whether a vendor will at some later stage be forced to take direction from security services of a foreign state.

The focus on cybersecurity is understandable, given the threat from North Korean cyber actors. The 2024 National Cybersecurity Strategy[122] identifies North Korea 'as the biggest threat to ROK cybersecurity', noting that in the previous year the country 'launched 1.3 million cyberattacks per day on ROK public institutions alone'. The strategy also proposed minimum security requirements for national infrastructure systems and designating trustworthy product and parts suppliers. Subsequently, in May 2024, the government formed a council to secure infrastructure across 10 sectors covering government facilities, water, transport, energy, information and communication, and maritime.[123] The government cited the risk of cyberattacks and foreshadowed cooperation with the US and Japan. It isn't known whether that effort will be sustained under the new government. So far, there have been no reversals or reforms on those fronts, although the longer term direction under the new government remains to be seen.

Compliance is enforced through a 'security-by-certification' model that combines domestic and international standards. Public-sector procurement rules contain unique security standards, often posing challenges even for close partners. For example, under the Cloud Security Assurance Program,[124] certified cloud services for government use must host all system components, personnel and data (including backups) in South Korea and meet local encryption standards; major foreign providers have begun qualifying, including Microsoft's Azure and AWS.[125] For on-premise and network security products, Korea is transitioning from the National Intelligence Service (NIS)[126] to the Security Verification Scheme (SVS).[127] SVS verifies products against Korean security criteria and requires certain solutions, such as virtual private networks, to use cryptography validated under the Korea Cryptographic Module Validation Program, which is creating *de facto* barriers for vendors unable to meet those technical and operational thresholds.[128] Agencies are also increasingly cautious with AI services; several ministries have blocked tools such as DeepSeek,[129] and the NIS has worked on guidelines for the secure use of generative AI.[130] Again, this affects all of the ROK's trading partners, including the US, which has reportedly raised concerns without formal resolution.

Oversight is distributed across specialised authorities: the Ministry of Science and ICT and the Korean Internet and Security Agency handle certifications and audits; the NIS defines encryption requirements and conducts product testing; and the Ministry of Trade, Industry and Energy, in conjunction with the NIS, oversees strategic technology investments and supply-chain resilience.[131] Cross-sectoral monitoring ensures that vendors remain compliant over time, and escalation or disengagement can be triggered if risks emerge. While formally country-neutral, those requirements function as effective filters against vendors potentially subject to foreign state influence.

Complementing those measures, the 2023 Framework Act on Supply Chain Stabilisation and related economic security legislation designate 'economic security items', mandate resilience plans and incentivise domestic production and supply-chain diversification.[132] By integrating cybersecurity standards, procurement rules and economic security policies, South Korea creates a cohesive ecosystem that raises entry thresholds for foreign vendors and mitigates exposure to coercion or technology leakage.

Part 3: 5G as an early test case for technology security frameworks

The rollout of 5G mobile networks from the late 2010s represented a step change over 4G, offering super-fast, high-bandwidth, low-latency connections capable of linking every device with a chip across the economy—including critical infrastructure. The 5G case demonstrates how a combination of technical architecture, supplier origin and national-security risk assessments can shape the deployment of critical infrastructure technologies in a contested geopolitical environment.

Divergent strategies, convergent outcomes: managing Chinese 5G vendors

Across the Indo-Pacific, countries adopted different strategies to manage Chinese 5G vendors, reflecting distinct threat perceptions, domestic industrial priorities and geopolitical considerations:

- *Australia* assessed that the security risks of Huawei and ZTE 5G equipment couldn't be mitigated, designating those companies as high-risk vendors and ultimately banning their involvement in national 5G networks [early, explicit, legalistic ban].
- *India* imposed procurement rules requiring telcos to source equipment only from vaguely defined 'trusted sources', with Chinese vendors never included [gradual exclusion via certification and procurement rules].
- *Japan* added opaque security requirements to public-sector and telco procurement, resulting in Chinese vendors being excluded from all mobile networks [exclusion through procurement guidelines and security incentives].
- *Singapore* enforced stringent performance, security and resilience standards for telecom equipment, ensuring that all licensees used non-Chinese vendors for core network infrastructure [performance-based standards ensured that sensitive network elements were insulated].
- *South Korea* imposed no regulatory restrictions, although only one telco selected a Chinese vendor; the largest operators chose non-Chinese suppliers [market-led approach with minimal government intervention].

Two challenges defined the 5G security landscape. First, unlike 4G networks—in which sensitive information and core functions were sealed off—5G networks are highly virtualised, with connections operating at net speed within a single cloud. Vendors supplying and maintaining 5G equipment thus gained potential access to the entire telecommunications backbone, requiring a high degree of trust. Second, the leading 5G vendors were Chinese—Huawei and ZTE—offering high-quality, lower cost equipment. By the late 2010s, China had also become the dominant cyber threat in the region; its domestic laws enable the CCP to compel companies to cooperate with state security agencies.

Australia responded first, in 2018, with the most robust and legally unambiguous approach. Reforms required telcos to notify the government of any system changes that could compromise network security. The Australian Signals Directorate determined that no combination of technical controls could sufficiently mitigate risks from Huawei or ZTE, leading to a ban on vendors 'likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law'.[133] The policy, although described as 'country-agnostic', triggered strong Chinese protests and later contributed to broad export restrictions on Australia.

India acted more gradually. Following a border skirmish with China in June 2020, the government issued the National Security Directive on Telecommunications mandating that providers purchase only certified 'trusted products' from 'trusted sources'.[134] Chinese vendors were excluded from approval processes and never listed. By 2022, India's major operators had phased out Chinese 5G components in favour of Ericsson, Nokia and Samsung.[135] Huawei's attempts to assuage security concerns through 'no backdoor' agreements were rejected due to the overarching Chinese legal environment. By March 2025, India had deployed more than 469,000 5G base stations to 250 million subscribers without Chinese vendor involvement.[136]

Japan pursued a stealthier approach. In December 2018, revised internal procurement guidelines barred Chinese-made computers, servers and telecom equipment for central government agencies and the Japan Self-Defense Force.[137] Coupled with spectrum allocation conditions and the 2022 5G Security Guidelines, those measures incentivised operators to select non-Chinese suppliers while avoiding explicit bans. As a result, all four major operators partnered with Ericsson and Nokia.[138]

Singapore similarly achieved Chinese vendor exclusion without overt bans. Stringent performance, security and resilience requirements for 5G licensees, enforced by the Infocomm Media Development Authority and Cyber Security Agency, led operators to choose Ericsson and Nokia for core networks.[139] Limited use of Huawei and ZTE outside core infrastructure was permitted, maintaining the appearance of neutrality.

South Korea took a low-profile approach, imposing no regulatory restrictions. LG Uplus adopted Huawei equipment for its 5G base stations,[140] although major operators SK Telecom and KT selected non-Chinese suppliers for financial, technological and operational reasons. Security considerations appear to have played a secondary role, reflecting a careful balance between US security expectations and economic ties with China. By 2023, over 70% of LG Uplus's 5G base stations used Huawei technology.

A separate ASPI report, Part II in this series and informed by this five-country comparative analysis, provides policy and governance options for governments and industry to mitigate risks and strengthen trusted technology ecosystems.

Appendix 1: Comparative overview of legislative and regulatory frameworks

AUSTRALIA		
Domain	**Legal/regulatory instrument**	**Effect**
Telecommunications	*Telecommunications Act 1997* Telecommunications Sector Security Reforms[141] *Sections 313–315*	• Minister for Home Affairs can direct carriers or providers to cease using or supplying specific services deemed prejudicial to security. • Directions issued based on security advice from ASIO. • Legally binding compliance requirement for affected telecommunications providers.
Cybersecurity	*Cybersecurity Act 2024*[142]	• Establishes a review board with powers to investigate major cyber incidents, mandate security standards for internet-connected products, and require ransomware payment reporting by large businesses. • Expands Security of Critical Infrastructure Act coverage to critical business data systems, with penalties for noncompliance, and imposes enhanced cyber obligations on 'systems of national significance'. • Encourages voluntary cyber incident reporting to the Australian Signals Directorate through legal protections limiting enforcement use of shared information.
Protective security	Protective Security Policy Framework[143]	• Issues legally binding protective security directions to 100 federal departments and agencies. • Provides 'better practice' guidance for an additional 90 Commonwealth corporate entities and wholly owned companies. • Establishes baseline requirements for physical, personnel and information security to safeguard government resources and operations.
Critical infrastructure	*Security of Critical Infrastructure Act 2018*[144]	• Requires responsible entities for critical infrastructure assets to maintain and comply with a risk-management program covering physical, cyber, supply-chain and personnel security. • Imposes additional reporting, incident notification and system security requirements on designated 'systems of national significance'. • Grants the minister and relevant agencies authority to issue binding directions or take direct action to protect assets against serious cyber or security threats.
Data and privacy	*Australian Privacy Act 1988*[145]	• Entities must ensure that overseas recipients handle personal information in line with Australian Privacy Principles, with the original entity remaining accountable. • Entities must implement reasonable measures to protect data from misuse, interference, loss and unauthorised access or disclosure. • Enables the Office of the Australian Information Commissioner to investigate, audit and impose civil penalties for breaches, including those involving foreign vendors.
Economic security	*Foreign Acquisitions and Takeovers Act 1975*[146]	• Allows the Treasurer to block, impose conditions on or unwind foreign investments deemed contrary to the national interest (including national security). • Requires foreign investors to notify the Foreign Investment Review Boad of certain investments in sensitive sectors, including telecommunications and critical infrastructure. • Enables legally binding conditions to mitigate security risks and provides enforcement powers for breaches.

