PROTOSTAR
STRATEGY

Securing the Future

AI, Critical Infrastructure, and Regulatory Readiness in the Indo-Pacific

October 2025

AmCham
access to opportunity

paloalto®
NETWORKS

About Protostar Strategy

Protostar Strategy is a boutique advisory firm at the intersection of geopolitics and technology. Founded by Dr. Tobias Feakin, Australia's first Ambassador for Cyber Affairs and Critical Technology, the firm helps governments, companies, and investors navigate the strategic risks and opportunities created by emerging technologies. Protostar Strategy provides high-level analysis, executive advisory, and tailored engagement on issues ranging from AI governance and cybersecurity to supply chains, infrastructure resilience, and international tech diplomacy.

Independence Statement

Protostar Strategy is a commercial advisory firm, but independence remains at the core of our work. We collaborate with clients and sponsors on selected projects, yet our analysis and conclusions are our own. This report has been informed by the contributions of participants in workshops held across the region, whose perspectives and experience enriched its content. However, responsibility for the analysis and final conclusions rests with Protostar Strategy and the author. The views expressed do not necessarily reflect the positions of partner organisations, sponsors or contributors.

Contact

Protostar Strategy

W: www.protostarstrategy.com

ABN: 92989642552

Copyright

Contents

Foreword

The Indo-Pacific is entering a decisive moment in its technological transformation. Nowhere else in the world are the pressures of rapid adoption, geopolitical rivalry, and infrastructure vulnerability converging at such speed and scale. The choices the region makes about how to govern artificial intelligence in its critical systems will not only shape national resilience but also influence the balance of trust, security, and influence in global technology governance.

History reminds us that every generation has faced similar inflection points. The twentieth century's great infrastructure projects, bridges, aviation, energy grids, were eventually made safe through codes and standards, often only after crises forced action. For the Indo-Pacific today, the test is whether it can learn faster, to build the guardrails for AI in infrastructure before a failure compels them.

This report was conceived to address that challenge. Over the course of 2025, we convened senior policymakers, regulators, infrastructure operators, and industry leaders in Australia, India, Indonesia, and Singapore to examine how AI is being integrated into critical infrastructure, and how governance frameworks are, or are not, keeping pace. The conversations were frank, grounded and often sobering. What emerged was not just a set of national case studies, but a regional portrait of systems under pressure: rapid adoption layered on ageing infrastructure, uneven regulatory architectures, and an intensifying geopolitical contest over the digital foundations of power.

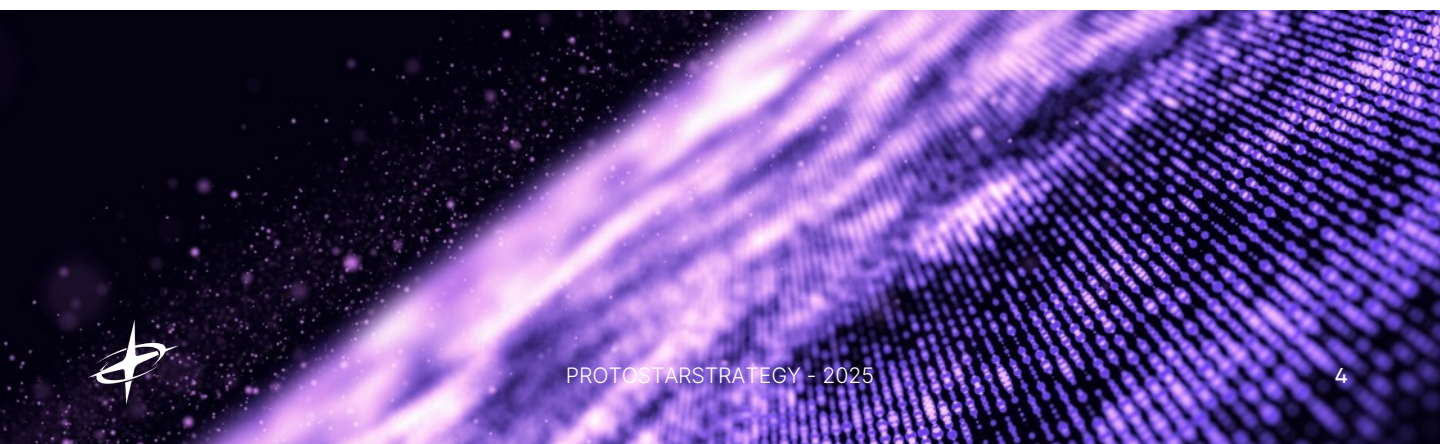
Our findings underline a simple truth: fragmentation is vulnerability. Divergent national approaches create seams that adversaries can exploit, slow the coordination of response in crises, and weaken trust in the reliability of regional systems. But fragmentation is not destiny. The Indo-Pacific can still converge on shared principles, interoperable assurance practices, and models of co-governance that bring together the state, the private sector, and international partners. If the region succeeds, it will not only strengthen its own resilience but also help shape global standards for how AI is governed in mission-critical settings.

The task ahead is urgent but achievable. The choice is not whether AI will govern the region's critical infrastructure, it already is beginning to. The choice is whether the region will govern AI in time.

On a personal note, I am deeply grateful to the many voices across the region who shared their insights, experience, and candour through our workshops. This project would not have been possible without the partnership of the American Chamber of Commerce in convening diverse stakeholders across four countries, and the support of Palo Alto Networks in enabling the work. Their contributions, and the openness of participants, remind us that resilience is not built by governments or companies alone, but through collaboration and trust. It is my hope that this report helps to advance that conversation, offering both a warning and a path forward at a moment when the stakes could not be higher.

Dr Tobias Feakin

Managing Director
Protostar Strategy



Partner Statement

October 2025

The Indo-Pacific is the world's most strategically vital region, and artificial intelligence (AI) is the most transformative technology shaping its future. The region is at an inflection point where critical decision-making on regulatory, research, and readiness priorities must be urgently addressed. Australia has an opportunity to lead the regional response.

The American Chamber of Commerce in Australia (AmCham) is proud to partner with Palo Alto Networks and Protostar Strategy to uncover new insights on how AI can be utilised to support growth, productivity and efficiency in a challenging geopolitical environment and evolving threat landscape.

This report makes clear AI is fast becoming a ubiquitous technology and the conversation has moved rapidly from abstract principles to operational practices. Opportunities, as well as vulnerabilities, must be better understood to ensure governments and businesses have the settings in place to thrive.

Critical infrastructure is the frontline where governments and industry intersect, with direct consequences for citizens. AI is deeply embedded in our most critical infrastructure, affecting how people access water, energy and transport. This presents much-needed opportunities to increase efficiency and productivity, while simultaneously demanding appropriate attention to ensure these life-sustaining and prosperity-generating systems and services are resilient to both inadvertent mistakes and malicious intent.

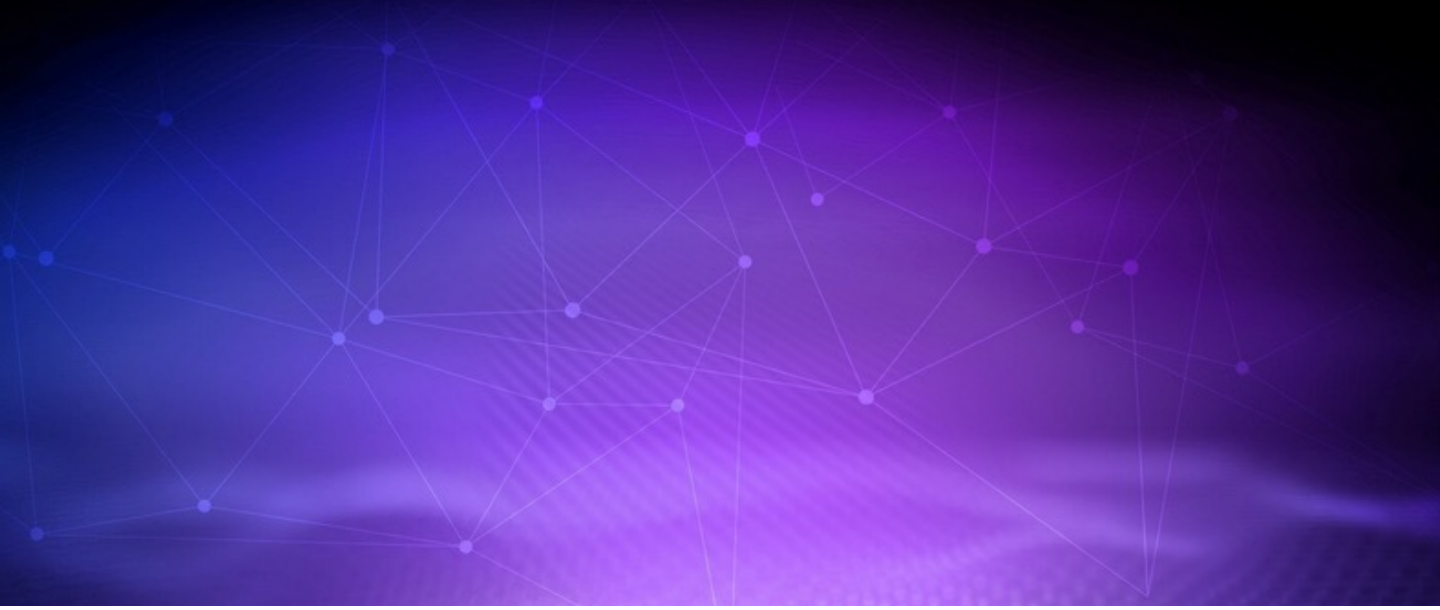
The regulatory approach should rapidly evolve to equal the innovation and agility of the burgeoning sector. The frameworks, if fit for purpose, will support innovators to flourish in a trusted operating environment.

This report is evidence of Australia's important role in the Indo-Pacific, connecting with partners in India, Indonesia and Singapore to share knowledge and uplift the resilience of the region. Much like our interconnected kinetic supply chains, networks and algorithms transcend borders. Collaboration on AI in critical infrastructure throughout the region is key to ensuring a free, open, secure and prosperous Indo-Pacific that benefits all nations.

On behalf of AmCham Australia, I thank all the participants of the workshops whose insights have been crucial to the depth of this research and congratulate the author for ensuring decision-makers are informed and equipped to advance Australia's AI innovation and secure the future. As Chair of AmChams of Asia Pacific, I would also like to thank our counterparts AmCham India, AmCham Indonesia and AmCham Singapore for their partnership.

April Palmerlee

Chief Executive Officer, AmCham Australia
Chair, AmChams of Asia Pacific



Partner Statement

October 2025

The integration of Artificial Intelligence into the operational fabric of critical infrastructure represents a profound and irreversible shift to a sector that is looking to move beyond legacy tools and processes.

As this report, "AI, Critical Infrastructure, and Regulatory Readiness in the Indo-Pacific," outlines, AI is no longer a theoretical tool - it's a foundational attribute of our digital infrastructure. It is actively powering the grids, ports, and transportation systems that sustain our societies, and helping to better deliver critical services to communities across the globe. This transition brings with it immense potential for enhanced efficiency and resilience, but it also introduces new complexities and vulnerabilities that demand our immediate attention.

Palo Alto Networks is proud to have supported the production of this timely, objective and critical report. I would like to express our sincere gratitude to the author, Dr. Toby Feakin, and the participating American Chambers of Commerce for facilitating this important work. Our thanks also extend to all the government and private sector participants for their invaluable contributions. The insights within reflect a clear-eyed view of the challenges and opportunities facing governments and industries in the Indo-Pacific, a region at the epicentre of this digital transformation. We are equally proud to contribute to this vital discussion, drawing on our expertise at the intersection of cybersecurity, AI, and global policy.

This report serves as both a roadmap and a call to action. It demonstrates that by working together, governments and industry can seize this opportunity to act proactively, embedding trust and security into the core of our AI-enabled infrastructure. The choices made today will determine whether the Indo-Pacific helps shape global digital standards or whether it is left to adapt to frameworks written elsewhere. We are optimistic that the region will choose the former, and we stand ready to partner with governments and industry alike to build a future where innovation and security are inextricably linked.

