Hyperscale cloud and shared security in the Indo-Pacific

Views from *The Strategist*

EDITED BY
JAMES CORERA AND
MALKI OPATHA

AUGUST 2025

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

Acknowledgements

ASPI would like to thank Oracle for its support of the articles in Part 1 of this compendium, which explore cloud and 5G security challenges in Australia. We also thank Microsoft for its partnership in supporting the Hyperscale Cloud *Strategist* series featured in Part 2. These collaborations have helped foster informed debate on cybersecurity and technology adoption in the Indo-Pacific, and on Australia's role in shaping these domains. Sincere thanks also go to *The Strategist* editorial team—Elizabeth Lawler and Adam Ziogas—for their dedicated work in publishing the articles, and to the individual authors for contributing their time and insights to the series.

About ASPI

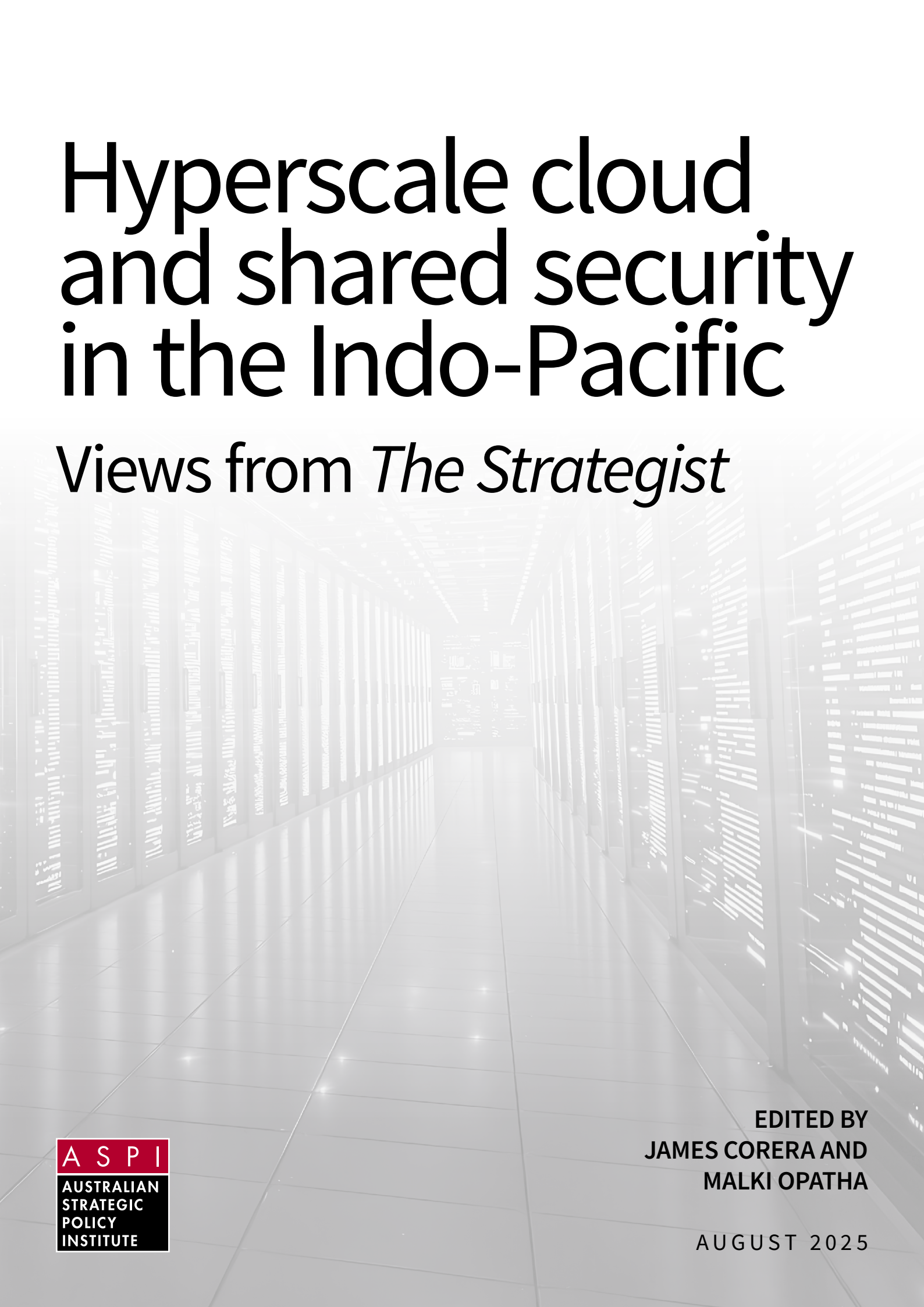
The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

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

Cover image: AdobeStock/Tanvir.