INDIA		
Domain	**Legal/regulatory instrument**	**Effect**
Telecommunications	2024 Critical Telecommunications Infrastructure Provisions[147]	• Allow government to designate telecom networks or components as critical telecommunications infrastructure subject to strict oversight. • Enable inspection of critical telecommunications infrastructure hardware, software and data at any time by government authorities. • Require prior approval for remote repairs or maintenance conducted outside India, enabling vetting and monitoring of critical network equipment.
	2020 National Security Directive on Telecommunication Sector[148]	• Establishes legal basis for India's 'trusted sources' regime. • Empowers India's National Security Council Secretariat to evaluate vendors and products for India's networks. • Enables cross-ministry coordination to collectively identify high-risk vendors and makes security vetting a precondition for market access to telecoms sector.
	2017 Mandatory Testing & Certification of Telecom Equipment (MTCTE)[149]	• Mandates pre-deployment testing and certification of telecom equipment by Telecommunication Engineering Centre (TEC) accredited labs. • Requires separate certification of each model and version to prevent unauthorised equipment variants. • Prohibits the sale or integration of non-certified products in public networks.
Cybersecurity	2013 National Cyber Security Strategy[150]	• Introduces a proactive principle of embedding cybersecurity from the outset in public and private digital systems. • Presents a unified strategy for securing ICT supply chains across procurement and domestic product development. • Establishes sectoral computer security incident response teams, promotes an indigenous security technology ecosystem and enhances coordination mechanisms to protect critical information infrastructure.
	2000 Information Technology Act[151] *Sections 70, 70A, 70B*[152]	• Government can declare any computer resource a 'protected system', triggering mandated security practices and penalties for unauthorised access. • Government may appoint a national agency responsible for protecting critical information infrastructure, including oversight, R&D and operational coordination. • CERT-In is empowered to issue mandatory directions to service providers, intermediaries, data centres and corporates to enforce cyber incident reporting, compliance and security standards. Noncompliance can attract penalties.
	Software Bill of Materials (SBOM)[153]	• Promotes transparency by requiring public- and private-sector entities to maintain and disclose an SBOM for all products. • Improves the government's ability to detect hidden foreign-origin code and security flaws in critical software. • Enables quicker identification and remediation of security risks through detailed software component data.
Protective security	2018 Minimum Security Requirements of Department of Telecommunications Licences[154] *Section 2(c)xi, 2(c)xiii, 2(c)xxviii*	• Telecom licensees must apply rigorous vetting of vendors and personnel and maintain a security management policy aligned with departmental standards. • Licensees must conduct security audits of their telecom assets and embed audit and inspection rights over vendor facilities, supply chains and IT systems in contracts. • Noncompliance with those security policies and audit mandates may result in regulatory penalties or loss of licence.

INDIA		
Domain	**Legal/regulatory instrument**	**Effect**
Critical infrastructure	2015 Guidelines for Protection of Critical Information Infrastructure[155] *Sections 6.2.1, 6.2.4, 6.3.2, 7.2.1, 8*	• Critical information infrastructure operators are expected to identify all network assets, understand interdependencies and map their supply chains, including any foreign technologies in use. • Operators are advised to conduct systematic risk assessments, including the evaluation of third-party vendors and components against defined security controls. • Regulators may audit systems and recommend the removal or substitution of unsafe products. Those recommendations can be escalated into binding actions by regulators where necessary.
Data and privacy	2023 Digital Personal Data Protection Act[156] *Section 16(1)*	• Allows government to restrict cross-border data transfers and allows for data localisation mandates in designated sensitive areas. • Those provisions can apply indirect pressure on foreign tech vendors to store and process data in India or other approved jurisdictions.
Economic security	2020 Atmanirbhar Bharat ('Self-Reliant India') Initiative[157]	• Encompasses programs and incentives to boost domestic capacity in critical industries. • Offers production-linked incentives for telecom equipment manufacturing and endorses indigenous alternatives. • Aims to reduce long-term dependency on foreign vendors by developing competitive local suppliers.
	2020 Foreign Direct Investment Policy Restrictions[158] *Section 3.1.1*	• Mandate prior government approval for FDI from entities based in countries sharing land borders with India. • Prevent opportunistic takeovers, by allowing security agencies to veto investment by suspect entities.
	2017 Public Procurement (Preference to Make in India) Order[159]	• Mandates that central government entities prioritise goods, services and works meeting the minimum local content threshold in public procurement. • Ministries can define content requirements and certify suppliers as 'local' based on explicit local value-add criteria. • Vendors unable to meet the local content threshold are disqualified from receiving preference.

JAPAN		
Domain	**Legal/regulatory instrument**	**Effect**
National security	2022 National Security Strategy[160] *Pages 6–7, articles 3(ii), 3(iii), (3)V; page 30, articles 5(iii), 5(v)*	• Expands Japan's national security scope to include economic security. • Prioritises supply-chain resilience, tech self-reliance and countering economic coercion. • Links critical infrastructure and advanced tech threats to national security, driving stricter investment screening and export controls.
Telecommunications	1984 Telecommunications Business Act[161] *Article 9, 10(iii), 12(iv)*	• Requires all telecom service providers to register with the Ministry of Internal Affairs and Communication. • Extends authority to foreign providers without a Japan presence, requiring a local representative and compliance with Japanese law. • Ministry of Internal Affairs and Communications must refuse registration if requirements aren't met.
	2022 5G Security Guidelines[162] *Sections 5.1.6, 5.3.1., 5.3.2., 5.3.3, 5.5.1*	• Direct operators' 5G procurement practices, encouraging vendor trustworthiness assessments, supply-chain transparency, software security and multivendor use. • Embedded in licensing conditions and public procurement, resulting in *de facto* exclusion of high-risk vendors.
Cybersecurity	2021 Cybersecurity Strategy[163] *Page 30, section 3, Ensuring trustworthiness of security products & services*	• Sets national cyber-defence priorities and shapes sectoral security policies. • Emphasises supply-chain diversity and resilient system architecture in critical sectors. • Signals plans to certify trusted security and verification providers for government use.
	2023 Cybersecurity Strategic Headquarters—Guideline for establishing safety principles for ensuring cybersecurity of critical infrastructure[164] *Section 5.1.4. System acquisition, development & maintenance; section 5.1.2. Supplier management*	• Provides authoritative baseline cybersecurity guidance for Japan's 15 critical infrastructure sectors, including supply-chain risk management. • Directs critical infrastructure operators to identify mission-critical systems, assess potential vendor compromise impacts, and vet third-party suppliers. • Used by sectoral regulators as *de facto* requirements when reviewing or challenging high-risk vendor use.
	2019 METI Cyber/Physical Security Framework[165]	• Voluntary, risk-based framework to secure converged cyber–physical systems through a 'three-layer' trust model: organisational trust, cyber–physical interface trust, and data trustworthiness. • Advises evaluation of vendors and components at each layer to identify vulnerabilities. • Widely adopted across energy, manufacturing, transportation and other critical sectors.
	2020 (METI-MIC-NCO-Digital Agency) Information System Security Management and Assessment Program (ISMAP)[166]	• Voluntary cloud security certification requiring rigorous audits of provider controls, including subcontractor management and supply-chain security. • In practice, functions as a positive list, as government agencies procure only from ISMAP-certified providers. • High standards, aligned with ISO and domestic requirements, indirectly exclude high-risk foreign vendors.
	2024 METI Software Bill of Materials (SBOM) Initiative[167] *Page 10*	• Voluntary industry guidance promoting detailed software supply-chain inventories and SBOM adoption to identify vulnerable components quickly. • Encourages secure, verifiable software and transparency benchmarks to improve third-party risk visibility. • Indirectly discourages opaque, insecure or untrusted foreign software.