Bruce Byrd

Executive Vice President & General Counsel
Palo Alto Networks

paloalto® NETWORKS

Executive Summary

AI is no longer confined to research labs or niche applications. In the Indo-Pacific, it is increasingly embedded in the operational core of critical infrastructure: balancing power grids, forecasting floods, steering port logistics and managing transport flows. The promise is efficiency and resilience; the peril is fragility and exposure. Algorithms that optimise can also misfire, cascade across systems and provide new vectors for adversaries.

The central challenge is whether governments can build governance frameworks fast enough to match the pace of adoption. Across the region, AI has become an infrastructure layer, integral to how societies deliver essential services and safeguard sovereignty. Yet regulation, assurance and public–private collaboration remain patchy and uneven.

Regional Landscape

The Indo-Pacific is a global engine of digital adoption but also a laboratory of vulnerability. Unlike earlier waves of digitisation, AI is entering systems at speed and scale, directly shaping physical processes. Fragmented national approaches complicate crisis response and invite exploitation by state-backed cyber actors. What emerges is a structural weakness: AI in critical infrastructure cannot be treated as a domestic issue alone.

AI in critical infrastructure cannot be treated as a domestic issue alone.

National Pathways

Australia

prioritises resilience over speed. Anchored in the Security of Critical Infrastructure Act 2018 (SOCI Act) and a mature cyber ecosystem, the Australian Government has moved incrementally toward guardrails but lacks AI-specific assurance. Its influence lies in linking domestic vigilance to standards-setting through the Quad, AUKUS and ASEAN, and others.

India

pairs global ambition with developing architecture. Federal diversity fuels innovation but produces uneven assurance and weakens accountability. Scale without safeguards risks systemic vulnerability. If aligned with trust, India could become the preferred supplier of non-Chinese AI systems across the Global South.

Indonesia

is dynamic but under-governed in the technology space. Smart city pilots, grid optimisation and private-sector experimentation abound, yet regulatory scaffolding lags and cybersecurity capacity could be increased. Geopolitical competition brings both capital and dependency, so the Government of Indonesia must channel pluralism into coherent assurance frameworks.

Singapore

has emerged as the region's governance laboratory. Its National AI Strategy 2.0, AI Verify initiative and Cyber Security Agency's (CSA) proactive standards embed assurance into water, energy, ports and transport sectors. Beyond its borders, Singapore leverages technical leadership as diplomatic currency, shaping ASEAN norms and global standards.

Strategic Choices

Three imperatives cut across the region:

Confront fragmentation

Divergent rules create vulnerabilities and complicate crisis response. Inconsistent standards invite regulatory arbitrage and slow coordination when infrastructure fails. Without baseline interoperability, adversaries will exploit the seams. Regional actors need not adopt identical laws, but common risk categories and assurance benchmarks are essential to contain cascading risks.

Shift to co-governance

Compliance audits are insufficient when governments depend on privately owned and globally sourced technologies. Structured mechanisms for joint risk assessments, red-teaming and incident simulations must become routine. Only through co-governance can the state gain visibility into systems they do not control, and only then can operators gain the predictability they need to innovate with confidence.

Balance liability with guardrails

Outcomes-based accountability can suffice for low-consequence uses, forecasting demand, scheduling staff or optimising traffic flows, where failures are manageable. But in high-consequence systems such as grids, ports or water supply, preventative guardrails are indispensable: mandated testing, transparency obligations and fallback mechanisms that pre-empt catastrophic failure.

Diplomacy is integral. The Indo-Pacific is already a battleground of standards, from China's Digital Silk Road to Western regulatory models. Regional convergence through ASEAN, the Quad or AUKUS has the potential to set interoperable norms. Failure to do so will leave the region adapting to frameworks written elsewhere, forfeiting both sovereignty and strategic leverage.

Conclusion

AI already runs parts of the Indo-Pacific's vital systems. The question is not whether adoption will proceed, but whether governance will catch up. The region can either drift into a future of uneven safeguards and exploitable gaps, or it can build interoperable frameworks that balance innovation with resilience and sovereignty with interdependence.

History shows that infrastructure safety codes emerged only after tragedy. The Indo-Pacific now has the chance to act sooner: to build the guardrails before the crisis, to embed co-governance between state and market, and to use diplomacy to hardwire trust across borders. Acting collectively and early, the region can demonstrate that AI can be harnessed without sacrificing security or sovereignty, and position itself as a rule-shaper in the global contest over digital standards. Acting late and alone would mean fragmented protections, brittle systems and rules imposed from elsewhere.

Part 1

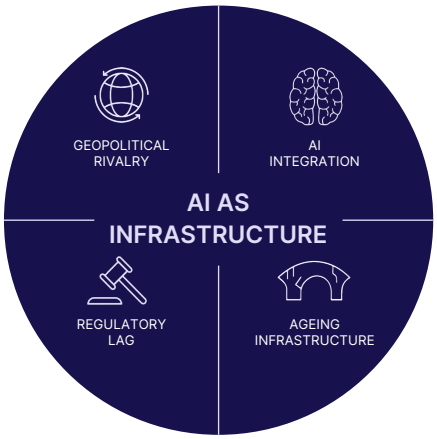
Regional Trends and Strategic Cross-currents

Part 1 of this report considers the wider strategic currents that frame national choices. Across the Indo-Pacific, AI is being pulled into the heart of critical infrastructure, even as regulatory frameworks lag and geopolitical rivalries sharpen. These regional dynamics set the stage for the country spotlights that follow in Part 2.

AI and Infrastructure in a Region Under Pressure

In the Indo-Pacific, where geopolitical friction meets rapid digital transformation, the rise of AI in critical infrastructure is becoming a defining test of resilience. Governments across the region are rushing to harness the promise of AI to optimise power grids, accelerate port logistics and modernise health care. But these same technologies are exposing critical systems to new vulnerabilities: errors embedded in opaque algorithms, cyber manipulation of automated processes and cross-border risks introduced by globally distributed supply chains.

Infrastructure that once depended on physical engineering and localised control is now intertwined with machine-learning models, frequently designed or updated outside national jurisdictions. In this context, AI has become an infrastructure layer, shaping how societies deliver essential services and how states protect sovereignty.[1]



This report examines the evolving relationship between AI and critical infrastructure in 4 key Indo-Pacific countries: Australia, India, Indonesia and Singapore. It draws on the findings of high-level strategic workshops held in each of these countries during July 2025, and offers an in-depth analysis of how these states are navigating the integration of AI technologies into essential services while managing the associated risks, including cyber threats.

The workshops brought together senior policymakers, regulators, infrastructure operators and private-sector executives – voices at the centre of both national security debates and operational decision-making, providing a uniquely authoritative vantage point.

At its core, this report grapples with 3 interlocking questions:

- How is AI being integrated into critical infrastructure?
- How are regulatory responses evolving to keep pace with that integration?
- What new models of public–private collaboration are needed to strengthen resilience in the face of emerging threats?

Each of the 4 countries faces a distinct set of pressures, but they share common structural challenges:

- ageing infrastructure systems being digitised in uneven ways
- regulatory architectures that need to adapt to cross-sectoral AI applications
- national security strategies that increasingly view digital dependence as a vulnerability.

These dynamics are unfolding in a region that sits at the frontline of great power competition, where technology is no longer just a tool of economic development but a terrain of geopolitical contest.

The Technological Tipping Point

In recent years, the Indo-Pacific has emerged as both a global growth engine and a digital testing ground. Mobile-first economies, large-scale infrastructure projects, and ambitious smart city plans have created fertile conditions for AI integration, particularly in sectors like transport, energy, health and water. From predictive maintenance of grid systems in New Delhi to AI-enabled flood forecasting in Jakarta, governments are betting that automation and intelligent analytics can drive efficiency, reduce human error and increase service continuity.[2]

Yet this optimism sits uncomfortably alongside growing anxiety. The more AI is embedded in critical systems, the more those systems depend on data integrity, algorithmic transparency and secure digital infrastructure. Threat actors, state-sponsored or otherwise, recognise this new terrain. In Australia, attacks on health systems and logistics providers have raised alarm about the fragility of digital dependencies.[3] In India, AI-powered surveillance tools have sparked debate about governance gaps and data protection.[4] In Indonesia, where infrastructure development is accelerating, the regulatory system is still playing catch-up.[5] And in Singapore, even with its high governance maturity, the government has publicly acknowledged the national security implications of AI proliferation.

The challenge for policymakers is not simply how to adopt AI, but how to govern it in mission-critical settings where failure could lead to cascading consequences.

Not All AI Carries Equal Risk

A crucial but often overlooked distinction in this debate lies between AI systems that operate at the operational technology (OT) layer and those that function at the information technology (IT) layer.

OT-layer AI directly controls physical processes, such as grid balancing, water flow, industrial automation and traffic management. Here, errors or manipulation can trigger real-world consequences, including blackouts, transport paralysis or water shortages.

IT-layer AI supports functions such as intrusion detection, data analysis or network optimisation. While generally one step removed from direct physical control, failures at this layer can cascade, undermining the OT systems they monitor or defend.

The risks escalate when OT and IT layers converge. For example, an AI-based cybersecurity tool might miss adversarial inputs corrupting an OT controller, or a cloud update could alter the behaviour of a model steering essential processes without operators realising the implications. Unlike legacy OT and IT systems, which were often localised and hard-wired, modern AI platforms are dynamic, remotely updated and trained on datasets with opaque provenance.

This convergence creates a governance blind spot. Without clear thresholds to determine when an AI tool moves from being a performance enhancer to a safety-critical system, and without certification regimes to test AI integrity under stress, both operators and regulators remain reactive. Innovation races ahead while systemic risk accumulates.

OT-layer AI

- Directly controls physical processes
- Errors → real-world impact

IT-LAYER AI

- Failures can cascade into OT systems
- One step removed, but still critical

Cybersecurity at the Core

Infrastructure has long been a target of strategic interest to both state and non-state cyber actors. The danger is magnified as OT systems, rarely designed with security at their core, are increasingly tethered to IT environments. This convergence compounds exposure, leaving OT systems and networks inherently vulnerable to compromise. Onto this fragile terrain emerge novel forms of digital attack: poisoned datasets can quietly distort training; adversarial inputs can nudge automated systems into error; tailored intrusions can recalibrate the very decisions that infrastructure operators rely upon. Such attacks evade traditional defences, obscure forensic trails, complicate attribution and deliver consequences that unfold in real time. For the Indo-Pacific, already the epicentre of persistent cyber contestation, the stakes are acute. State-backed groups, criminal syndicates and proxies routinely probe the region's infrastructure. As reliance on AI deepens, these systems become not only more attractive targets but also more brittle ones. In this environment, developing credible assurance frameworks is a matter of strategic necessity.

Systems Without Borders, Risks Without Owners

Compounding the issue is the transnational character of AI development. Many of the models used in Indo-Pacific infrastructure are built by foreign firms, trained on global datasets and hosted in overseas cloud environments. National operators are held responsible for outcomes but often depend on systems they cannot inspect or control. As one senior policymaker with responsibility for critical infrastructure put it, this is 'sovereignty without visibility'.

This dispersion of risk raises fundamental accountability questions:

- Who is liable when an offshore update triggers a fault in a domestic grid?
- How can governments safeguard resilience when critical systems blend local hardware, foreign software and international data flows?

Traditional procurement and risk assessment processes are ill-suited to this new reality. Infrastructure must now be understood not as a static physical asset but as adaptive, hybrid systems, part hardware, part algorithm, and embedded in global digital networks.