Hyperscale cloud and shared security in the Indo-Pacific

Views from *The Strategist*



EDITED BY
JAMES CORERA AND
MALKI OPATHA

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

AUGUST 2025

First published August 2025

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

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

Facebook.com/ASPI.org

@ASPI_org

Contents

Foreword

Jason Van der Schyff

Across the Indo-Pacific, cloud computing is no longer a niche technology conversation. It is the substrate of contemporary national security and economic resilience. From battlefield logistics to health systems, from real-time crisis response to AI development, hyperscale cloud infrastructure is becoming the engine room of state capacity.

As strategic competition sharpens across the region, that transformation is taking on clearer dimensions. Cloud infrastructure, such as undersea cables, is now a strategic national asset. Its security, interoperability and governance are becoming critical tests of sovereignty and trust. In this context, sovereignty does not mean doing everything alone or insisting on wholly domestic systems. It means having meaningful control, trusted partnerships and the capacity to operate on your own terms. This collection of articles shows just how quickly that shift is unfolding and what it means for countries navigating the intersection of digital ambition and strategic vulnerability.

Cloud matters not because it is efficient, but because it shapes the tempo and confidence of decision-making. It determines how securely data flows between allies, how quickly a government can recover from a shock, and how much visibility and control a state retains over its systems. These are not technical side issues; they are core questions in an era of cyber threats, coercion and contested infrastructure.

Hyperscale cloud, like subsea cable networks and trusted data routes, is now as foundational to regional resilience as it is to the security and prosperity of individual states. It is part of what allows partners to operate together, respond quickly and reinforce shared values. And it is what allows smaller states to modernise without falling into strategic dependence.

Australia has a responsibility and an opportunity in this domain. As Minister for Defence Industry Pat Conroy has noted, 'both defence and aid spending … are contributing to security', a recognition that digital infrastructure in the Pacific is as much about sovereignty and resilience as it is about development. Australia's strategic geography, regulatory settings and alliance networks give us a platform to shape how the region adopts, secures and governs hyperscale cloud. That includes building secure, inclusive digital ecosystems through investment, standards and skills development. It also includes continued support for physical infrastructure, such as the submarine cables we are funding across the Pacific, which are doing the quiet work of deterrence and trust-building. These initiatives create real dependencies, shared governance and durable regional partnerships that are hard to coerce and harder still to replace.

Cloud adoption is part of that same operating system. When Australia supports secure cloud capacity across the region, it is not just enabling better services. It is reinforcing sovereignty. It is embedding rules and relationships that strengthen both us and our neighbours.

This collection sets out what that effort could look like. It highlights how countries including Taiwan, South Korea, Japan and the Philippines are integrating cloud into their national security strategies. And it identifies a role for Australia: to lead where we are trusted, to partner where we are needed, and to help ensure that digital transformation supports resilience, sovereignty and stability across the Indo-Pacific.

The question is no longer whether cloud matters. It is how we secure it, govern it and use it to strengthen not only Australia's interests but also shared interests across the Indo-Pacific.

Introduction

Gatra Priyandita

Across the Indo-Pacific, governments are increasingly looking to the transformative powers of digital technology to bolster economic growth, improve public services, and address social and security challenges. At the centre of this transformation lies cloud computing, not merely as a commercial utility, but as a strategic enabler of national capability. Hyperscale cloud services now underpin everything from logistics and cyber defence to crisis response and public sector continuity. This shift is particularly relevant in a region where digital dependency intersects with rising strategic tensions, and where infrastructure resilience has become synonymous with national security.

This *Strategist* series brings together eight analytical pieces that collectively highlight the emerging importance and associated vulnerabilities of hyperscale cloud infrastructure in the Indo-Pacific. Through case studies from Taiwan, South Korea, the Philippines, Japan and Australia, as well as broader strategic analyses of cloud–5G convergence and AI-readiness, the collection illustrates a fundamental evolution in how governments must think about digital infrastructure: not simply as a technical solution, but as a pillar of national power. From battlefield to bureaucracy, and from disaster response to intelligence workflows, hyperscale cloud platforms are becoming deeply embedded in the machinery of state.