JAPAN		
Domain	**Legal/regulatory instrument**	**Effect**
Protective security	2024 Security Clearance System[168] *Introduced via the Utilisation of Important Economic Security Information Act*[169]	• Legally binding national-security clearance for individuals in the public and private sectors handling sensitive economic security information. • Enables secure sharing with trusted stakeholders while excluding personnel with significant foreign ties from sensitive projects. • Restricts foreign nationals or those with major overseas connections from roles involving security information.
Critical infrastructure	2024 Essential Infrastructure System & Required Information[170] *Articles 49–59 of ESPA (Chapter III)*	• 'Specified essential infrastructure providers' must notify the competent minister before major system upgrades or procurement of critical equipment/software. • Mandatory disclosure of vendor, product details, supplier ownership, country of origin, foreign ties, cybersecurity features and supply-chain routes. • Minister can block or modify high-risk configurations and disqualify vendors, effectively creating a pre-vetted 'positive list' of trusted suppliers.
Data and privacy	2003 Act on the Protection of Personal Information[171] *Chapter IV, Obligations of businesses handling personal information*	• Legally binding: regulates cross-border data transfers, requiring prior consent for non-whitelisted jurisdictions (e.g. EU, UK). • Mandates transparency and accountability in data use, with disclosure on protection measures. • Mitigates risk of sensitive data being sent to jurisdictions where it may be exposed to foreign government access.
Economic security	2022 Economic Security Promotion Act[172] (Chapter II)	• Legally binding: designates 'specified critical materials' essential to national security. • Offers subsidies and tax incentives for businesses that follow government-approved supplier diversification plans. • Encourages reduction of risky foreign supply dependencies through secure, diversified sourcing.
	1949 Foreign Exchange and Foreign Trade Act[173]	• Legally binding: requires prior notification and approval for foreign investors acquiring 1%+ stakes in Japanese companies in security-related sectors (threshold lowered from 10% in 2020). • Expanded scope to cover hi-tech, information processing, software development, telecoms and other sensitive industries. • Empowers authorities to block, modify or suspend transactions posing national-security risks.

SINGAPORE		
Domain	**Legal/regulatory instrument**	**Effect**
Telecommunications	1999 Telecommunications Act[174] *Sections 5, 26, 30, 31, 32–36*	• Legally binding: the Infocomm Media Development Authority (IMDA) can approve, suspend or revoke telecom operator licences and impose binding security and operational conditions. • Issues enforceable codes of practice and performance standards for equipment security and network resilience, with penalties for noncompliance. • Requires all telecom equipment to be registered and approved via the IMDA Equipment Registration and Approval Scheme, enabling vetting and exclusion of high-risk vendor products.
	2019 Infocomm Media Development Authority Policy[175] *Page 29, points 116–118, Network design and resilience*	• Requires operators to design networks with built-in resilience and cybersecurity measures, meeting IMDA regulations and international standards. • Mandates vendor equipment vetting for performance, reliability and compliance with service quality, resilience and security requirements.
	IMDA Equipment Registration and Approval Scheme[176] *Sections 2.1, 2.4, 3.1 and IMDA Equipment registration overview*	• Requires all telecom equipment to be registered and type-approved by IMDA before sale or use. • Ensures compliance with national technical and security standards, enabling IMDA to reject or revoke insecure or noncompliant equipment.
Cybersecurity	2018 Cybersecurity Act[177]	• Requires critical information infrastructure owners to secure systems, including those managed by third-party vendors, and comply with incident reporting and relevant codes of practice. • Holds operators accountable for vendor-related risks, indirectly managing high-risk vendor involvement.
	2024 Cybersecurity Amendment Act[178]	• Requires providers of essential services using third-party-owned critical information infrastructure to secure legally binding cybersecurity commitments from vendors. • Grants authority to terminate noncompliant third-party systems; extends oversight to FDI, entities of special cyber interest and offshore critical information infrastructure.
	2022 Critical Information Infrastructure Supply Chain Program[179] *Section 2.2.1–2.2.4 (Process for tracking vendors and performing risk analysis)*	• Provides structured vendor mapping and risk assessment for critical information infrastructure. • Evaluates vendor dependency, compromise impact and access levels to identify critical supply-chain risks.
	2022 Cyber Trust and Cyber Essentials Marks[180]	• Require vendors to obtain cybersecurity certification before participating in sensitive government contracts. • Standards to be expanded in 2025 to include emerging technologies, raising baseline requirements.
	2020 Third-Party Management[181] *Under 2001 Instruction manual for infocomm technology and smart systems (previously known as IM8)*	• Mandatory risk identification, assessment and mitigation for outsourcing in public-sector ICT projects. • Vendors subject to enhanced due diligence and stricter contractual and security clearance requirements. • Requires regular audits and ongoing monitoring of third-party performance and compliance.

SINGAPORE		
Domain	**Legal/regulatory instrument**	**Effect**
Protective security	2017 Infrastructure Protection Act[182]	• Requires designated critical infrastructure owners/operators to adopt a risk-based security-by-design process and submit a security plan covering all relevant risks. • Technology and vendor risks must be addressed if they affect infrastructure resilience, including preconstruction and major upgrades. • Sectoral regulations specify technical measures, as the framework sets only holistic, non-technical requirements.
Critical infrastructure	(New) Digital Infrastructure Act[183] *(to be introduced in 2025)*	• Will require critical digital infrastructure providers to meet baseline resilience and security standards, including vendor and supply-chain risk assessments. • Mandates strong contractual controls, secure configurations, vulnerability testing, access restrictions, incident reporting and business continuity plans. • Builds on IMDA's current voluntary advisory guidelines, making them legally binding once enacted.
	2025 IMDA Advisory Guidelines on Resilience and Security of Cloud Services[184]	• Encourage cloud providers to adopt robust third-party risk management, secure configurations and regular security testing of vendor-supplied systems. • Promote strong logging, monitoring and auditing to detect and respond to unauthorised activity. • Support best practice for supply-chain security in critical infrastructure through voluntary take-up.
	2025 IMDA Advisory Guidelines on Resilience and Security of Data Centres[185]	• Encourage data centre operators to vet employees and third-party vendors through background checks and enforce compliance with security policies. • Require regular review of vendor contracts and integration of security-by-design in new systems or services. • Strengthen supply-chain oversight to reduce risks from high-risk vendors across procurement and operations.
Data and privacy	2012 Personal Data Protection Act[186]	• Requires third-party vendors handling personal data to implement reasonable security arrangements, meet the Act's contractual and due diligence obligations and comply with cross-border transfer rules. • Mandates breach notification to authorities.
Economic security	2021 Monetary Authority of Singapore Technology Risk Management Guidelines[187] *Sections 4, 4.2.1, 5.3.1, 5.3.2*	• Require financial institutions to assess IT vendors' cybersecurity and monitor third-party access. • Mandate vendor risk ratings, dependency classification and secure application programming interface, software acquisition and system resilience practices. • Enforce vulnerability management, secure development and access control measures.
	Significant Investments Review Act[188]	• Establishes a mandatory investment screening regime for transactions involving designated critical entities to safeguard national security. • Empowers the Ministry of Trade and Industry to require pre-approval or notification for ownership changes and substantial investments and 'call in' and review completed transactions that may threaten Singapore's national security. • Complements existing sector-specific regulations in telecoms, media, utilities and other critical sectors by providing a holistic mechanism to assess and mitigate risks from foreign investments in critical infrastructure and technologies.