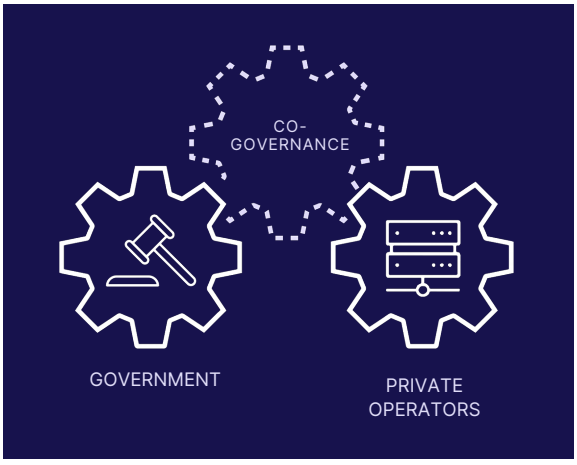
A Patchwork of Regulation

Regulatory approaches remain uneven across the 4 countries. Singapore has led with its AI Verify framework, one of the first government-backed assurance regimes.[6] Australia has amended the SOCI Act to embed AI and digital risk into sector-specific regulatory obligations.[7] India's Digital Personal Data Protection Act 2023 signals a rights-based approach but awaits implementation.[8] Indonesia is still drafting comprehensive AI and cybersecurity legislation, with a presidential regulation expected in 2025.[9]

Despite these national differences, a regional pattern is emerging, with policymakers increasingly recognising that AI in essential services must be treated as a public risk, not just a private innovation. Regulators often lack the technical depth to evaluate complex AI models, while overlapping jurisdictions blur responsibility and slow response. At the same time, AI developers and infrastructure operators work across borders, creating a mismatch between where regulation is applied and where risks ultimately materialise.

As a result, countries face a critical question: how to safeguard sovereign control over infrastructure resilience while remaining open to international innovation and investment?

The Missing Middle: Public–Private Coordination



One of the most consistent insights from our workshops is that current governance frameworks are structurally dependent on private actors yet often fail to integrate these actors into national resilience planning. Across the Indo-Pacific, from cloud providers and telecom operators to energy companies and logistics networks, private entities own and operate vast portions of infrastructure now deemed critical to state functioning. These systems increasingly rely on AI tools developed, maintained or hosted by global firms outside national jurisdiction, creating a strategic misalignment between where the technology lives and where state-level risk must be managed.[10]

In theory, public–private partnerships (PPPs) are meant to bridge this gap. In practice, many remain transactional. In Indonesia and India, PPPs in AI and infrastructure tend to focus on short-term pilot projects, with unclear scalability or long-term ownership.[11]

In Australia, regulatory obligations for critical infrastructure providers are expanding, especially under the SOCI Act, but dialogue between government and operators is still largely reactive, rather than anticipatory. Singapore's engagement model is more proactive, enabling early collaboration between government and industry regarding AI deployment, yet even their policymakers acknowledge the need for more iterative, risk-sharing frameworks.[12]

True resilience requires a shift beyond compliance toward co-governance, where public and private actors jointly identify systemic vulnerabilities, establish safety baselines and conduct regular joint incident simulations. Such collaboration cannot be improvised during crises; it must be institutionalised with formal mandates, trust-based communication channels and shared operational clarity.

Why the Indo-Pacific Region Matters

This report does not argue for a one-size-fits-all approach. Each country's political system, technological capacity and economic structure will shape its path forward. But there is a compelling case for greater regional coordination. As AI proliferates in supply chains and infrastructure systems that cross borders – undersea cables, satellite networks, cloud platforms – the risks become more distributed. A failure in one country's electricity grid or port system could cascade across borders, creating second and third order effects that no single government can manage alone.

Strategic competition over AI and its underlying infrastructure is intensifying, driven by concerns over dependency, control and the resilience of the digital systems underpinning security and governance. Yet competition can also act as a catalyst for innovation, spurring investment in research, accelerating deployment and motivating governments to strengthen governance frameworks. For the Indo-Pacific, where great power rivalry intersects with high-stakes economic integration, the challenge is to harness these competitive dynamics as a source of progress while building regional mechanisms that safeguard shared assets, contain cross-border crises, and set common guardrails for safe and reliable AI deployment.

The Indo-Pacific is emerging as a critical arena for shaping AI governance. While the United States and European Union still set many of the global benchmarks, the region's choices, through ASEAN-led initiatives, Quad dialogues or emerging bilateral agreements, are beginning to carry wider influence. With massive infrastructure investment underway and geopolitical competition sharpening, the Indo-Pacific's policy decision on AI in critical infrastructure will generate ripple effects well beyond its shores. It is in this context that a new governance model of AI in critical infrastructure must take shape, one that balances openness with sovereignty, innovation with safety and domestic imperatives with regional cooperation.

AI is no longer an experiment confined to research labs; it is becoming infrastructure.

This report aims to chart that model. It offers a grounded, yet forward-leaning analysis of how the region can navigate the coming wave of AI-driven transformation in its most vital systems. The stakes could scarcely be higher. AI is no longer an experiment confined to research labs; it is becoming infrastructure. And once infrastructure is digitised and automated, it ceases to be merely a technical asset; it becomes a strategic vulnerability. How the Indo-Pacific chooses to govern that reality will define its future.

The chapters that follow move from regional dynamics to country case studies, before setting out strategic pathways for cooperation and resilience.

Part 2

Country Spotlights

Regional trends tell only part of the story. The governance of AI in critical infrastructure ultimately plays out within national contexts, shaped by political cultures, institutional capacities and strategic priorities. The Indo-Pacific is too diverse for a single model to prevail. Instead, each country adapts to the pressures of digitisation, cybersecurity and geopolitical competition in its own way, revealing both unique challenges and shared dilemmas. The 4 case studies that follow – presented in alphabetical order: Australia, India, Indonesia and Singapore – illustrate this diversity.

Australia | Cautious Innovation in a Risk-Aware State

Australia approaches the integration of AI into critical infrastructure with a characteristic mix of caution and pragmatism. Where some states treat rapid adoption as a race to be won, the Australian Government leans toward resilience and security, even if that slows the pace. This instinct reflects more than bureaucratic conservatism: it is rooted in a political culture shaped by cybersecurity imperatives, close intelligence ties through the Five Eyes, and a regulatory tradition that prioritises oversight in sectors like finance, energy and health.[13] Policymakers want AI to deliver efficiency and productivity, but not at the cost of introducing new vulnerabilities into systems the state has spent decades trying to secure.

One former senior policymaker described this as Australia's 'default risk reflex'. In their words, 'we cannot afford a blind embrace of AI in critical infrastructure, resilience must be the baseline, not an afterthought'.[14] That reflex has been consistent across governments. AI is seen as a potential enabler but also as a source of hazards that, if left ungoverned, could bring considerable risks to society. Geography plays a role as well. Australia's distance from allies, coupled with its exposure to regional instability, reinforces the instinct to hedge against technological disruption rather than rush into it.

The wider environment sharpens this caution. Across the Indo-Pacific, digital infrastructure has become an arena of geopolitical competition. Data centres, cloud services and AI-driven logistics are no longer just commercial ventures; they are instruments of power projection. In that context, Australia has charted a deliberate middle path: encouraging innovation but bounding it within strong oversight.

That risk calculus is complicated by dependence on external technology ecosystems. Australia is more consumer than producer when it comes to AI platforms and standards, which heightens the need for trustworthy procurement and alignment with allied benchmarks. As an industry participant observed, 'our strategic challenge is not just how we use AI, but how we ensure the systems we import meet resilience thresholds'.[15] This makes Australia less a first mover than a careful standard-setter, aiming to shape adoption conditions rather than chase deployments without safeguards.

The result is an approach that is steady, deliberate and risk sensitive. It does not generate headlines about technological leaps, but it builds the scaffolding for secure deployment over the long term. Yet there are signs that this posture may be shifting. Proposals such as age-based restrictions on social media suggest a growing appetite for firmer intervention when risks are judged to be systemic or socially harmful. The Australian Government's resilience-first instinct remains intact, but it is being recast in ways that are more assertive, with policymakers willing to legislate directly rather than rely solely on voluntary adoption of safeguards. Whether this evolution proves to be an asset or a liability will depend on how effectively principle is translated into practice and on whether its resilience-first posture can keep pace with the accelerating speed of technological change.

Strategic Framing and Governance Posture

Australia has deliberately avoided rushing into a comprehensive AI Act, instead building its governance posture incrementally and in line with international developments. This reflects a recognition that AI policy is unfolding in a global context, with the European Union moving toward a dedicated AI Act, the United States favouring sectoral and executive-order approaches, and regional partners experimenting with hybrid models. The Australian Government choices sit within this shifting landscape, and it has signalled that it is keeping options open rather than pre-committing to a single model.

The National Artificial Intelligence Centre, hosted by CSIRO's Data61, now embedded within the Department of Industry, Science and Resources, acts as an industry enabler and convenor rather than a regulator, but its shift into government reflects closer alignment between innovation policy and regulatory preparedness. Australia also participates in the International AI Safety Institute Network, maintaining access to global expertise even as national approaches diverge.

From 2023 to 2024, the Australian Government moved from discussion to concrete proposals. The Safe and Responsible AI in Australia discussion paper recognised the need for targeted guardrails in high-risk contexts.[16] A year later, the Proposals Paper on mandatory guardrails outlined 10 possible requirements, including human oversight, transparency and resilience testing, while the government also released Voluntary AI Safety Standards for industry.[17] In parallel, work began on a National AI Capability Plan, linking AI governance to infrastructure resilience and the Senate Select Committee on Adopting AI urged economy-wide legislation with explicit reference to large language models.[18]

Together, these steps reflect a shift toward more assertive exploration of AI regulation, though the government has not yet settled on a definitive legislative model. The unresolved question is whether Australia should rely primarily on outcomes-based frameworks, strengthening existing sectoral regimes in response to harms, or shift toward an ex-ante model that mandates preventative guardrails before deployment.

For now, oversight of AI in critical infrastructure remains mediated through sectoral regulation, energy, finance, health and transport, supported by cybersecurity obligations under the SOCI Act. This incremental approach provides flexibility, but it also raises questions about consistency across sectors and the adequacy of safeguards for algorithmic systems that evolve in unpredictable ways.

Infrastructure Integration: Patchy but Expanding

AI adoption in Australian critical infrastructure is advancing, but unevenly. The energy sector uses predictive algorithms to forecast demand and monitor grid vulnerabilities.[19] Water utilities deploy AI-enabled sensors to detect leaks and anticipate failures. Urban authorities in Sydney and Melbourne experiment with machine-learning models to recalibrate traffic flows, improve emergency response and pilot autonomous vehicles.[20] Airports have moved past testing with biometric kiosks and smart gates now operational in 8 international airports. Ports are exploring AI for logistics and cargo management.

Workshop participants described this as a 'varied landscape of deployment': promising initiatives, but inconsistent. One noted, 'many of these systems are not tested against the same resilience threshold. Some are heavily stress-tested; others move forward without consistent evaluation'.[21] Without a national testing protocol, applications often move forward without red-teaming or independent scrutiny. The risks compound as systems evolve from decision-support tools into semi-autonomous actors influencing grid stability, transport routing and emergency dispatch.

A further complication is visibility. Unlike financial services where regulators such as Australian Prudential Regulation Authority (APRA) mandate structured reporting on algorithmic risk, many infrastructure deployments occur beyond central oversight. Vendors and operators can introduce AI tools without informing the government, so long as they comply with existing cyber and privacy rules. The result is a partial view of how AI is reshaping essential services.

Participants also pointed to what they called an 'innovation paradox'. On the one hand, Australia seeks AI adoption to drive productivity and resilience. On the other, the absence of registries, testbeds or structured sandboxes creates uncertainty. Companies either experiment quietly or avoid innovation altogether for fear of scrutiny without clear guardrails. Several argued for a 'structured permission pathway', a model that would couple experimentation with assurance, allowing innovation to proceed while reducing systemic risk.