At the heart of this transformation are hyperscale cloud providers—tech giants such as Microsoft Azure and Google Cloud—whose global footprints are rapidly expanding across the Indo-Pacific. 'Hyperscale' refers to their ability to dynamically scale workloads across vast, distributed data centres, offering governments and businesses unmatched computing power, storage capacity and service availability. While these capabilities have helped accelerate innovation and reduce costs, they also introduce strategic risks, especially where local jurisdictions lack legal extraterritoriality, visibility into foreign ownership, or the capacity to enforce incident response protocols.

In the Indo-Pacific, these vulnerabilities are compounded by a highly contested security environment. China's growing willingness to deploy cyber operations and economic coercion against regional states—alongside broader concerns about digital influence and espionage—raises urgent questions about data integrity, sovereignty and resilience. Taiwan's experience offers a compelling case: under constant threat of cyberattack and physical disruption, Taipei has embraced cloud platforms as part of its broader resilience strategy, decentralising key assets and building the capability to maintain digital continuity even in the event of large-scale infrastructure attacks.

South Korea has also recalibrated its approach to cloud. While Seoul has taken meaningful steps toward modernising its digital security architecture through cloud adoption, the country still faces significant institutional friction. Regulatory conservatism, market consolidation, and reluctance within defence and intelligence agencies to outsource to external cloud environments have slowed progress. But the direction of travel is clear: cloud technology is becoming central to national security modernisation efforts.

In the Philippines, the transition to hyperscale cloud is accelerating, but governance frameworks have not kept pace. Manila risks becoming overly dependent on foreign providers whose infrastructure, legal accountability and security protocols remain only partially aligned with local needs. In the absence of clearer regulations, localisation policies or a national cloud strategy, key government and commercial systems may be exposed to external pressure or data compromise, especially as geopolitical competition deepens.

Japan's ambitions, from the Society 5.0 vision to regional tech leadership, depend on hyperscale infrastructure. Society 5.0 aims to solve domestic social challenges through innovation, and this infrastructure underpins the nation's push to transform governance, stimulate innovation and ensure economic resilience. But opportunity brings risk: foreign dependency, lagging domestic capacity and intensifying cyber threats expose structural vulnerabilities.

A recurring challenge across these case studies is interoperability—how states work with partners and

private providers on trusted terms. Standards across the region are fragmented, regulatory maturity is uneven and incident response mechanisms are often underdeveloped. This creates serious vulnerabilities not just within countries, but between them.

Addressing these challenges will require foundational investment, especially in skills, energy infrastructure and legal frameworks. Across all case studies, persistent bottlenecks are evident. Talent shortages in cloud engineering and cyber forensics, delays in zoning and permitting for data centres, and unclear regulatory protocols for breaches or foreign access are repeatedly identified as friction.

Finally, our authors call on Australia to treat cloud as strategic infrastructure, shaping procurement and regulation to align with sovereign interests, ensuring innovation strengthens rather than erodes national security, resilience, and public trust. Cloud computing offers the benefits of scalability, cost-efficiency, and agility, but it also introduces vulnerabilities—particularly around data sovereignty, operational control, and supply chain security. Governance frameworks need to extend beyond geographic data residency to ensure visibility into infrastructure, assurance of supply chains, privileged access auditability, and enforceable constraints on data movement. Furthermore, technology alone is insufficient; corresponding cultural and organisational change is essential to realise AI's potential. Secure-by-design principles need to be embedded, with clear responsibility across stakeholders: providers securing infrastructure layers; customers managing data, configuration, and access; and government protecting against foreign interference.

1 Aligning cloud, 5G and AI for national security

Cloud and 5G convergence is a national security imperative

Andrew Horton

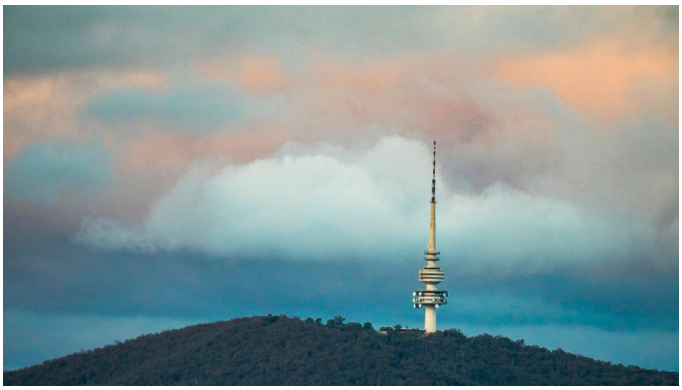


Image: Daniel Morton/Unsplash.