SOUTH KOREA		
Domain	**Legal/regulatory instrument**	**Effect**
Telecommunications	1983 Telecommunications Business Act[189] *Articles 17, 20, 62.1*	• Ministerial approval required for telco expansion into equipment manufacturing or infrastructure, enabling screening of foreign vendors. • Prior approval mandated for installation or updates to key telecom equipment to oversee security, origin and integrity. • Noncompliance punishable through registration revocation or market-access restrictions.
Cybersecurity	2019 National Cybersecurity Strategy[190] *Strategic tasks: 1 (all), 3.2, 4.1, 4.2*	• Sets strategic direction for agencies and critical infrastructure operators, promoting life-cycle security controls, voluntary equipment assessments and security-by-design for ICT products. • Encourages early security planning, inspection schemes for equipment vulnerabilities and procurement reforms prioritising performance over price. • 2024 updates propose designating trusted products and sources and introduce minimum security requirements for national infrastructure.
	2001 Act on the Promotion of Information and Communications Network Utilisation and Information Protection[191] *Articles 3, 4, 8, 9, 47*	• Imposes mandatory technical and managerial security obligations for secure network operations, product standardisation and certification. • Functions as compliance thresholds that can indirectly exclude noncompliant or insecure foreign technologies.
	1999 ISO15408 (Common criteria for IT security evaluation)[192] 2005 ISO18045 (Evaluation methodology for IT security)	• Establish legally binding international technical standards (e.g. ISO/IEC 15408, 18045) for evaluating and certifying ICT product and system security. • Embed accredited testing and certification into telecom and critical infrastructure regulations, enabling validation of vendor security claims and exclusion of non-certified products.
	2014 NIS Security Evaluation Scheme (SES)[193] *Additional domestic requirements added to common criteria certification*	• Imposes mandatory domestic cybersecurity and conformity assessments for ICT products in public-sector and national infrastructure, in addition to common criteria certification. • Requires compliance with Korean encryption standards (e.g. ARIA, SEED), effectively excluding vendors unable to integrate approved cryptographic modules.
	2016 Cloud Security Assurance Program (CSAP)[194] *Articles 14, 15, 23, 46*	• Requires CSAP-certified cloud service providers to localise all data, backups and management operations in South Korea, reducing foreign access risks. • 2023 update introduced a three-tier certification restricting foreign vendor participation in government projects by service sensitivity, with physical infrastructure separation for mid/high-tier projects. • Mandates use of approved Korean encryption algorithms (e.g. ARIA, SEED) to meet national-security standards.
	2023 NIS Security Verification Scheme (SVS)[195]	• The 2014 NIS Security Evaluation Scheme (SES) was updated to SVS 3.0 in August 2023 • Eased requirements in some parts for security certification, including domestic common criteria mandates and encryption algorithms, even though it maintains mandatory domestic cybersecurity and conformity assessments for ICT products in the public sector.
Protective security	Only partially covered in Special Act	

SOUTH KOREA		
Domain	**Legal/regulatory instrument**	**Effect**
Critical infrastructure	2001 Critical Information Infrastructure Protection Act[196] *Articles 5, 5.2, 6, 8, 9*	• Requires operators of designated critical information infrastructure to implement technical and physical protection measures and undergo periodic compliance verification. • Mandates government-led or certified third-party security assessments, enabling close scrutiny of critical systems. • Oversight mechanisms allow authorities to indirectly restrict high-risk foreign vendors from participating in critical information infrastructure operations.
Data and privacy	2011 Personal Information Protection Act[197]	• Legally binding: obligations apply to all entities that process the personal data of Korean citizens. • Enables government to restrict cross-border data transfers, mandate oversight of outsourced processors, and enforce corrective measures or administrative fines for noncompliance. • 2023 amendments shifted the emphasis from criminal penalties to economic sanctions. • Offers an indirect framework to manage vendor risks in data-sensitive critical infrastructure.
Economic security	2022 Act on Special Measures for Strengthening and Protecting Competitiveness of National High-Tech Strategic Industry[198] *2022 Enforcement decree*	• Legally binding: requires government pre-approval for export, foreign merger, acquisition or joint ventures involving designated high-tech strategic technologies. • Entities handling those technologies must implement mandatory safeguards (restricted zones, access control, real-time monitoring and physical security) to prevent leakage or misuse. • Employers must enforce confidentiality and personnel exit protocols. Severe penalties for unauthorised acquisition, use or disclosure.
	2023 Framework Act on Supply Chain Stabilisation Support for Economic Security[199] *Preceded by the 2022 Basic Act on Supply Chain Stabilisation. Enacted 2024* *Articles 13, 14–17, 18-(22)26, 27–36, 37–42*	• Legally binding: establishes early-warning systems to detect foreign dependency risks in designated 'economic security items', including critical technologies and services vulnerable to external disruption. • Provides financial incentives and government support to diversify import sources and reduce reliance on specific foreign countries. • Enables information sharing with certified 'stabilisation leading business entities' committed to lowering foreign dependence and establishes the Supply Chain Resilience Fund to support domestic production capacity and strategic tech development.

Notes

1 Cabinet Secretariat, *System for ensuring stable provision of specified essential infrastructure services under the Economic Security Promotion Act (briefing material)*, Japanese Government, 1 August 2025, online.

2 Simeon Gilding, *De-risking authoritarian AI: a balanced approach to protecting our digital ecosystems*, ASPI, Canberra, July 2023, online.

3 Mitchell Clark, Alex Heath, 'TikTok's parent company accessed the data of US journalists', *The Verge*, 23 December 2022, online.

4 Dakota Cary, Kristin Del Rosso, *Sleight of hand: how China weaponizes software vulnerabilities*, Atlantic Council, 6 September 2023, online.

5 Antonia Hmaidi, 'Huawei is quietly dominating China's semiconductor supply chain', *MERICS*, Mercator Institute for China Studies, 9 April 2024, online.

6 Rush Doshi, *China's new national security laws: risks to American companies and conflicts of interest*, Council on Foreign Relations, 24 September 2024, online.

7 'Responsible value chain', ASML, no date, online.

8 'Xi's policies serve strategic national goals beyond growth', MERICS, Mercator Institute for China Studies, 12 October 2023, online.

9 Peter Harrell, *Managing the risks of China's access to US data and control of software and connected technology*, Carnegie Endowment for International Peace, 30 January 2025, online.

10 European Union, *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)* [2021] OJ L 206, 11 June 2021, online.

11 Cybersecurity and Infrastructure Security Agency, 'AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations', US Government, 17 December 2020, online.

12 Gregory C Allen, 'Across drones, AI, and space, commercial tech is flexing military muscle in Ukraine', Center for Strategic and International Studies, 19 July 2023, online.

13 Jill C Gallagher, *Secure and Trusted Communications Networks Reimbursement Program: frequently asked questions*, Congressional Research Service, US Congress, 30 January 2025, online.

14 Federal Communications Commission, 'Wireline Competition Bureau announces availability of additional funding for the Rip-and-Replace Program', public notice DA 25-342, US Government, 15 April 2025, online.

15 'Huawei lobbyists banned from accessing European Parliament after bribery arrests', *Independent*, 14 March 2025, online.

16 Department of Home Affairs (DHA), 'Factsheet—Technology Vendor Review Framework', Australian Government, 2024, online.

17 'No need to choose China or US: Howard', *Sydney Morning Herald*, 2 October 2012, online.

18 Australian Government, *Defending Australia in the Asia Pacific Century: Force 2030*, 2009, 34, online.

19 Will Glasgow, 'China's warning to Australian delegation over "two-faced" policy in "security-focused" Beijing talks', *The Australian*, 20 September 2025, online.

20 'Canberra cannot butter bread on both sides', editorial, *China Daily.com*, 16 September 2025, online.

21 Foreign Investment Review Board, *Australia's Foreign Investment Framework*, Australian Government, 14 March 2025, online.

22 DHA, *Foreign ownership, control or influence (FOCI) risk assessment guidance*, Australian Government, 5 March 2025, online.

23 Critical Infrastructure Security Centre, *Security of Critical Infrastructure Act 2028 (SOCI)*, Australian Government, 27 August 2024, online.

24 Critical Infrastructure Security Centre, 'Critical Infrastructure Risk Management Program—Part 2A *Security of Critical Infrastructure (SOCI) Act 2018* factsheet', Australian Government, April 2025, online.

25 Clare O'Neil, 'Protecting Australia's critical infrastructure assets', media release, 8 September 2023, online.

26 See DHA, 'PSPF annual release 2025', Australian Government, 24 July 2025, online. The PSPF applies to 97 non-corporate Commonwealth entities and is considered better practice for 71 Commonwealth corporate entities and 18 wholly owned Commonwealth companies.

27 See DHA, 'PSPF Direction 001-2024', Australian Government, 5 July 2024, online; DHA, 'PSPF Direction 002-2024', Australian Government, 5 July 2024, online; DHA, 'PSPF Direction 001-2025', Australian Government, 5 February 2025, online. In April 2023, the government banned TikTok on non-corporate Commonwealth entity devices due to significant security and privacy risks, allowing use only on approved stand-alone devices with mitigations. In July 2024, three directions were issued to manage risks from foreign owned, controlled or influenced technology: (1) identify, monitor, and report FOCI risks in technology assets to Home Affairs; (2) conduct technology asset stocktakes, prepare risk management plans and address supply-chain vulnerabilities; and (3) share cyber threat intelligence with the Australian Signals Directorate. In February 2025, a further direction prohibited all DeepSeek AI products and services on Australian Government systems, citing unacceptable security risks.

28 Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cwlth), second reading, 9 October 2024, online.

29 *Senate Hansard*, 25 November 2024, vol. 28074, Australian Parliament, online.

30 Australian Security Intelligence Organisation, *Annual report 2021–22*, Australian Government, 2022, 5, online.

31 Jonathan Mills, 'Bills digest no. 29, 2024–25: Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024', Parliamentary Library, DHA, 13 November 2024, online.