Cybersecurity and the Critical Infrastructure Nexus

Australia has long cast itself as a regional leader in cybersecurity, particularly when it comes to safeguarding critical infrastructure. The SOCI Act, significantly expanded in 2021 and 2022, mandates risk management programs and incident reporting across 11 sectors, from energy and communications to transport and data storage.[22] The 2023–2030 Cyber Security Strategy built on this foundation, introducing the concept of layered 'cyber shields' to protect national systems, extending obligations to cloud and software vendors, and preparing for post-quantum resilience. On paper, this gives Australia one of the Indo-Pacific's most advanced defensive postures.[23]

Yet AI-specific risks remain a gap. The SOCI Act compels operators to secure networks and disclose incidents, but it does not require algorithmic transparency, AI auditability or robustness testing. As one cyber security executive put it, 'we know how to mandate patching for software, but not for models that learn and adapt'. Threats such as data poisoning, adversarial prompts, model inversion or cascading failures fall outside reporting thresholds. This creates a paradox: operators may be fully compliant with the SOCI Act while still deploying AI systems that could behave unpredictably or be manipulated in ways regulators cannot yet capture.[24]

The 2023 strategy's ambition to embed resilience-by-design only partially addresses this challenge. Its focus on quantum readiness, cloud accountability and intelligence fusion is forward-looking, but it sidesteps the distinctive vulnerabilities of AI decision-making in critical systems. Participants warned that adversaries, from organised crime groups to hostile state actors, are increasingly likely to target AI itself, exploiting biases and weaknesses invisible to traditional network defences. One senior policymaker noted that 'it's the blind spot we'll be judged on,' pointing to the absence of any mandate for stress-testing AI once embedded in infrastructure.[25]

Governance adds another layer of complexity. Cybersecurity agencies focus on external intrusion, sectoral regulators on service reliability. When an algorithm fails inside the system, for example, by misrouting emergency calls, responsibility becomes blurred. Participants called this the 'governance grey zone', where no single agency feels fully accountable. Without dedicated assurance mandates, AI vulnerabilities risk slipping between institutional cracks.[26]

Even so, Australia begins from a position of strength. Its mature incident-response ecosystem and deep Five Eyes partnerships provide a solid base for adapting oversight to AI. Cyber authorities already run joint exercises with infrastructure operators, and several industry participants suggested that AI red-teaming could be folded into existing SOCI Act compliance audits. The task is less about building new bureaucracies than extending established ones to cover the algorithmic

Public–Private Collaboration: Mature Foundations, Modest on AI

Australia has long relied on public–private partnerships to protect its infrastructure, anchored in institutions such as the Critical Infrastructure Centre and the sector-based Trusted Information Sharing Networks (TISNs). These arrangements have created channels of trust between government, operators and technology providers, and they have proven their worth in traditional cyber risk management.[27]

When it comes to AI, however, these mechanisms are still developing. Few structured avenues exist for AI-focused threat modelling, joint testing or procurement standards. As several workshop participants remarked, collaboration is still evolving with many interactions 'relying on personal networks rather than formalised systems'. Some utilities and transport authorities maintain regular contact with government, but in many cases, AI deployments proceed with limited consultation.

Financial services represent a notable exception. Regulators including APRA, Australian Securities and Investment Commission (ASIC), Australian Competition and Consumer Commission (ACCC) and the Governor of the Reserve Bank of Australia have all spoken publicly on the risks of algorithmic systems, creating a more structured dialogue around AI.[28] This breadth of engagement provides a useful precedent for infrastructure regulators to follow.

The lack of shared testing environments compounds the problem. Australia has no dedicated AI testbed for critical infrastructure, no venue where operators, vendors and regulators can jointly trial systems under controlled conditions.

Building such facilities is beyond the capacity of individual operators, but without public leadership they rarely emerge, since the costs and risks are too widely dispersed. A hybrid model is needed. Government should provide the convening authority and initial investment, while operators and vendors contribute technical systems, data and co-funding. In the absence of this, projects either leap straight into production, carrying significant risks, or stall indefinitely at the pilot stage. As one infrastructure executive put it, 'if we had a safe place to break things, we'd all be more confident to build'. Another was blunter: 'Right now we either over-engineer solutions before they're tested, or we improvise in production. Both approaches are risky.' [29]

Trust between industry and government is necessary but no longer sufficient. As one technology executive put it: 'The collaboration exists, but it doesn't yet touch AI in a systematic way. We're still having yesterday's cyber conversations when tomorrow's risks are already here.'[30] That observation captures a wider unease: unless new structures are built, AI will slip through the cracks of otherwise mature cyber–infrastructure partnerships.

Closing that gap will require moving beyond ad hoc cooperation. Establishing formal testbeds, embedding AI into existing cyber collaboration frameworks, and creating structured dialogue platforms between industry and government would provide both confidence and guardrails for operators. If done well, these measures could convert Australia's established culture of cyber collaboration into a proactive model of AI resilience.

A Middle Power's Strategic Leverage

Australia occupies a distinct position as a middle power navigating an increasingly contested Indo-Pacific. Its decisions on AI and critical infrastructure governance matter not only for resilience at home but also for the credibility it projects abroad. Participants repeatedly stressed that the Australian Government's international influence derives less from technological scale than from its ability to model sound governance.[31]

By demonstrating how a democracy can weave AI into essential systems while maintaining transparency and assurance, Australia has the potential to shape regional and global norms. Mechanisms such as the Quad, AUKUS and ASEAN dialogues provide avenues to promote interoperable testing standards, secure supply-chain protocols and trusted AI frameworks. As one former senior policymaker warned, 'if we don't fill that governance space, someone else will, and it will most likely not be a democratic model'.[32]

Australia's impact is magnified when working with peers. Collaboration with Japan, Singapore and India on AI assurance could amplify middle-power voices in global standards-setting, ensuring that governance is not dictated solely by the United States or China. In this way, domestic policy choices double as foreign policy tools: the stronger and more coherent Australia's frameworks at home, the greater its leverage abroad.

The stakes are high. If Australia's approach remains incremental and uncoordinated, its ability to shape regional norms will diminish. But if it develops a consistent model that balances innovation with resilience, it has the chance to exercise disproportionate influence as a middle power in the emerging Indo-Pacific technology order.

Charting a Distinct Path Forward

For Australia, the challenge is not to reinvent AI governance from scratch but to bring coherence to a fragmented landscape. Sectoral pilots, the absence of a national assurance regime, and the opacity of vendor-led deployments all point to the need for structured integration. A credible path forward could rest on 3 interlocking moves:

Institutionalise assurance in critical infrastructure.

Creating a national AI registry for high-risk deployments in sectors such as energy, transport, water and health would provide visibility across systems that underpin daily life. Crucially, this scoping should distinguish between AI embedded in operational technology, where errors can trigger physical consequences in grids, pipelines or transport flows, and AI in IT environments, where failures are disruptive but less immediately existential. Coupled with mandatory resilience testing and a formalised sandbox for infrastructure AI, such a framework would give operators and regulators a common foundation for permissioned innovation, encouraging adoption while keeping systemic risks in check.

Embed AI into the cybersecurity architecture.

Australia's mature cyber backbone offers a strong base, but safeguards must now extend to AI itself. Embedding algorithmic auditability, incident reporting for AI-driven failures and systematic red-teaming against adversarial manipulation would align AI oversight with the rigour already applied to cyber threats. This would close the gap participants identified between external compromise and internal system fragility.

Leverage middle-power diplomacy to shape global standards.

Australia's credibility lies in linking domestic practice with international advocacy. If credible assurance is embedded at home, the Australian Government can use Quad, AUKUS and ASEAN platforms to push for interoperable testing regimes, resilient supply chains, and procurement norms that prioritise assurance. This is a strategic niche: not competing with the United States or China on scale but offering a democratic governance model that resonates across the Indo-Pacific.

Taken together, these moves would give Australia a coherent AI governance identity: risk-aware but forward-leaning, innovation-friendly yet resilience-orientated, and internationally influential because of its domestic vigilance. Rather than chasing deployment speed, Australia's contribution can be to prove that in critical infrastructure, slow and steady is not just prudent, it can be strategically decisive.

India | Strategic Autonomy Meets Digital Acceleration

India is racing to modernise and stands at a pivotal juncture in the Indo-Pacific's critical infrastructure and AI evolution. Its infrastructure networks are expanding at speed, its digital economy is growing exponentially, and its leadership routinely champions AI as a national priority. While India is a recognised innovator in digital public infrastructure (DPI) and large-scale AI deployment, it also wrestles with regulatory fragmentation, capacity gaps and significant cyber vulnerabilities. Against this backdrop, India will host the AI Impact Summit in February 2026, the first such gathering led by a major Global South nation. Following the United Kingdom's focus on 'safety' and France's on 'action', India's choice of 'impact' signals both ambition and an intent to shape the next phase of global AI governance.

Of the 4 Indo-Pacific countries examined in this report, India arguably has the most at stake in getting this right. It is a country of continental scale, regional influence, and strategic vulnerability. Its power grids stretch across multiple climate zones. Its urban population is swelling by millions each year. Its strategic infrastructure, ports, highways and logistic corridors will serve as the backbone of the economy and as key arteries for Indo-Pacific connectivity in the decades ahead.[33]

AI is already being deployed across these systems, to forecast energy demand, predict maintenance failures in railways, automate water distribution and streamline logistics. But the frameworks for ensuring that these technologies are safe, secure and resilient are still in formation. What India illustrates most clearly is the governance challenge of scale: the difficulty of regulating frontier technologies in a federal, fast-moving and politically complex environment.

Ambition Outpacing Architecture

India has made AI a national priority, but it does not yet have a national system for governing it. The 2018 National Strategy for AI set an ambitious vision, and more recently, the IndiaAI Mission has been established to build national capacity and foster innovation.[34] The 2023 Digital Personal Data Protection Act represents a major step forward in data regulation which indirectly puts some framing around certain data elements for model training and development. Yet India still lacks a dedicated legislative or institutional framework for overseeing AI use in critical infrastructure.[35]

Instead, AI adoption has proceeded through a mosaic of pilots, public–private partnerships and ministry-led innovation schemes. For example, the Ministry of Power supports predictive maintenance projects in energy grids. The Ministry of Railways has launched AI tools for dynamic scheduling and fault detection. The Ministry of Urban Affairs encourages the use of AI in smart city planning, and the Reserve Bank of India published a responsible AI framework.[36] But there is little integration across these efforts, no single authority empowered to coordinate AI deployment, evaluate systemic risks or certify safety.

The workshop found that AI functions are often embedded into vendor platforms with little disclosure or assurance, creating what participants described as a 'black box' reality. Here the concern was not model explainability, the usual sense of AI 'black boxes', but network visibility: operators often lack even a basic inventory of which AI systems are deployed and what models they rely on. As one senior technology provider noted: 'There's no inventory. We don't know what's been deployed, let alone what models are being used.'[37] This absence of visibility complicates incident response and magnifies supply-chain risk, underscoring why operators and regulators alike emphasised the importance of building transparent, sector-wide assurance frameworks.

The problem is compounded by India's federal structure. Some states invest heavily in AI-enabled systems, while others lag due to resource constraints, producing a patchwork that complicates national coordination.

This fragmented structure creates several risks. First, it limits institutional learning. Failures or vulnerabilities in one sector rarely inform governance in another. Second, it impedes accountability. When AI tools malfunction, for example, misallocating water during droughts, misclassifying security footage, or failing to alert during a system anomaly, there is no clear process for investigation or redress. Third, it opens the door to inconsistent standards. Infrastructure operators and state governments may adopt AI tools with widely varying levels of scrutiny, vendor oversight or technical capability. As one senior industry representative noted, 'the same AI system can be deployed with high assurance in one state and almost no oversight in another, there's no national baseline'.[38]

Federalism as Strength, and Constraint

Even when national strategies and policies exist, India's federal structure strongly shapes their implementation. Many of the sectors where AI is most rapidly being integrated – electricity distribution, water management, public transport – fall under the jurisdiction of state governments. This has enabled experimentation and innovation, but also produces significant disparity in digital maturity, procurement practice and cybersecurity readiness.

Some states, like Maharashtra, Karnataka and Tamil Nadu, have embraced AI in infrastructure planning and operations.[39] Others, particularly in the north-east and interior, have limited capacity to evaluate or integrate such tools effectively. 'At state level, procurement is driven by cost, not resilience, and that is a systemic risk,' one workshop participant stated.[40]

The central government's role, while influential, is often advisory rather than directive. Its ability to mandate AI risk standards or enforce interoperability protocols across the country remains limited. The result is a regulatory asymmetry of exposure. The same AI system used to manage rail crossing, for example, may be deployed with high assurance in one state and minimal oversight in another. In a country of over 1.4 billion people, such inconsistencies can magnify risk, especially as systems scale.

Cybersecurity in the Rearview Mirror

India's cybersecurity framework has improved significantly in recent years, including expanded threat monitoring by the Indian Computer Emergency Response Team (CERT-In). The 2020 National Cyber Security Strategy was announced with the promise of a more proactive government role in protecting critical infrastructure sectors. Public drafts and industry submissions are available, but a final, fully adopted version has not yet been officially published or operationalised. Enforcement remains largely reactive, after incidents rather than pre-emptively.