The convergence of cloud computing and 5G technology is set to revolutionise Australia's digital landscape, transforming how the nation communicates, operates and defends itself. While this technological leap promises great benefits, it will also bring security challenges that could, left untreated, undermine our national interests. To capitalise on the potential of these innovations while protecting national security, the government must act strategically and decisively.

Cloud computing has already reshaped industries by offering on-demand access to computing resources, enabling faster innovation and improved efficiency across sectors. With the rollout of 5G, this transformation will accelerate.

Next-generation 5G networks promise faster speeds, higher capacity and ultra-low latency, facilitating real-time communication and processing across various applications.

Together, the cloud and 5G will provide the foundation for breakthroughs like the internet of things (IoT), artificial intelligence, and smart infrastructure. These advancements will offer enhanced connectivity, real-time data processing and an ability to analyse massive amounts of data in previously impossible ways. They will transform everything from healthcare and manufacturing to transport and urban planning, improving decision-making and optimising resource use on a national scale.

This digital revolution is not without its risks.

The expanded reliance on cloud infrastructure and 5G networks creates a significantly larger attack surface for cyber adversaries. These technologies are integral to energy, transport and communications services. A successful cyberattack could have devastating consequences, compromising national security, economic stability and public safety.

The complex and interconnected nature of cloud and 5G ecosystems, which involve multiple vendors and international supply chains, makes them vulnerable to exploitation. Weaknesses in these systems could be abused to disrupt services or access sensitive data.

Additionally, as Australian organisations increasingly move their data to the cloud, concerns about data sovereignty and privacy arise. Securing sensitive information from foreign surveillance and ensuring that Australia's data remains under its control is crucial in an era of geopolitical competition in cyberspace.

China's growing dominance in cloud and 5G technologies presents a particular threat. As China expands its influence in global technology markets, it can embed vulnerabilities or backdoors into critical infrastructure. Given the Chinese government's track record of exploiting technology for strategic advantage, Australia must carefully scrutinise any technology from Chinese companies. This digital influence could give China leverage over global supply chains, leading to espionage, intellectual property theft and the disruption of critical services.

To counter this growing digital influence, Australia must diversify its technological partnerships, reduce its reliance on Chinese-made technologies and work closely with like-minded nations, particularly its Five Eyes allies.

The Australian government must adopt a proactive, whole-of-government approach to address these national security challenges.

First, it must develop and implement a comprehensive cybersecurity strategy addressing the challenges that cloud and 5G technologies pose. This strategy should focus on securing critical infrastructure, protecting supply chains and ensuring data sovereignty. The government should also develop and enhance its cybersecurity capabilities, ensuring that the country can respond to emerging cyber threats quickly and effectively. This includes strengthening threat intelligence, vulnerability assessments and incident response capabilities.

Collaboration will be crucial in managing these risks. The Australian government should foster closer collaboration between industry, academia and international partners. As part of its ongoing work within the Five Eyes intelligence-sharing alliance, Australia should continue to engage in joint initiatives to strengthen cybersecurity frameworks, share threat intelligence and develop common standards for securing cloud infrastructure and 5G networks. These partnerships will ensure that Australia is not alone in confronting cyber threats.

The private sector also plays a central role in securing critical infrastructure. Public-private partnerships should be encouraged in order to enhance cybersecurity resilience across industries, ensuring that businesses can handle the evolving cyber threat landscape.

In addition to promoting international and industry collaboration, the Australian government must strengthen its domestic technological capabilities. This includes investing in Australian-owned cloud services and 5G solutions not subject to foreign influence or control. By diversifying its technological partnerships and building homegrown capabilities, Australia can reduce its exposure to foreign vulnerabilities, particularly from China, and ensure a more secure and independent digital infrastructure.

Finally, public awareness and education on cybersecurity should be a priority. The government must ensure that all sectors of society, from government agencies to private businesses and individuals, understand the risks associated with cloud and 5G technologies and are equipped to protect themselves. National cybersecurity awareness campaigns and training programmes should be expanded to ensure that the Australian public, both as consumers and as part of the workforce, are equipped with the knowledge to recognise and mitigate cyber risks.