32 'Explanatory memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024', Australian Parliament, 2024, 36, online.

33 DHA, *Technology Vendor Review Framework*, Australian Government, 20 December 2024, online.

34 Simeon Gilding, 'Tiptoeing around China: Australia's framework for technology vendor review', *The Strategist*, 16 January 2025, online.

35 DHA, *Foreign ownership, control or influence (FOCI) risk assessment guidance*, Australian Government, 5 March 2025, online.

36 See DHA, *Foreign ownership, control or influence (FOCI) risk assessment guidance*. The process has two stages: (1) a vendor review questionnaire to determine whether a FOCI risk assessment is required, covering factors such as potential for foreign government data access, prior Australian cyber attributions, evidence of economic coercion or IP theft, state ownership or control, and politically exposed persons in leadership; and (2) a FOCI risk assessment, considering jurisdictional hazards, organisational exposure, FOCI activity risks and treatment options.

37 See Matthew Cranston, 'Dutton to force Chinese company to sell Darwin Port, Albanese agrees', *Australian Financial Review*, 4 April 2025, online. During the 2025 election campaign, Prime Minister Albanese matched the Opposition Leader's pledge to terminate the 2015 lease of the Port of Darwin to a Chinese company, calling it a strategic asset.

38 Foreign Investment Review Board, 'Announcement of reforms to Australia's Foreign Investment Framework', Australian Government, 1 May 2024, online.

39 S Jaishankar, 'Remarks by External Affairs Minister, Dr S Jaishankar at Nani Palkhivala Memorial Lecture "India and the World"', Ministry of External Affairs, Indian Government, 18 January 2025, online.

40 Chietigj Bajpaee, 'Modi's SCO summit visit shows China and India want to reset relations. But the "dragon–elephant tango" will be tough', Chatham House, 1 September 2025, online.

41 Jaishankar, 'Remarks at the Nani Palkhivala Memorial Lecture "India and the World"'.

42 Jaishankar, 'Remarks at the Nani Palkhivala Memorial Lecture "India and the World"'.

43 Jaishankar, 'Remarks at the Nani Palkhivala Memorial Lecture "India and the World"'.

44 'About us', Make in India, 18 August 2025, online.

45 Prime Minister's Office, *Atmanirbhar Bharat: The Foundation of a Strong and Developed India*, Indian Government, 15 August 2025, online.

46 Ministry of Electronics and Information Technology, Government of India, "Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order," Press Information Bureau, 29 June 2020, online.

47 'India can even do digital strike: IT Minister Ravi Shankar Prasad on banning 59 Chinese apps', *India Today*, 2 July 2020, online.

48 Telecommunication Engineering Centre, 'Mandatory testing and certification of telecom equipment (MTCTE)', Indian Government, 2025, online.

49 Interview with Colonel KPM Das, Adjunct Fellow at Takshashila Institution, 21 April 2025.

50 The government initially briefed the media that there would be a blacklist, but that was dropped. Sujan Chinoy, 'Boost for India's telecom security: new directive cuts reliance on foreign equipment, including from dubious sources', *Times of India*, 28 December 2020, online.

51 While the 'trusted products' policy isn't retrospective, the government has asked telcos to assess and report on legacy equipment in their networks from 'non-trusted sources', to enable it to evaluate the potential costs of replacing that equipment. ZTE and (reportedly) Huawei are exploring local joint ventures to manufacture telecommunications equipment, and it's possible the government will be open to that. One official clarified that companies can manufacture those kinds of products in India but their equipment can't be deployed in Indian networks.

52 Muntazir Abbas, Ashutosh Kumar, 'India to bar Chinese vendors, mandate "trusted" IoT modules', *Economic Times (Telecom)*, 7 December 2024, online.

53 Abbas & Kumar, 'India to bar Chinese vendors, mandate "trusted" IoT modules'; Aditya Kalra, 'India's alarm over Chinese spying rocks the surveillance industry', *Reuters*, 31 May 2025, online; 'India moves to curb imports of Chinese solar cells', *Asia Financial*, 11 December 2024, online.

54 Kalra, 'India's alarm over Chinese spying rocks the surveillance industry'.

55 Ruta Deshpande, 'Chinese espionage fears trigger tech crackdown: India imposes tough new rules on CCTV industry', *DeftechTimes,* 28 May 2025, online.

56 'About us', Make in India, 18 August 2025, online.

57 '"China part of concern": India's CCTV crackdown over spying fears hits global giants like Hikvision, Xiaomi', *Business Today*, 28 May 2025, online.

58 Uma Gupta, 'India creates non-tariff barrier for Chinese solar products', *PV Magazine*, 30 April 2024, online.

59 'Government working on replicating trusted source product rules for power equipment: NCSC', *Telecom Economic Times*, 9 January 2025, online.

60 Sylvia Malinbaum, *India's quest for economic emancipation from China*, Asie.Visions no. 145, IFRI, January 2025, online.

61 Malinbaum, *India's quest for economic emancipation from China*.

62 The restrictions targeting Chinese solar panels from 2026 were reportedly a re-announcement of an earlier initiative that was not implemented due to the lack of local manufacturing capacity at competitive prices. See 'The import restrictions on solar PV cells', *Vajiram & Ravi*, 10 April 2024, online.

63 Naman Jain, Surendar Singh, 'India's big bet on supply chain realignment', *Policy Circle*, 26 July 2025, online.

64 Shinzo Abe, 'Policy speech by Prime Minister Shinzo Abe to the 183rd session of the Diet', Japanese Government, 28 February 2013, online.

65 Cabinet Secretariat, *National Security Strategy* (provisional translation), Japanese Government, 17 December 2013, online.

66 Ministry of Foreign Affairs, *National Security Strategy (NSS)*, Japanese Government, 16 December 2022, online.

67 Shiro Armstrong, *Economic security in Japan: evolution, context and emerging questions*, RIETI discussion paper series 24-E-083, Research Institute of Economy, Trade and Industry, December 2024, online.

68 Foreign Exchange and Foreign Trade Act (外国為替及び外国貿易法, Act no. 228 of December 1, 1949), translated 4 March 2025, online.

69 Ministry of Foreign Affairs, *National Security Strategy (NSS)*, Japanese Government, 16 December 2022, online; Armstrong, *Economic security in Japan: evolution, context and emerging questions*.

70 Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures (tentative translation), Act no. 43 of 18 May 2022, online; Takashi Suzuki, 'Exploring Japan's Economic Security Promotion Act', *Asia Business Law Journal* (expert briefing), Law.asia Limited, 25 March 2025, online; Cyber Security Division, *The Cyber/Physical Security Framework: to ensure trustworthiness of a new type*

of supply chain in 'Society 5.0', version 1.0, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry (METI), Japanese Government, 18 April 2019, online.

71 Cyber Security Division, *The Cyber/Physical Security Framework: to ensure trustworthiness of a new type of supply chain in 'Society 5.0'.*

72 National Center of Incident Readiness and Strategy, 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」[Agreement on the procurement policy and procedures for the procurement of national goods, etc. or services], Japanese Government, 10 December 2018, online.

73 Prime Minister's Office, 'Opening ceremony of National Cybersecurity Office [provisional translation]', Japanese Government, 1 July 2025, online.

74 Foreign Exchange and Foreign Trade Act (外国為替及び外国貿易法, Act no. 228 of December 1, 1949), translated 4 March 2025, online.

75 Recommended as best practice but not mandatory for regional governments and the private sector. Information System Security Management and Assessment Program (ISMAP), Japanese Government, operated by the Cabinet Cyber Security Center, Digital Agency, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry, supported by the Information-technology Promotion Agency, online.

76 ISMAP Steering Committee, *ISMAP Cloud Service Registration Rules*, ISMAP portal, 3 June 2020, last revised 1 November 2022, page.1, online.

77 Cabinet Secretariat, 'System for ensuring stable provision of specified essential infrastructure services under the Economic Security Promotion Act (briefing material)', Japanese Government, 1 August 2025, online.

78 Cabinet Secretariat, 'Summary of the Act on the Protection and Utilization of Critical Economic Security Information', Japanese Government, May 2024, online.

79 Jun Suzuki, 'Japan legal update: establishment of a security clearance system in the economic security sector', *AMT Legal*, 16 October 2024, online.

80 This is expected to grow when those obligations are extended to providers in the port and harbour transportation sector in November 2025. Cabinet Office, 'System for ensuring stable provision of specified essential services under the Economic Security Promotion Act (briefing material)'.

81 Taku Matsumoto, Masato Ishikawa, 'Japan legal update: updates of the Economic Security Promotion Act', *Anderson Mori & Tomotsune*, 13 March 2024, online.