Existing obligations stop short of addressing the distinctive risks of AI systems. Under the 2022 CERT-In directions, operators across sectors must report specified cybersecurity incidents within 6 hours, retain logs for forensic use and cooperate with government investigations.[41] Sectoral regulators have also introduced requirements. The Reserve Bank of India mandates penetration testing and IT risk audits for financial operators, while the Central Electricity Authority enforces cybersecurity standards for grid operators. Yet none of these frameworks require AI-specific assurance measures such as adversarial testing, documentation of training data provenance or disclosure of model dependencies.

This gap is significant because AI is already embedded in platforms hosted abroad, maintained by foreign vendors and updated in ways operators cannot fully inspect. As one infrastructure provider observed during the workshop, 'we are deploying AI in water distribution, but governance always comes after deployment'.[42]

This lack of AI-specific cybersecurity governance creates 3 distinct risks:

Unseen vulnerabilities

India will continue to adopt AI systems at scale without meaningful visibility into their security risks.

Unprepared operators

Infrastructure providers will remain unprepared to handle the unique failure modes of machine learning (a subset of AI), such as data drift, adversarial inputs or model misclassification.

AI-enabled disruption

Public trust in infrastructure resilience could be undermined by a high-profile incident where an AI system itself fails or is manipulated to trigger cascading consequences.

The Private Sector Dilemma

India's private sector is at the centre of AI innovation, both as a developer of tools and as an operator of infrastructure. Major Indian firms are building predictive logistics models, smart grid systems and AI-enabled control platforms, often in partnership with global technology providers.[43]

But the private sector's incentives remain misaligned with the demands of public resilience. Procurement decisions are often guided by efficiency and cost savings rather than by assurance standards. 'Private operators treat AI as an efficiency play, not a national security question', observed one workshop participant.[44] Even in sectors designated as 'critical,' there are few structured mechanisms for government–private collaboration on AI governance. Information sharing tends to occur after incidents, not before. And operators rarely engage in joint scenario planning, red-teaming or stress testing with regulators.

Without a formal co-governance model, responsibility for infrastructure AI safety is diffused, and frequently deflected. This not only limits India's ability to respond to systemic threats but also weakens its leverage in setting regional norms and standards.

A recurring theme from the workshop was the disconnect between where technical capability resides and where policy decisions are made. India's deep AI and cybersecurity talent pool is overwhelmingly concentrated in the private sector, but public–private collaboration remains reactive and transactional. Government agencies often involve industry only after frameworks are drafted, missing opportunities for co-design that could embed operational realities into policy from the start.[45]

The notion of 'trusted AI' emerged as a particularly contested space, not just a technical metric, but a geopolitical and economic concept. For some, trust is about data provenance and algorithmic transparency, for others, it is about the geopolitical alignment of suppliers, control of model training and the sovereignty of cloud infrastructure. Without a shared definition, operationalising trust across sectors remains elusive.

Hardware-related vulnerabilities illustrate why this matters. The presence of Chinese-made Unisoc chips, with a 30% share of India's low-end mobile market in devices used by vulnerable populations, was cited as a case study in supply-chain risk. While hardware itself does not generate disinformation, compromised or insecure chips could provide a vector for surveillance or facilitate the delivery of manipulated content during sensitive periods such as elections. Participants called for a centralised malware repository, harmonised vetting mechanisms for suppliers and even bilateral or multilateral agreements to safeguard hardware and software supply chains.[46] While global tools such as VirusTotal already provide malware sharing, these are not tailored to India's infrastructure needs. Likewise, supplier vetting frameworks exist in fragments across sectors, but they remain inconsistent, and bilateral arrangements are largely ad hoc. What participants were emphasising was the absence of a coordinated, sovereign framework to bring together fragmented hardware and software supply-chain protections and translate them into systematic assurance for critical infrastructure.

From Ambition to Assurance

India's choices on AI governance will shape more than just its domestic infrastructure. As the country deepens its leadership role in the Global South, positions itself as a hub for trusted technology supply chains, and strengthens its strategic partnerships with the United States, Japan and Australia, its credibility will increasingly rest on its ability to deliver secure, scalable and principled technology adoption at home.

The strategic backdrop is inescapable. China is racing ahead on AI deployment, both in civilian infrastructure and in state-backed campaigns targeting critical systems abroad. For India, AI governance is therefore not only defensive, ensuring that critical infrastructure is insulated from foreign-manufactured models and hardware, but also an opportunity. Many countries are actively seeking non-Chinese suppliers of AI-enabled platforms. If India can align scale with assurance, it could emerge as a preferred provider of trusted AI systems for partners across the Global South. At the same time, India's role within BRICS alongside China and Russia adds another layer to this positioning, offering opportunities to shape Global South debates, while requiring careful calibration to maintain credibility with its Western partners.

Failure to build a robust governance framework for AI in critical infrastructure could therefore constrain India's influence abroad. Allies and partners may hesitate to integrate systems, share intelligence or co-invest in infrastructure if governance is seen as fragmented or opaque. At the same time, adversaries will view India's infrastructure ecosystems as attractive targets of opportunity, especially if they appear digitised but relatively poorly defended.

Despite the scale of the challenge, there is clear political momentum. Senior political leaders, from Prime Minister Modi down to state chief ministers, have demonstrated active interest in AI policy and digital public infrastructure.

At the conclusion of the workshop, 5 key imperatives for progress became clear:

Close the compute gap

Through investment in domestic AI infrastructure, from high-performance computing clusters and sovereign cloud capacity and semiconductor supply lines.

Embed cybersecurity by design in AI systems from the outset

Going beyond audits to systematic approaches such as adversarial red-teaming, automated stress testing and integrated incident-response protocols that anticipate vulnerabilities.

Define and operationalise 'trusted AI'

Requires cross-sector standards that clarify what constitutes trustworthy systems: provenance tracking to verify datasets, transparency benchmarks for explainability and supply-chain assurance to guard against tampering or insecure vendors.

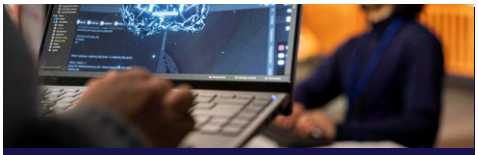
Accelerate its regulatory framework

Instead of waiting for perfect legislation, regulators can create experimental testbeds and sandboxes where norms are trialled, adapted and scaled, ensuring that the rule-making process keeps pace with the speed of technological change.

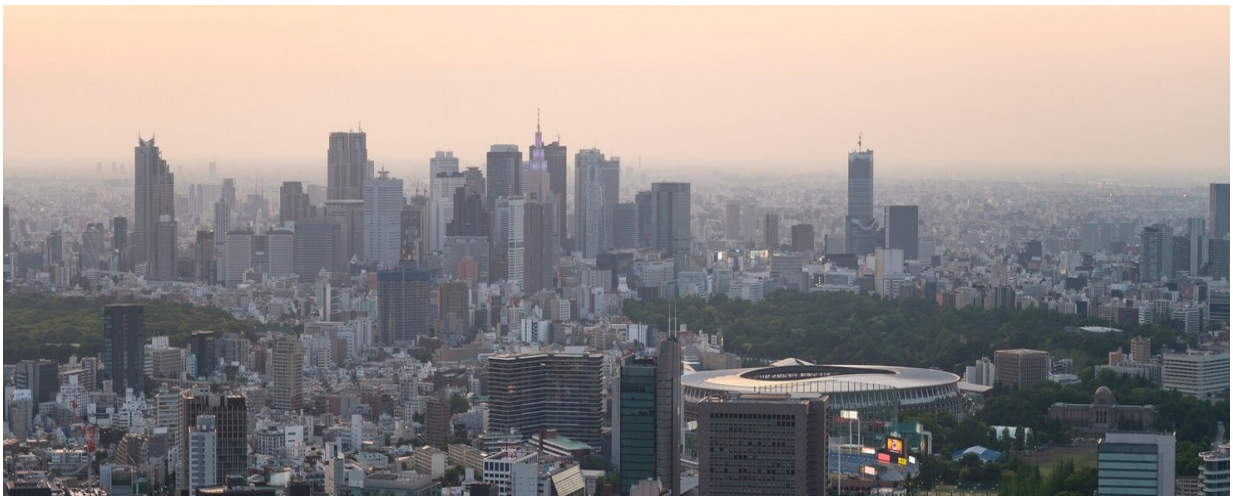
Expand skills and institutional capacity

Create joint programs with the private sector and government whereby secondments of technical experts into ministries and investments in public officials who can translate technical complexity into policy foresight becomes mainstreamed.

India illustrates both the promise and the potential difficulties of AI-enabled infrastructure. Its ambition is unquestionable, and its talent-base is world-class. But scale without safeguards creates a high degree of risk. By strengthening governance at home and embedding co-governance with partners, India can turn its size into a source of resilience, not vulnerability, and set a standard for the Indo-Pacific as a whole. The credibility will be on display in February 2026, when New Delhi hosts the AI Impact Summit. As the first Global South nation to lead this process, India's choice of 'impact' as its theme will showcase ambition, but its real test is not rhetoric, but assurance, proving that rapid adoption can be matched by robust, trusted and durable systems.



India illustrates both the promise and the potential difficulties of AI-enabled infrastructure.



Indonesia | Innovation Amid Institutional Flux

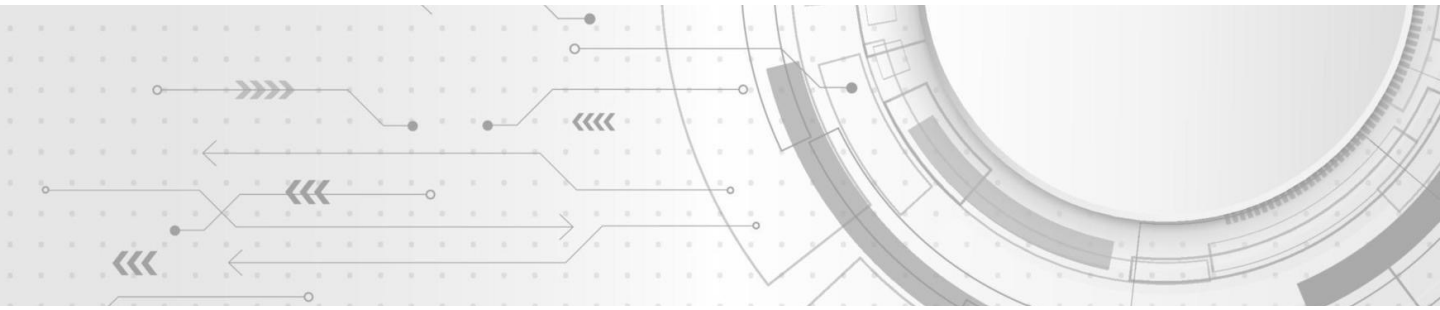
Indonesia, Southeast Asia's largest economy and most populous nation, stands at a crossroads in its approach to AI governance and critical infrastructure. With an archipelagic geography of more than 17,000 islands, where moving people, goods and data is both a developmental imperative and a national security challenge, AI offers much more than efficiency gains. In Government of Indonesia policy circles, it is increasingly framed as a cornerstone of resilience: a way to optimise energy distribution, anticipate and mitigate natural disasters, strengthen food security and manage sprawling transport systems. At the same time, the governance scaffolding to support this ambition has yet to fully take shape.

As one infrastructure operator put it, Indonesia has 'no shortage of pilots and prototypes, what's missing is the scaffolding to connect them into a resilient, trusted system'.[47]

A Nascent but Strategic AI Vision

Indonesia launched its National AI Strategy (Strategi Nasional Kecerdasan Artifisial 2020–2045) with the ambition of embedding AI in the nation's long-term development trajectory. The strategy outlined 5 priority sectors: healthcare, bureaucratic reform, education, food security, and mobility. While critical infrastructure was not explicitly mentioned, the broader thrust was unmistakable: AI would be central to achieving the nation's 'Golden Indonesia 2045' goals.