82 Cabinet Secretariat,' System for ensuring stable provision of specified essential infrastructure services under the Economic Security Promotion Act (briefing material)'.

83 Cabinet Secretariat, 'System for ensuring stable provision of specified essential infrastructure services under the Economic Security Promotion Act (briefing material)', 10.

84 Interview with Professor Kazuto Suzuki, Professor of Science and Technology, Graduate School of Public Policy, University of Tokyo, 1 May 2025; interview with Dr Akira Igata, Project Lecturer at the Research Center for Advanced Science and Technology, University of Tokyo, 2 May 2025.

85 In May 2024, to facilitate these kinds of discussions (and no doubt impose formal security obligations on their participants), the government introduced a security clearance system to grant clearances to eligible officials and private individuals for classified information on critical infrastructure and product supply chains. By bringing Japan into line with the information protection practices of partner countries, the new system is also designed to enable information exchange and joint research on critical technologies. 'Summary of the Act on the Protection and Utilization of Critical Economic Security Information', *Japanese Law Translation*, no date, online; Kosuke Iwamoto, 'New law for boosting Japan's economic security to enhance international collaboration; impacts on personnel to be considered', *Japan News*, 11 May 2024, online.

86 'Singapore—trade (% of GDP)', *Trading Economics*, online.

87 Ministry of Defence, 'Total Defence strengthened with addition of Digital Defence as the sixth pillar', Singapore Government, 15 February 2019, online.

88 Ministry of Finance, 'C. advancing our growth frontier', Budget statement, Singapore Government, 2025, online.

89 Muhammad Faizal Abdul Rahman, 'As cyber threats grow, Singapore walks a careful line on identifying state actors', S Rajaratnam School of International Studies, 29 July 2025, online.

90 Louise Marie Hurel, 'What Singapore's first public cyber attribution tells us', Royal United Services Institute, 30 July 2025, online.

91 Singapore Government Technology Agency (GovTech), 'Government Zero Trust Architecture (GovZTA)', 16 May 2023, online.

92 Ministry of Defence, 'Total Defence strengthened with addition of Digital Defence as the sixth pillar'.

93 Koh Wan Ting, 'DBS, Citibank outages caused by cooling system "technical issue" at data centre', *Channel NewsAsia*, 16 October 2025, online.

94 Cyber Security Agency of Singapore, 'Cybersecurity Act', Singapore Government, 2 April 2025, online.

95 Janil SM Puthucheary, Senior Minister of State for Communications and Information, closing speech for second reading of Cybersecurity (Amendment) Bill, Cyber Security Agency of Singapore, 7 May 2024, online.

96 Singapore Cyber Security Agency and Boston Consulting Group, 'Critical Information Infrastructure Supply Chain Programme—a national effort in managing cyber supply chain risks', June 2023, online.

97 William Yuen Yee, 'Singapore's new investment screening law', Lawfare Institute, 9 July 2024, online.

98 Monetary Authority of Singapore, *Technology risk management guidelines*, Singapore Government, 18 January 2021, online.

99 Monetary Authority of Singapore, *Guidelines on outsourcing (financial institutions other than banks)*, Singapore Government, January 2025, online.

100 Infocomm Media Development Authority (IMDA), 'Equipment registration', Singapore Government, 28 August 2024, online.

101 Ministry of Digital Development and Information, 'New Digital Infrastructure Act to enhance resilience & security of digital infrastructure & services', Singapore Government, 1 March 2024, online; Ministry of Communications and Digital Infrastructure, 'Summary of announcements under Smart Nation 2.0', Singapore Government, 1 October 2024, online.

102 Yeo Han-Koo, 'Is South Korea de-risking?', Peterson Institute for International Economics, 26 January 2024, online.

103 'South Korea—trade (% of GDP)', *Trading Economics*, online.

104 Presidential Office (National Security Office), 국가 사이버안보 전략 [*National Cybersecurity Strategy*], ROK Government, 1 February 2024, 14, online. Translation note: quoted phrase '년 수립된 전략에는 우리나라의 가장 큰 실제적 위협인 북한의사이버위협에 대한 직시 rendered as 'the 2019 strategy lacked a direct recognition of our country's greatest real threat, North Korea's cyber threat.'

105 Hyunsu Yim, 'South Korean military suspends loudspeaker broadcasts aimed at North Korea', *Reuters*, 11 June 2025, online.

106 Moksh Suri, Abhishek Sharma, 'South Korea's economic security dilemma', *The Diplo*mat, 25 January 2025, online.

107 Speculation that US–ROK relations were heading for rough times under the Trump administration haven't yet come to pass; indeed, the new centre-left government reached a trade deal with the administration in late July. Pak Yiu, Kim Jaewon, 'Trump says South Korea has secured US trade deal with 15% tariff', *Nikkei Asia*, 31 July 2025, online.

108 Seo Ji-Eun, 'New Korean president vows to pursue "pragmatic" foreign policy based on alliance with the US', *Korea JoongAng Daily*, 4 June 2025, online

109 Transcript from 'Statesmen's Forum: his Excellency Lee Jae Myung, President of the Republic of Korea' Center for Strategic and International Studies, 25 August 2025, online.

110 Evans JR Revere, Kuyoun Chung, Ryan Hass, Chaesung Chun, 'How will South Korea navigate US–China competition in 2025?'2, convened by Andrew Yeo and Hanna Foreman, Brookings Institution, 22 January 2025, online.

111 Ronald Watkins, 'US think tank urges major troop cuts in South Korea', *The Defense Post*, 16 July 2025, online.

112 'South Korea exports by country', *Trading Economics*, online.

113 US–China Economic and Security Review Commission, *China's response to US – South Korean missile defense system deployment and its implications*, US Government, July 2017, online; Yeo Han-koo, *Is South Korea de-risking?*, Peterson Institute for International Economics, 26 January 2024, online.

114 Notably, a trifecta of bills passed in 2024: the Framework Act on Supply Chain Stabilization Support for Economic Security; the Special Measures to Strengthen the Competitiveness of Materials, Parts, and Equipment Industry Act; and the Special Act on National Resources Security.

115 For example, the Act on Prevention of Divulgence and Protection of Industrial Technology (which entered into force in 2020) tightens scrutiny for investment proposals involving designated 'national core technology'. The 2022 National High-Tech Strategic Industries Act targets foreign investment in local firms with cutting-edge technology, defined as 'national high-tech strategic industries'. In 2024, the government enforced a decree drawing on the Foreign Investment Promotion Act aimed at further protecting local companies with 'national high-tech strategic technologies' by enabling regulators to review undeclared investments suspected of endangering national security.

116 Jiyoung Sonh, Rhiannon Hoyle, 'The $1.7 billion takeover brawl fueled by a fear of China', *Wall Street Journal*, 28 September 2024, online; Simon Lester, Huan Chu, 'CFIUS and Korean Government finishing up security review of Chinese purchase of Korean semiconductor company', *China Trade Monitor*, 17 September 2021, online.

117 'South Korea plans $34 bln fund for strategic sectors like chips and autos', *Reuters,* 5 March 2025, online.

118 Jihoon Lee, 'South Korea makes AI investment a top policy priority to support flagging growth', *Reuters,* 22 August 2025, online.

119 Telecommunications Business Act (Act no. 17352), 9 June 2020, Republic of Korea, online.

120 Act on the Protection of Information and Communications Infrastructure (Act no. 11690), 23 March 2013, Republic of Korea, online.

121 Act on the Protection of Information and Communications Infrastructure (Act no. 11690).

122 Scott J Shackelford, 'South Korea's 2024 Cyber Strategy: a primer', *Strategic Technologies*, Center for Strategic and International Studies, 2 August 2024, online.

123 Kuksung Nam, 'South Korea launches security council to strengthen critical infrastructure resilience', *The Readable*, 29 May 2024, online.

124 'AWS compliance: Cloud Security Assurance Program (CSAP)', Amazon Web Services, online.

125 International Trade Administration, *Korea—Digital economy*, Department of Commerce, US Government, 19 September 2024, online; 'Microsoft Azure gains approval for use in South Korea's public sector', *The Korea Bizwire*, 2 December 2024, online.

126 International Trade Administration, *Korea—Digital economy.*

127 국가사이버안보센터 (National Cyber Security Center), '보안적합성 검증: 개요 및 체계' [Security Verification Scheme: overview & system], ROK Government, no date, online.

128 'The Korea Cryptographic Module Validation Program (KCMVP): a cornerstone of national cybersecurity', *Lawfirm Lawwin*, 29 July 2025, online.

129 Park Eun-lee, Seo Ji-eun, Lee Jae-lim, Chin Ha-nee, 'Experts call on Korea to form "DeepSeek-pursuing" task force', *Korea JoongAng Daily*, 6 February 2025, online.

130 Megha Besuccess, 'Korean intelligence agency to release security guidelines for ChatGPT amid rising cybersecurity threats', *Korea Tech Today*, 13 June 2023, online.

131 International Trade Administration, *Korea—Digital economy.*

132 Ministry of Government Legislation, Framework Act on Supply Chain Stabilization Support for Economic Security, Act no. 19828 (26 December 2023), ROK Government, online.

133 Mitch Fifield, 'Joint release – Treasurer – Government provides 5G security guidance to Australian carriers', 23 August 2018, online.

134 Sujan Chinoy, 'Boost for India's telecom security: new directive cuts reliance on foreign equipment, including from dubious sources', *Times of India*, 28 December 2020, online.

135 'Huawei and ZTE left out of India's 5G trials', *BBC News*, 5 May 2021, online.

136 Juan Pedro Tomás, 'Indian operators expand 5G to 469k base stations, 250m subscribers', *RCR Wireless News*, 26 March 2025, online.

137 'Japan bans Huawei and its Chinese peers from government contracts', *Nikkei Asia*, 10 December 2018, online.

138 Bloomburg, 'Huawei loses key 5G network customer as SoftBank turns to Nokia and Ericsson', *South China Morning Post*, 31 May 2019, online.

139 Lester Wong, Irene Tham, 'Singtel- and StarHub-M1 consortium finalises vendors for 5G coverage', *The Straits Times*, 24 June 2020, online.

140 Park Chan-kyong, 'Using Huawei 5G, South Korea presents little security risk', *South China Morning Post*, 7 June 2019, online.

141 DHA, 'Telecommunications sector security reforms', Australian Government, September 2018, 7, online.

142 *Cyber Security Act 2024* (no. 98, 2024), enacted 29 November 2024, Australian Parliament, online.

143 DHA, 'Protective Security Policy Framework (PSPF) annual release', Australian Government, 2925, online.

144 DHA, *Security of Critical Infrastructure Act 2018* (Cwlth), no. 29, Australian Government, 2018, consolidated version, online.

145 *Privacy Act 1988* (Cwlth), Schedule 1—Australian Privacy Principles, Australian Parliament, latest version as of 10 June 2025, online.

146 *Foreign Acquisitions and Takeovers Act 1975* (Cwlth), Australian Parliament, updated 1 January 2021, online.

147 'India introduces new rules for critical telecom infrastructure', *Digital Watch*, 1 December 2024, online.

148 National Security Council Secretariat, 'Launch of the "Trusted Telecom Portal" for implementation of the National Security Directive on the Telecommunication Sector', Indian Government, 15 June 2021, online.

149 Department of Telecommunications, *Mandatory Testing and Certification of Telecom Equipment (MTCTE)*, Telecommunications (Framework to Notify Standards, Conformity Assessment and Certification) Rules, 2025, Ministry of Communications, Indian Government, online; Telecommunication Engineering Centre, 'Procedure for mandatory testing and certification of telecommunication equipment (MTCTE)', version 3.0, Indian Government, April 2024, online.

150 *The evolving cybersecurity regulatory landscape in India: 2025 and beyond*, Nasscom Centre of Excellence for Cybersecurity, July 2025, online; Department of Electronics and Information Technology, *National Cyber Security Policy 2013*, Indian Government, July 2013, online.

151 Information Technology Act, 2000 (Act no. 21 of 2000), enacted 9 June 2000, effective from 17 October 2000, Indian Parliament, online.

152 Press Information Bureau, 'Government of India taking measures to protect critical infrastructure and private data against cyber attacks', Indian Government, 18 July 2025, online.

153 Indian Computer Emergency Response Team (CERT-In), *Technical guidelines on software bill of materials (SBOM), quantum BOM (QBOM), cryptographic BOM (CBOM), artificial intelligence BOM (AIBOM), and hardware BOM (HBOM)*, version 2.0, Ministry of Electronics and Information Technology, Government of India, July 2025, online.

154 Department of Telecommunications, 'Minimum requirements for security policy of DoT licensees', Ministry of Communications, Indian Government, 26 September 2018, online.

155 *National Critical Information Infrastructure Protection Centre (NCIIPC) guidelines,* version 2, Indian Government, online.

156 Digital Personal Data Protection Act, 2023, section 16(1), Indian Parliament, online.

157 Prime Minister's Office, *Atmanirbhar Bharat: the foundation of a strong and developed India*, Indian Government, 15 August 2025, online.

158 Department for Promotion of Industry and Internal Trade (DPIIT), 'Consolidated foreign direct investment (FDI) policy circular', effective from 15 October 2020, Ministry of Commerce and Industry, Indian Government, online; Press Information Bureau, 'Investment from land border sharing countries', Ministry of Commerce and Industry, Indian Government, 17 April 2020, online.

159 DPIIT, Public Procurement (Preference to Make in India) Order, 2017, Indian Government, online; 'Revision to the Public Procurement (Preference to Make in India) Order', *ELP Law*, 9 June 2020, online; Press Information Bureau, 'Press Information Bureau—official media unit of Government of India', Indian Government, online.

160 Ministry of Foreign Affairs, *National Security Strategy (NSS)*, Japanese Government, 16 December 2022, online.

161 Telecommunications Business Act (Act no. 86 of December 25, 1984), Japanese Government, online; '2020 amendment of the Telecommunications Business Act including registration requirement for certain foreign providers', *Digital Policy Alert*, online.

162 Ministry of Internal Affairs and Communications, *5G security guidelines*, version 1, Japanese Government, 22 April 2022, online; Louise Matsakis, *Japan's 5G approach sets a model for global cooperation*, Lawfare Institute, 14 September 2020, online.

163 National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity Strategy 2021*, Japanese Government, September 2021, online.

164 Cybersecurity Strategic Headquarters, *Guideline for establishing safety principles for ensuring cybersecurity of critical infrastructure*, Japanese Government, 4 July 2023, online.

165 METI, *The Cyber/Physical Security Framework (CPSF)*, version 1.0, Japanese Government, 18 April 2019, online.

166 Information System Security Management and Assessment Program (ISMAP), operated by the Cabinet Cyber Security Center, Digital Agency, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry, Japanese Government, supported by the Information-technology Promotion Agency, online.

167 METI, 'Guidance on introduction of software bill of materials (SBOM) for software management', version 2.0, Japanese Government, 29 August 2024, online; METI, 'Guide of introduction of software bill of materials (SBOM) for software management' formulated, Japanese Government, 28 July 2023, online.

168 Jun Suzuki, 'Establishment of a security clearance system in the economic security sector', *Anderson Mori & Tomotsune*, 16 October 2024, online; 'Japan launches economic security clearance system amid privacy woes', *Kyodo News*, August 2025, online; Kosuke Iwamoto, Yomiuri Shimbun, 'New law for boosting Japan's economic security to enhance international collaboration; impacts on personnel to be considered', *Japan News*, 11 May 2024, online.

169 Cabinet Secretariat, 'Summary of the Act on the Protection and Utilization of Critical Economic Security Information', Japanese Government, May 2024, online.

170 Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures (Act no. 43 of 2022), Japanese Government, translated version online; Cabinet Office, 'System for ensuring stable provision of specified essential services under the Economic Security Promotion Act (briefing material)', Japanese Government, August 2025, online; Cabinet Office, '.2Outline of the Essential Infrastructure System and required information (introduction of specified facilities)', Japanese Government, August 2025, online.

171 Act on the Protection of Personal Information, Act no. 57 of 2003, as amended, Japanese Government, online.

172 Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures (Economic Security Promotion Act), Act no. 43 of 18 May 2022, Japanese Government, translated version online.

173 Foreign Exchange and Foreign Trade Act (外国為替及び外国貿易法, Act no. 228 of 1 December 1949), translated 4 March 2025, online; Ministry of Finance, 'Rules and regulations of the Foreign Exchange and Foreign Trade Act', Japanese Government, 24 April 2020, online; Foreign Investment Policy and Review Office, *Foreign Investment Screening System annual report (FY2023)*, International Bureau, Ministry of Finance, Japanese Government, 2023, online.

174 Singapore Parliament, Telecommunications Act (Chapter 323), originally enacted as Act 43 of 1999, revised edition as of 30 December 2000, online.

175 IMDA, 'Policy for fifth-generation (5G) mobile networks and services in Singapore', Singapore Government, 17 October 2019, online.

176 IMDA, *Guide to Equipment Registration Framework*, issue 1, rev. 11, Singapore Government, August 2024, online; IMDA, 'Equipment registration', Singapore Government, online.