Yet the strategy has struggled to take root institutionally. Ownership has shifted between ministries; implementation has lacked cohesion and efforts to update or operationalise the strategy remain sluggish. There is currently no dedicated AI regulatory or independent oversight body, and coordination across ministries, particularly in infrastructure-intensive sectors like transport, energy and communications remain fragmented. As one policy advisor highlighted, 'our vision is strong, but without a permanent home for AI governance, execution will always be reactive'.[49]



AI in the Infrastructure Ecosystem

Despite uneven central coordination, AI tools are being deployed across several infrastructure domains, often through local government initiatives or pilot partnerships with the private sector. Jakarta's smart city programme, for example, uses AI to analyse traffic flows, predict flood patterns and manage public complaints through chatbot interfaces. PLN, the state-owned electricity company, is experimenting with AI to optimise load balancing and detect anomalies in power grids. In agriculture and fisheries, AI-powered satellite imaging is being trialled to monitor land use, predict yields and track illegal fishing.[50]

These initiatives demonstrate creativity and ambition, but they tend to be ad hoc and disconnected. Without a national framework for risk classification or deployment standards, there is limited assurance that such systems are secure, interoperable or accountable to end-users. As one policy expert noted: 'In physical infrastructure, we have safety codes and engineering standards. For AI, we have nothing equivalent.'[51]

Governance Gaps and Cybersecurity Blind Spots

Indonesia's cybersecurity architecture is still evolving. The National Cyber and Crypto Agency (BSSN), established in 2017, has primary responsibility for cybersecurity policy but remains constrained by limited resources, a broad mandate and insufficient authority over sectoral regulators. One senior technology provider observed that while the BSSN provides a foundation, 'its capacity to oversee AI-specific risks, from adversarial attacks on learning systems to data poisoning or deepfakes, is still limited'. These risks are not yet addressed in national cybersecurity guidelines.

The 2022 Personal Data Protection Law marked a step forward for digital governance but omits AI-specific provisions relevant to critical infrastructure. Nor does Indonesia have a binding equivalent of Singapore's Cybersecurity Act or Australia's SOCI Act, which establish risk management and incident reporting obligations for operators. One infrastructure provider summed up the concern starkly: 'Our systems may be modernising, but our threat models are still stuck in 2010.'[52]

In the absence of regulatory scaffolding, infrastructure operators rely on general-purpose cybersecurity standards or voluntary corporate practices. Risk assessments are infrequent, incident reporting is inconsistent and public–private information sharing is still in its early stages. This lack of visibility creates fertile ground for both domestic vulnerabilities and foreign interference, particularly as geopolitical competition intensifies around digital infrastructure nodes in the Indo-Pacific. Yet Indonesia's relatively early-stage regulatory architecture also presents an opportunity. With fewer legacy constraints it could design AI assurance frameworks that leapfrog older models and position itself as a regional standard-setter.

The Private Sector as Early Mover

Indonesia's AI ecosystem is increasingly driven by the private sector. Technology platforms, system integrators and startups are leading the rollout of AI-based infrastructure tools, from predictive maintenance to digital twins. Major telecom providers like Telkom Indonesia and Indosat are experimenting with AI for network optimisation and 5G infrastructure deployment.[53] Fintech and Healthtech companies are applying AI models for identity verification and service triage, often in ways that intersect with state systems.

This dynamism is a strength, but it remains decoupled from public governance. Few formal mechanisms exist for coordinated procurement, co-regulatory experimentation or cybersecurity assurance. As a result, innovation often outpaces oversight. As a senior technology expert warned, 'we can build cutting-edge AI tools, but there's no national process to prove they're safe before they touch critical systems'.[54]

If structured engagement can be institutionalised, through shared sandboxes, procurement standards or joint stress-testing, Indonesia could harness its private sector dynamism as an engine for resilience rather than a source of unmanaged risk.

The Geopolitical Dimension

Indonesia's AI governance trajectory is unfolding in a competitive regional environment. As the world's fourth most populous country and a pivotal Indo-Pacific state, the Government of Indonesia is under increasing pressure to define rules for emerging technologies in ways that safeguard sovereignty while remaining open to foreign investment and innovation.

China's technology footprint in Indonesia, from Huawei's role in telecoms infrastructure to Alibaba Cloud's expansion, has already shaped AI adoption patterns. At the same time, Japan, South Korea and the United States are funnelling development finance and strategic investments into Indonesian digital infrastructure. This competition provides Indonesia with capital, technology and know-how that can accelerate AI deployment. But it also creates dependencies – over-reliance on external vendors, platforms and finance – that can leave Indonesia vulnerable to political leverage, shifting terms of access or embedded security risks. Participants noted that without robust vetting of foreign-supplied hardware and software, the country risks importing not just capability but also exposure to risk.

The absence of clear AI security standards magnifies this dilemma. Indonesia has room to act as a 'swing state' in AI governance, able to draw investment from multiple partners while shaping rules that reflect its own interests. But unless the Government of Indonesia can set assurance benchmarks that cut across these partnerships, it risks ceding control of its infrastructure ecosystems to the very powers whose competition it seeks to balance.

As one national security official observed, 'we have to balance openness with sovereignty; AI is no different from any other strategic resource'.[55]

Charting a Strategic Path Forward

For Indonesia, the challenge is not about whether AI will enter the operational core of its critical infrastructure – it already has. The question is whether governance can keep pace. A successful path forward would rest on 3 key priorities:

Institutional clarity and leadership

Establishing a lead AI agency or coordinator to unify oversight, align strategies across ministries and integrate AI governance into national security and development planning.

Cybersecurity modernisation

Expanding the BSSN's mandate, resourcing and partnerships to develop AI-specific infrastructure protection standards, while enhancing operator capacity for threat detection and mitigation.

Structured public–private engagement

Creating structured channels for shared risk assessments, technology certification and operational exercises between government, infrastructure providers and AI developers.

Indonesia has the capability, ambition and geopolitical weight to shape AI-enabled infrastructure resilience in Southeast Asia. Its choices will determine whether AI becomes an accelerator of development or a new vector of vulnerability. By coupling its vibrant private sector with stronger regulatory scaffolding, and by embedding AI governance within both domestic institutions and regional diplomacy, the Government of Indonesia could position itself as a standard-setter rather than a standard-taker. The alternative is a future where innovation races ahead but resilience lags, leaving the country exposed at precisely the moment it seeks to project stability and leadership on the regional stage.

Singapore | Enabling Trusted Innovation at Scale

Among Indo-Pacific nations, Singapore has emerged as the most institutionally advanced in governing AI in critical infrastructure. Its approach is not driven by scale, urgency or sheer demand, as in India or Indonesia, but by an intentional strategy to shape global AI norms, institutionalise responsible innovation and de-risk adoption through calibrated, anticipatory regulation.[56]

Singapore's model rests on 3 pillars: strategic foresight, legal codification, and trust as a service. It has positioned itself as an early adopter of AI technologies in public infrastructure and as a policy lab for governance innovation. It offers a model of how smaller states can exert outsized influence in setting global standards.

A Vision Anchored in Governance

Singapore's approach to AI has always been about more than productivity. From the outset, the government has viewed AI as a strategic enabler of national competitiveness and social cohesion. The launch of its National AI Strategy in 2019 reflected this dual ambition: to transform the economy and enhance lives, while reinforcing trust in digital systems.

The updated National AI Strategy 2.0, released in December 2023, sharpened this focus, identifying key 'National AI Missions' in healthcare, finance, logistics and public services. Importantly, it expanded Singapore's ambitions from sectoral transformation to ecosystem leadership, seeking to position the country as a global hub for trusted AI.[57] Participants noted that delivering on these ambitions will also require sustained investment in people. Building deep, domain-specific AI expertise for critical industries takes time, and long-term training pathways and career development schemes will be needed to ensure Singapore maintains the specialised talent to deploy and test mission-critical systems.

Rather than pursuing rapid horizontal adoption of AI across all infrastructure domains, Singapore has targeted specific high-impact use cases and built structured frameworks to govern them.[58] For example, AI is used to manage port logistics at PSA Singapore, to optimise energy use in smart buildings and to enhance predictive maintenance across public transport systems. In each case, technical deployment is accompanied by explicit procurement standards, cybersecurity protocols and assurance mechanisms.

Workshop participants consistently described this as 'principles without dogma', a framework flexible enough to evolve, yet clear enough to command industry buy-in. As one senior policymaker observed: 'Regulation done too early freezes innovation. Regulation done consultatively creates buy-in.'[59]

Regulation as a Living Process

Singapore's strength lies in its ability to align policy, regulation and implementation. The Model AI Governance Framework and AI Verify testing toolkit, launched in 2022 and updated in 2024, provide guidance rather than hard mandates, enabling companies to assess their systems against fairness, explainability, robustness, safety and security principles.[60] This is supported by extensive industry engagement: firms reported participating in multiple consultation rounds with the Infocomm Media Development Authority (IMDA) and the CSA of Singapore, building not only better governance but deeper trust.[61]

This restraint is strategic. Principle-based standards avoid locking in requirements that may rapidly date, while agencies quietly embed AI-specific considerations into existing risk frameworks, particularly where AI intersects with OT or network infrastructure.[62] The Singapore Government's evolving guidance on AI governance and testing, audit protocols and tiered oversight reflects a readiness to seed assurance measures in critical sectors, without closing the door on innovation.

AI and Critical Infrastructure: A Converging Agenda

AI is increasingly woven into Singapore's infrastructure fabric. In water management, the Public Utilities Board deploys smart sensors coupled with AI-driven analytics to refine models of consumption patterns, optimise distribution and detect anomalies before they become crises. The Energy Market Authority uses AI to anticipate demand surges, smooth the integration of renewable sources and maintain balance in the national grid. On the roads, the Land Transport Authority's next-generation Electronic Road Pricing system recalibrates congestion charges in real time, responding to shifting traffic flows.[63] Binding these capabilities together is the Smart Nation Sensor Platform, a vast network that aggregates data from Internet of Things (IoT) devices across the island, feeding insights that range from early flood warnings to live traffic optimisation.

Singapore also recognises the cyber-physical convergence risks associated with these systems. AI tools operating at both the OT and IT network layers can introduce new failure modes, from cascading system errors to adversarial manipulation. In response, the CSA has issued detailed OT cybersecurity guidelines and is now working on AI-specific guidance for critical infrastructure contexts, a move described by one government official as 'designing AI assurance frameworks now because we don't want to be caught flat-footed later'.[64] Participants also noted that access to high-quality datasets remains a limiting factor in critical industries, suggesting that frameworks for public–private data sharing, or curated government-managed test sets, could further strengthen Singapore's trusted environment for AI.

Cybersecurity in the Age of AI

Unlike its regional peers, Singapore explicitly links AI deployment with cyber resilience, taking a proactive approach to cybersecurity. The government's Cybersecurity Strategy 2021, reinforced by the Cybersecurity Act and the creation of the CSA highlights this proactive approach.[65] AI systems used in critical infrastructure are subject to the same rigorous cybersecurity standards as other critical assets. The CSA works closely with both private sector organisations and international partners to ensure that AI deployments in these sectors are secure and resilient. Furthermore, the CSA has been active in creating cybersecurity standards and guidelines for AI, which are particularly relevant as the adoption of AI in infrastructure becomes more pervasive.[66] These standards aim to ensure that AI systems used in the critical infrastructure sector adhere to best practices in terms of data security, risk management and system transparency.

Despite these measures, Singapore is mindful that as AI technologies evolve, the challenges surrounding cybersecurity will become even more pronounced, requiring continuous monitoring and adaptation of security frameworks. The nation's experience in cybersecurity governance offers valuable lessons for other countries balancing innovation with robust security measures.

Participants praised CSA for its 'dialogue over diktat' style in creating an investment climate grounded in trust. 'We've had 5 years of trust-building with the government. That's why we invest here', one private-sector leader noted.[67] Yet challenges remain as cross-jurisdictional operations, multi-cloud architectures and managed service models can blur accountability. Questions over liability, breach notification and contractual alignment persist, particularly in cross-border contexts.

Singapore's answer has been twofold: invest in local cybersecurity talent and trusted vendors, while extending its reach through active international dialogue and collaboration. Beyond strengthening its domestic ecosystem, Singapore has sought to shape the regional and global conversation on technology governance by engaging in both bilateral partnerships and multilateral platforms. Regional capacity building has been central to this approach, exemplified by initiatives such as the ASEAN-Singapore Cybersecurity Centre of Excellence. At the same time, Singapore has contributed to broader global efforts through forums such as the United Nations, and the Organisation for Economic Co-operation and Development (OECD), ensuring its trusted environment principles align with and help inform international standards.

Technical Leadership as Diplomatic Currency

Singapore's AI governance model is designed not only for domestic assurance but for international alignment. It is a founding member of the Global Partnership on AI (GPAI), contributes to the OECD's AI policy work, and is actively shaping ASEAN AI governance norms through its chairmanship of ASEAN's Workgroup on AI Governance. Singapore's AI Verify Foundation, launched in 2023, aims to position its assurance frameworks as globally adoptable standards, especially for fast-developing economies seeking light-touch but credible approaches to AI governance.[68] This outward-facing strategy reflects a key insight: that trust is a trade and diplomatic asset. As cross-border data flows, digital services and infrastructure integration deepen across the Indo-Pacific, interoperable trust frameworks will become essential. Singapore's bet is that those who can enable trust at scale will be central to the next phase of digital geopolitics. As one former national security official reflected: 'Once you take geopolitics off the table and ask how do we make you more cyber secure? Things get done.'[69]

Risks and Strategic Limits

Singapore's AI and critical infrastructure strategy occupies a distinctive middle ground in a world increasingly split between no regulation and rigid state control. It is an architecture built for precision without prescription, pairing regulatory foresight with the agility to adapt as technologies and risks evolve. This model is not without its constraints. Singapore's small size enables administrative cohesion and rapid policy experimentation that larger, deferral systems may find difficult to replicate. Its tightly managed political environment supports long-term planning but can narrow the space for public debate on controversial or emergent AI risks, from biometric surveillance to algorithmic bias in policing.

Much of Singapore's success rests on its ability to steer private sector behaviour collaboratively through non-legislative means, guidelines, incentives, sandboxes and reputational cues, rather than through prescriptive lawmaking. This approach relies heavily on sustained government credibility and on companies' willingness to engage in good faith. Should international firms redirect their compliance priorities elsewhere, or domestic stakeholders demand stronger AI rights and remedies, the delicate balance between trust and efficiency could come under strain.

Looking forward, 3 interlinked forces are set to shape Singapore's trajectory:

Institutionalise AI assurance in critical sectors

Build on voluntary tools such as AI Verify by embedding binding, sector-specific requirements that ensure transparency, robustness and resilience in the systems that underpin national security and daily life.

Secure digital infrastructure sovereignty

Continue to attract foreign capital and expertise, but maintain decisive control over operational risk, cloud governance and the terms of technological dependency, so that openness does not dilute strategic autonomy.

Deepen cross-border collaboration

Expand efforts to align accountability frameworks and assurance models with regional and global partners, recognising that AI supply chains and infrastructure networks are inherently transnational.

Singapore's blend of agility, anticipation and exportable governance practices positions it uniquely in the Indo-Pacific. By focusing less on grand pronouncements and more on building an enduring foundation for trusted, interoperable systems, it offers a credible and influential alternative for states seeking to navigate the contested and rapidly shifting digital order.

Country Spotlight Conclusions

The country spotlights underscore how unevenly the Indo-Pacific is adapting to the challenge of embedding AI in critical infrastructure. Each state faces distinct constraints: resilience-first caution in Australia, federal complexity in India, institutional flux in Indonesia, and assurance-led governance in Singapore. Yet common themes emerge: fragmented oversight, growing dependence on foreign vendors, and a widening gap between rapid deployment and the safeguards needed to secure trust.

These shared vulnerabilities point to a larger question that no country can resolve alone: how to build interoperable frameworks and cooperative mechanisms that can contain cross-border risks. It is to these regional pathways, and the strategic choice they entail that the report now turns.

Part 3

Strategic Pathways Forward

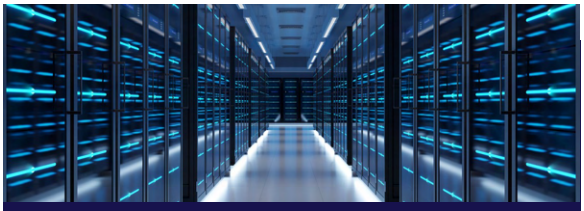
Part 3 examines the strategic pathways available to the region as a whole, considering how national efforts can be reinforced by regional cooperation, public–private co-governance and international standard setting. If Part 2 traced the contours of national experiments in governing AI, this section asks how those experiments can be stitched together into a framework for regional resilience, one that balances innovation with assurance, sovereignty with interdependence and domestic priorities with the realities of cross-border systems.

Governing AI as Infrastructure

The Indo-Pacific has become the world's engine of digital adoption as well as a proving ground for how to govern technologies that outpace existing institutions. Australia, India, Indonesia and Singapore each face distinct dilemmas in embedding AI into critical infrastructure, yet their experiences reveal common pressures. What makes this challenge distinct is the combination of velocity and vulnerability. Unlike earlier waves of digitisation, where technologies entered incrementally, AI is being incorporated rapidly into the operational core of grids, transport systems, logistics hubs and emergency services. As these systems learn, adapt and operate autonomously, the consequences of failure grow more severe and vulnerabilities are magnified across interconnected regional networks.

Divergent governance approaches are compounding these risks. Different standards make it difficult for operators to know which rules apply, and they complicate coordination in times of crisis. Regional strategic competitors are alert to these gaps. State-backed cyber actors already target infrastructure nodes as sites of leverage. In this environment, fragmentation is not just an administrative challenge but a structural weakness.

If there is a lesson that emerges across the country chapters, it is this: the Indo-Pacific cannot afford to treat AI in critical infrastructure as a domestic issue alone. Just as undersea cables, cloud platforms and power grids cross jurisdictions, so too must the frameworks that govern their algorithmic control. The task is therefore to build a regional framework for resilience, not a monolithic treaty or a single 'AI Act for infrastructure' but as a set of interoperable norms and practices that make national systems safer to run and easier to repair when they fail.



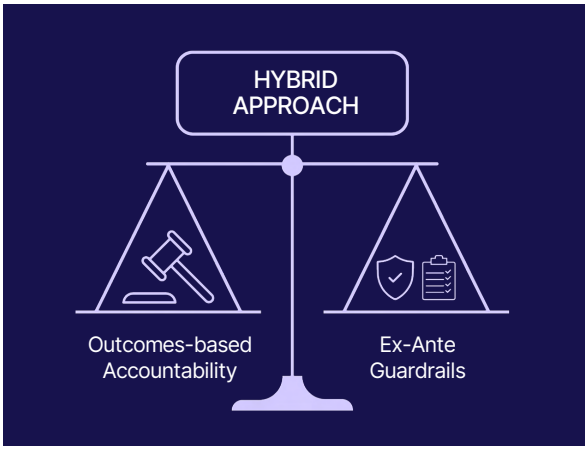
The Indo-Pacific cannot afford to treat AI in critical infrastructure as a domestic issue alone.

Guardrails and Governance Choices

The path to such a framework runs directly through a debate now unfolding in every capital: whether to regulate AI in critical infrastructure through outcomes-based accountability or through ex-ante guardrails. The former relies on strengthening liability after harm has occurred, punishing negligence, tightening rules and deterring future lapses. The latter demands safeguards before deployment, mandated testing, transparency requirements and structured fallback mechanisms designed to prevent harm in the first place.

This is not an abstract argument. It is the same dilemma that has haunted cybersecurity policy for decades. Australia and Singapore only moved decisively to impose obligations on operators after successive 'wake-up call' intrusions forced their hand. India's data protection law came after years of high-profile privacy breaches. Indonesia's move toward comprehensive cybersecurity legislation reflects a lack of political urgency until incidents accumulate.

AI magnifies the stakes of this choice. Waiting for outcomes before acting means waiting for failures in systems that are increasingly safety critical. A water allocation algorithm that prioritises industry during a drought, or a predictive maintenance system that misses a transformer fault, may not simply be inefficiencies; they may become national emergencies. On the other hand, imposing blanket ex-ante obligations too early risks stifling innovation in countries where capacity is scarce and experimentation essential.



The more realistic path is a hybrid approach, managing low-consequence AI primarily through outcomes-based liability, while requiring preventative guardrails for high-consequence systems. Just as building codes emerged to govern physical infrastructure, assurance regimes must now govern digital ones. These guardrails need not be identical across jurisdictions, but they must be sufficiently interoperable to allow systems that cross borders, ports, grids or logistics chains to function without introducing new seams of vulnerability.

From Compliance to Co-Governance

Any credible strategy for AI in critical infrastructure must start from the understanding that the state does not own most of the systems that it now depends. Critical infrastructure in the Indo-Pacific is largely privately operated, and many AI models come from vendors headquartered abroad. This creates a sovereignty dilemma: governments remain responsible for resilience yet depend on technologies they do not control. Compliance audits and contractual obligations provide limited assurance. What is required is a reconfiguration of the state-market relationship: a shift from compliance to co-governance.

Singapore's example illustrates what this can look like. Its Cybersecurity Act mandates information sharing and incident reporting, but more importantly, the government has invested in building trust-based channels where private operators and regulators collaborate on testing, simulation and standard-setting. Australia's TISNs serve a similar function, although they remain focused on established cyber threats rather than emerging AI risks. In India and Indonesia, engagement is patchy and often informal. Moving toward structured co-governance would mean institutionalising joint risk assessments, shared incident simulations and agreed standards of assurance.

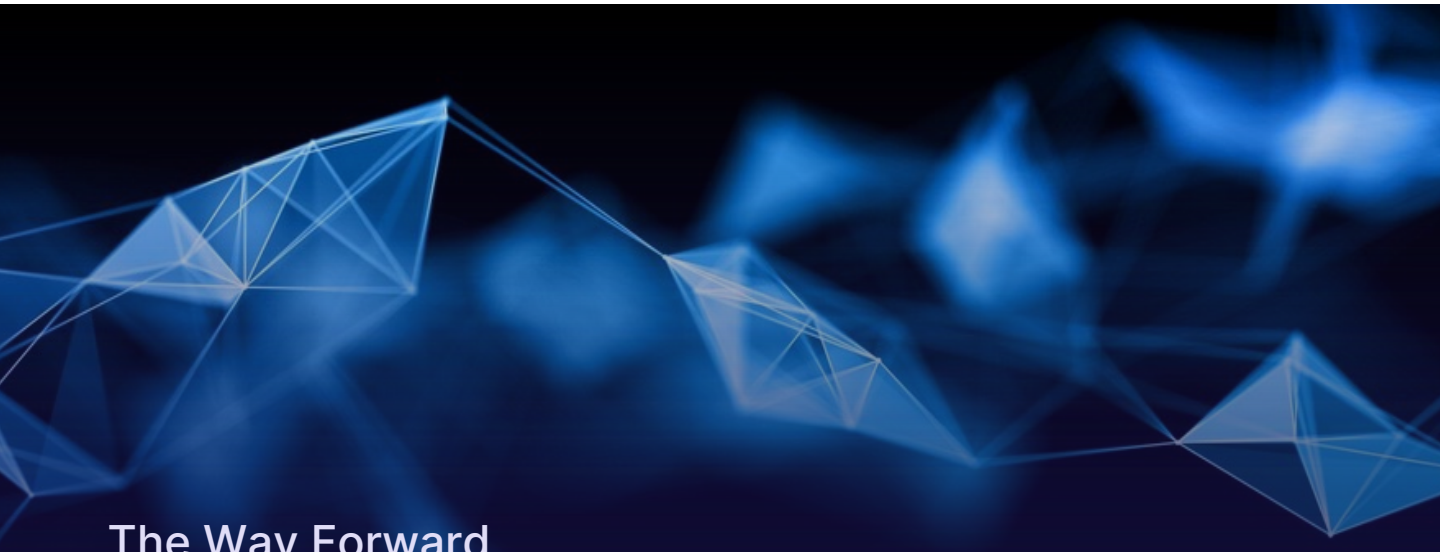
Regulation should not be seen as a brake but as an enabler. Clear obligations, transparent thresholds, and predictable rules give firms the certainty to invest and innovate within defined boundaries. Ambiguity, by contrast, leads to hesitation.