177 Singapore Parliament, Cybersecurity Act (Cap. 215A), enacted 2018, online.

178 Singapore Parliament, Cybersecurity (Amendment) Act 2024, online; Janil Puthucheary, Senior Minister of State for Communications and Information, 'Opening speech for second reading of Cybersecurity (Amendment) Bill', Cyber Security Agency of Singapore, 7 May 2024, online; Janil Puthucheary, Senior Minister of State for Communications and Information, 'Closing speech for second reading of Cybersecurity (Amendment) Bill', Cyber Security Agency of Singapore, 7 May 2024, online; Cyber Security Agency of Singapore, 'Cybersecurity (Amendment) Bill infographic', 2024, online.

179 Singapore's Cyber Security Agency and Boston Consulting Group, *Critical Information Infrastructure Supply Chain Programme—a national effort in managing cyber supply chain risks*, June 2023, online.

180 Cyber Security Agency of Singapore, *Cyber Trust V202208*, 2022, online.

181 *Instruction manual for ICT & SS management*, Singapore Government, online.

182 Singapore Parliament, Infrastructure Protection Act 2017 (no. 41 of 2017), 2020 revised edition, online.

183 Ministry of Digital Development and Information, 'New Digital Infrastructure Act to enhance resilience & security of digital infrastructure & services', Singapore Government, 1 March 2024, online; IMDA, 'IMDA media release on advisory guidelines for cloud services and data centres', Singapore Government, 25 February 2025, online.

184 IMDA, 'Advisory guidelines for resilience and security of cloud services', 25 February 2025, online.

185 IMDA, 'Advisory guidelines for resilience and security of data centres'.

186 Personal Data Protection Act 2012 (no. 26 of 2012), *Singapore Statutes Online*, online.

187 Monetary Authority of Singapore, *Technology risk management guidelines*, Singapore Government, 18 January 2021, online.

188 William Yuen Yee, 'Singapore's new investment screening law', Lawfare Institute, 9 July 2024, online.

189 Korean Telecommunications Business Act, Act no. 55920, version as of 9 June 2020, online.

190 National Security Office, *National Cybersecurity Strategy*, ROK Government, April 2019, online; Scott J Shackelford, 'South Korea's 2024 Cyber Strategy: a primer'.

191 Korean Law Information Center, Act on Promotion of Information and Communications Network Utilization and Information Protection, Law no. 13520, enacted 1 December 2015, effective 2 June 2016, online.

192 'Common criteria for information technology security evaluation', CC:2022, revision 1, *Common Criteria Portal*, November 2022, Part 4: Framework for the specification of evaluation methods and activities, November 2022, online; 'What is common criteria (CC) for information technology security evaluation?', *TechTarget*, 5 December 2024, online.

193 US Commercial Service Korea, 'Korea digital economy', US Government, 2024, online.

194 US Commercial Service Korea, 'Korea digital economy'; 'Korea's MSIT amended notification on Cloud Security Assurance Program (CSAP) goes in effect', *Kim & Chang*, 19 January 2023, online; 'South Korea's cloud service restrictions', Information Technology and Innovation Foundation, 25 May 2025, online.

195 National Intelligence Service, 'Security Verification Scheme', National Intelligence Service (Republic of Korea), n.d., online.

196 Act on the Protection of Information and Communications Infrastructure, Act no. 28812, enacted 22 May 2009, ROK Government, online; Act on the Promotion of the Provision and Use of Public Data, Act no. 136754, enacted 23 March 2013, ROK Government, online.

197 Personal Information Protection Act, Act no. 10465, promulgated 29 March 2011, amended 14 March 2023, ROK Government, online; Kathrin Gardhouse, 'Changes to South Korea's Personal Information Protection Act to take effect on March 15, 2024', *Private AI*, 18 June 2025, online; Personal Information Protection Commission, 'Amended Personal Information Protection Act and its enforcement decree become effective', ROK Government, 15 September 2023, online.

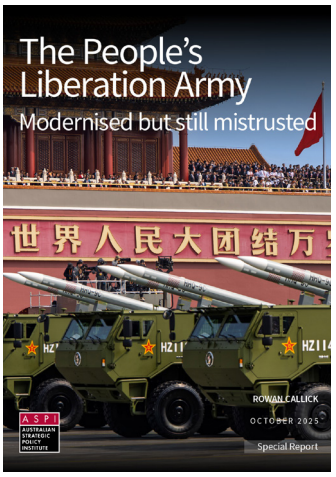
198 Act on Special Measures for Strengthening and Protecting Competitiveness of National High-Tech Industry, Act no. 18813, promulgated 3 February 2022, effective 4 August 2022, ROK Government, online; 'Korea Legal Insight Series', *Kim & Chang*, 27 September 2023, online; 'Korea implements new Act on Special Measures for Strengthening and Protecting Competitiveness of National High-Tech Strategic Industries', *Lee & Ko*, newsletter no. 892, 7 September 2022, online.

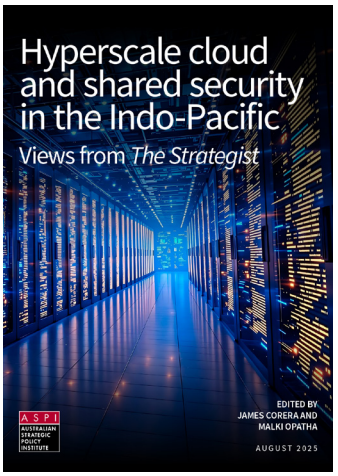
199 Framework Act on Supply Chain Stabilisation Support for Economic Security, Act no. 19828, promulgated 26 December 2023, effective 27 June 2024, ROK Government, online; Ministry of Trade, Industry and Energy, 'Korean Government holds 3rd supply chain stabilization committee meeting', ROK Government, 19 December 2024, online; Ministry of Economy and Finance, 'The Enactment of Framework Act on Supply Chain', ROK Government, 27 December 2023, online.

Acronyms and abbreviations

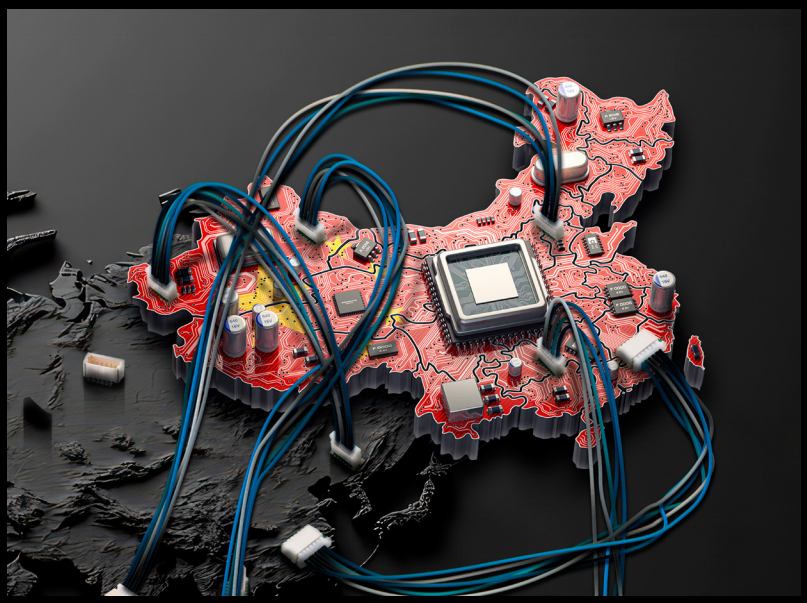
AI	artificial intelligence
ASIO	Australian Security Intelligence Organisation
BRICS	Brazil, Russia, India, China, South Africa
ESPA	*Economic Security Promotion Act 2022* (Japan)
EU	European Union
FDI	foreign direct investment
FIRB	Foreign Investment Review Board (Australia)
FOCI	foreign ownership, control and influence
GDP	gross domestic product
ICT	information and communications technology
IMDA	Infocomm Media Development Authority (Singapore)
IoT	internet of things
IP	intellectual property
ISMAP	Information System Security Management and Assessment Program (Japan)
IT	information technology
MAS	Monetary Authority of Singapore
METI	Ministry of Economy, Trade and Industry (Japan)
MTCTE	mandatory testing and certification of telecom equipment
NIS	National Intelligence Service (South Korea)
NSS	National Security Strategy (Japan)
PSPF	Protective Security Policy Framework (Australia)
R&D	research and development
ROK	Republic of Korea
SBOM	software bill of materials
SOCI Act	*Security of Critical Infrastructure Act 2018* (Australia)
SVS	Security Verification Scheme (South Korea)
TEC	Telecommunication Engineering Centre (India)

Some recent ASPI publications





ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE



ISSN 2200-6648