Diplomacy and Standards

Beyond the national and corporate spheres lie the regional and geopolitical ones. The Indo-Pacific is already a contested terrain for technological standards. China's efforts to export digital infrastructure through the Digital Silk Road, and to shape norms through standards bodies, are matched by United States and Australian initiatives and growing European regulatory influence. Middle powers such as Japan, South Korea and India are increasingly active in proposing alternative models.

For Australia, India, Indonesia and Singapore, the focus should be on pursuing domestic resilience as well as positioning themselves in this global standards contest. The region's ability to articulate credible, interoperable approaches to AI in critical infrastructure will determine whether it is a rule-taker or a rule-shaper. If ASEAN, the Quad or AUKUS can converge on common definitions of high-risk AI uses, shared principles or assurance and joint incident-response protocols, they will set a template that others may follow. If they cannot, the vacuum will be filled by external powers, leaving the region to adapt to rules written elsewhere.

There is an opportunity to leverage existing diplomatic platforms as vehicles for practical convergence. ASEAN's Digital Ministers meetings could host the development of a regional glossary of AI risk categories. The Quad, already collaborating on critical technologies, could pilot joint testbeds for AI in power grids or ports. AUKUS with its deep security integration, could quietly extend its collaboration to red-teaming AI models in defence and dual-use infrastructure. These initiatives need not produce uniform regulation. What matters is that they reduce the friction of operating across borders, build habits of trust and signal to adversaries that AI-related vulnerabilities in infrastructure will not be exploited in a vacuum.



The Way Forward

The Indo-Pacific stands at an inflection point. AI has already become infrastructure, but the institutions, norms and partnerships needed to govern it are still under construction. The country chapters in this report have shown 4 paths: Australia's risk-aware but cautious posture, India's rapid adoption but lagging coherence, Indonesia's leapfrogging innovation amid fragile governance, and Singapore's anticipatory regulation and soft-power ambition. Each offer lessons for the region.

The common thread is the recognition that fragmentation is a vulnerability. Divergent national approaches create uneven incentives, invite regulatory arbitrage and complicate cross-border crisis management. Yet fragmentation is not destiny. The Indo-Pacific can still choose to converge around shared principles, interoperable practices and co-governance models that balance sovereignty with interdependence.

This report has argued for a framework that treats AI in critical infrastructure as a public risk, not merely a private innovation.

That means recognising the distinction between high-consequence and low-consequence use cases, imposing preventative guardrails where failures would cascade and building the institutional muscle for continuous assurance. It means re-casting regulation as an enabler of innovation, not a barrier to it. And it means embedding AI governance within the region's diplomatic architecture, so that shared systems come with shared standards and shared responsibilities.

The stakes are clear. If Indo-Pacific governments act individually and belatedly, they will face a future of proliferating AI deployments governed by uneven rules, prone to systemic failure and vulnerable to geopolitical exploitation. If they act collectively and early, they can build a model of democratic resilience that demonstrates to the world how AI can be harnessed without sacrificing sovereignty or safety.

History offers a reminder. The safety codes and engineering standards that underpinned the 20th century's great infrastructure projects, from bridges to aviation, were not inevitable. They were forged through trial, tragedy and eventually coordination. The Indo-Pacific has the chance to learn faster, to build the guardrails before the crisis and to shape a digital order that reflects its own priorities. The choice is not whether AI will run the region's critical infrastructure – it already does. The choice is whether the region will govern it in time.

Glossary

Term	Description
ACCC	Australian Competition and Consumer Commission
AI	Artificial intelligence
AmCham	American Chamber of Commerce in Australia
APRA	Australian Prudential Regulation Authority
ASEAN	Association of Southeast Asian Nations
ASIC	Australian Securities and Investments Commission
AUKUS	Trilateral security partnership between Australia, the United Kingdom and the United States.
BRICS	A bloc of emerging economies, Brazil, Russia, India, China and South Africa cooperating on economic, political and global governance.
BSSN	National Cyber and Crypto Agency (Indonesia)
CERT-In	Computer Emergency Response Team (India)
CSA	Cyber Security Agency (Singapore)
DPI	Digital public infrastructure
GPAI	Global Partnership on AI
IMDA	Infocomm Media Development Authority (Singapore)
Indo-Pacific	A geopolitical region covering nations and islands surrounding the Indian Ocean and Pacific Ocean.
IoT	Internet of Things
IT	Information technology
OECD	Organisation for Economic Co-operation and Development
OT	Operational technology
PPP	Public–private partnership
Quad	A grouping or partnership between Australia, India, Japan and the United States, focused on regional security, technology, and economic cooperation in the Indo-Pacific.
SOCI Act	Security of Critical Infrastructure Act 2018
TISNs	Trusted Information Sharing Networks

References

[1] AI Asia Pacific Institute, Annual report 2024, AI Asia Pacific Institute, Singapore, 2024.

[2] United Nations Economic and Social Commission for Asia and the Pacific, Study on small port reforms and port digitisation in Asia-Pacific, UNESCAP, 2024.

[3] B Kaye, 'Google to help build cyber protection for Australian infrastructure', Reuters, 21 August 2024 and J Taylor, 'Qantas attack reveals one phone call is all it takes to crack cybersecurity's weakest link: humans', The Guardian, 6 July 2025.

[4] Workshop insight taken from meeting held on 2 July 2025 in New Delhi, India.

[5] Workshop insight taken from meeting held on 10 July 2025 in Jakarta, Indonesia.

[6] AI Verify Foundation, What is AI Verify?, AI Verify Foundation website, n.d.

[7] Australian Government, Security Legislation Amendment (Critical Infrastructure) Act 2021, Australian Government, 2021.

[8] P Suraksha, 'India's long wait for data protection law', The Economic Times, 11 August 2025.

[9] S Widianto, 'Indonesia targets foreign investment with new AI roadmap', Reuters, 22 July 2025.

[10] PWC, The new equation to protect Australia's critical infrastructure, February 2022.

[11] Workshop insight taken from meeting held on 2 July 2025 in New Delhi, India and meeting held on 10 July 2025 in Jakarta, Indonesia.

[12] Workshop insight taken from meeting held on 7 July 2025 in Singapore.

[13] Critical Infrastructure Security Centre, Security of Critical Infrastructure Act, Australian Government, 2018.

[14] Workshop insight taken from meeting held on 30 June 2025 in Canberra, Australia.

[15] Workshop insight taken from meeting held on 30 June 2025 in Canberra, Australia.

[16] Department of Industry, Science and Resources, Supporting responsible AI: discussion paper, Australian Government, 2023.

[17] Department of Industry, Science and Resources, Introducing mandatory guardrails for AI in high-risk settings: Proposals paper, Australian Government, 2024.

[18] Select Committee on Adopting Artificial Intelligence, Final Report, Parliament of Australia, 2024.

[19] Sustainable Future Australia, Smart energy forecasting: how AI is revolutionizing Australia's power grid, Sustainable Future Australia website, 2025.

[20] Infrastructure Magazine, 'Smart tech making Sydney's roads safer', Infrastructure Magazine, 19 November 2024.

[21] Workshop insight taken from meeting held on 30 June 2025 in Canberra, Australia.

References

[22] Department of Home Affairs (2022) Security legislation amendment (Critical infrastructure protection) Act 2022, Australian Government, 2022.

[23] Department of Home Affairs, 2023–2030 Australian Cyber Security Strategy, Australian Government, 2023.

[24] Workshop insight taken from meeting held on 30 June 2025 in Canberra, Australia.

[25] Workshop insight taken from meeting held on 30 June 2025 in Canberra, Australia.

[26] Workshop insight taken from meeting held on 30 June 2025 in Canberra, Australia.

[27] Department of Home Affairs, Critical Infrastructure Resilience Strategy, Australian Government, 2023.

[28] APRA, Remarks to the AFIA Risk Summit 2024, APRA website, 2024 and ASIC, ASIC move to modernise trading system rules to keep pace with technology and AI, ASIC Newsroom, 27 August 2025.

[29] Workshop insight taken from meeting held on 30 June 2025 in Canberra, Australia.

[30] Workshop insight taken from meeting held on 30 June 2025 in Canberra, Australia.

[31] Workshop insight taken from meeting held on 30 June 2025 in Canberra, Australia.

[32] Workshop insight taken from meeting held on 30 June 2025 in Canberra, Australia.

[33] World Bank, Benchmarking Infrastructure Development 2023, Washington, DC, 2024.

[34] Ministry of Electronics and IT, IndiaAI Mission Framework, Government of India, 2024.

[35] A Mohanty A and S Sahu, India's Advance on AI Regulation, Carnegie, India, 2024.

[36] The Reserve Bank of India, FREE-AI Committee Report – Framework for Responsible and Ethical Enablement of Artificial Intelligence, 2025.

[37] Workshop insight taken from meeting held on 2 July 2025 in New Delhi, India.

[38] Workshop insight taken from meeting held on 2 July 2025 in New Delhi, India.

[39] World Economic Forum, How government can attract innovative manufacturing industries and promote 4IR technologies like AI, World Economic Forum website, 24 June 2024.

[40] Workshop insight taken from meeting held on 2 July 2025 in New Delhi, India.

[41] Ministry of Electronics and Information Technology, Directions under sub-section (6) of section 70B of the IT Act, Government of India, New Delhi, 2022.

[42] Workshop insight taken from meeting held on 2 July 2025 in New Delhi, India.

[43] Economic Times, Indian IT giants bet big on AI, rewire business DNAs for AI-driven future, CIO.com, 2025.

[44] Workshop insight taken from meeting held on 2 July 2025 in New Delhi, India.

[45] Workshop insight taken from meeting held on 2 July 2025 in New Delhi, India.

References

[46] Workshop insight taken from meeting held on 2 July 2025 in New Delhi, India.

[47] Workshop participant, 10 July 2025, Jakarta.

[48] Asia Society Policy Institute, Raising Standards: Data and Artificial Intelligence in Southeast Asia – Indonesia, Asia Society Policy Institute website, 2022.

[49] Workshop participant, 10 July 2025, Jakarta.

[50] United Nations Climate Change Technology Executive Committee, Urban flood management in Jakarta, United Nations Climate Change, 2023.

[51] Workshop participant, 10 July 2025, Jakarta.

[52] Workshop participant, 10 July 2025, Jakarta.

[53] OpenGov Asia, 'Indonesia: Public-Private Partnerships to Drive Digital Ecosystem', OpenGov Asia, 19 July 2025.

[54] Workshop participant, 10 July 2025, Jakarta.

[55] Workshop participant, 10 July 2025, Jakarta.

[56] M-Y Ho, Singapore's National Strategy in the Global Race for AI, Konrad Adenauer Stiftung, Singapore, 2024.

[57] Smart Nation and Digital Government Office, National AI Strategy 2.0, Smart Nation Singapore website, 2023.

[58] Y Sivakumar, 'DPM Lawrence Wong unveils Singapore's National AI Strategy 2.0', Vulcan Post, 5 December 2023.

[59] Workshop insight taken from meeting held on 7 July 2025 in Singapore.

[60] IMDA, Singapore launches world's first AI testing framework and toolkit to promote transparency, Infocomm Media Development Authority, 25 May 2022.

[61] AR Choudhury, 'Singapore's AI verification framework welcomed by industry', IT News Asia, 30 May 2022.

[62] YZ Kin, Singapore's AI Verify builds trust through transparency, OECD.AI, 16 August 2022.

[63] M-Y Ho, Singapore's National Strategy in the Global Race for AI, Konrad Adenauer Stiftung, Singapore, 2024.

[64] Workshop insight taken from meeting held on 7 July 2025 in Singapore.

[65] Cybersecurity Agency of Singapore, Singapore Cybersecurity Strategy 2021, CSA, Singapore, 2021.

[66] Cybersecurity Agency of Singapore, Companion Guide on Securing AI Systems, CSA, Singapore, 2024.

[67] Workshop insight taken from meeting held on 7 July 2025 in Singapore.

[68] AI Verify Foundation, What is the AI Verify Foundation?, AI Verify Foundation website, 2025.

[69] Workshop insight taken from meeting held on 7 July 2025 in Singapore.


PROTOSTAR
STRATEGY