The convergence of cloud and 5G technologies offers Australia an unprecedented opportunity to enhance its national security and technological capabilities. However, it also introduces risks that require immediate and sustained attention. By adopting a proactive and comprehensive approach to cybersecurity, strengthening international partnerships and investing in domestic capabilities, Australia can secure the benefits of this digital revolution while safeguarding its sovereignty and national security.

The time for action is now—Australia cannot afford to wait as these technologies reshape the future of global competition and security

Published on 9 December 2024, https://www.aspistrategist.org.au/cloud-and-5g-convergence-is-a-national-security-imperative/

Mitigating Australia's cloud-computing risks is still work in progress

Andrew Horton

Image: Canva AI image generator.

The appeal of cloud computing is undeniable. It provides remarkable scalability, cost-efficiency and agility, qualities that attract government and business. However, for all its benefits, there are also risks, not least of which is maintaining sovereignty over Australian data.

The Australian government is working on mitigating the risks but needs to do more. Further necessary measures include improving cloud-computing regulation and encouraging development of entirely Australian services.

Data sovereignty is the principle that information is subject to the laws and regulations of the country in which it is collected and stored, ensuring that individuals and organisations maintain control over their data within national boundaries. It's important because, as former prime minister Malcolm Turnbull said, 'Data is the new oil. It's the currency of the digital age, and we need to make sure that it's controlled by Australians for the benefit of Australians'.

Relying on foreign cloud providers raises serious concerns about who ultimately controls our data and the systems that host it.

Some foreign governments can use extraterritorial law to compel cloud service providers to disclose data, even contrary to Australian law. Furthermore, foreign governments may pressure cloud providers to manipulate or disrupt services—for example, in war.

Debates around data sovereignty have persisted in Australia for nearly a decade, reaching a peak around 2020 during the COVID-19 pandemic. In response to this debate, hyperscalers—as the largest cloud services, such as Oracle, Amazon Web Services, Google Cloud and Microsoft Azure, are known—have invested time and resources to reshape the foundational elements of cloud infrastructure. They are now implementing technical controls designed to prevent offshore data replication and restrict transmission of telemetry data containing personally identifiable information beyond national borders.

The Australian Hosting Certification Framework aims to establish robust guidelines and standards for secure domestic storage and management of sensitive data. However, its weaknesses include limited enforcement mechanisms and a lack of comprehensive coverage for all data types, leaving potential gaps that malicious actors could exploit.

Even with strong contracts and data residency requirements, risks of unauthorised access, data breaches and foreign surveillance remain. This erosion of data sovereignty undermines our ability to protect sensitive information and uphold our legal and regulatory frameworks.

The Australian government must be fully aware of where its and its citizens' data is stored, who has access to it, and the safeguards to protect it. Cloud providers often struggle to reconcile these requirements, which is arguably affected by governments' lack of understanding of cloud technology and its technical strengths and weaknesses.

Until 2020, Australia relied on the Certified Cloud Services List of products that the Australian Signals Directorate (ASD) had certified. However, ASD struggled to keep pace with demand for certifications, keeping products on the shelf and reducing competition between firms that could supply the government. Although the list has been replaced by the Infosec Registered Assessors Program (IRAP), the problem of slow processing may persist due to a shortage of IRAP assessors.

The government must carefully consider the broader implications of its policies. If the process remains cumbersome, businesses may choose to take their operations elsewhere.

The ASD stresses this need for transparency in its cloud security guidance:

Transparency is essential to building trust in cloud services. Agencies should clearly understand the security controls implemented by cloud service providers and their ability to meet the agency's security requirements.

Recognising the shared challenges of data sovereignty, members of the Five Eyes intelligence alliance are collaborating to forge a unified approach. They are sharing information on threats and vulnerabilities, developing secure cloud technologies and promoting interoperability among national cloud infrastructures. By working together, the Five Eyes nations—Australia, Canada, New Zealand, Britain and the United States—enhance their collective resilience against foreign interference while preserving their individual sovereignty.

Australia must augment the Five Eyes' efforts with a comprehensive strategy to protect its data sovereignty and control in the cloud.

First, it needs to strengthen its legal and regulatory frameworks to address the challenges that cloud computing poses. This includes clarifying data ownership and access rights, enhancing data-breach notification requirements and establishing clear guidelines for cloud service providers operating in Australia. It is important to note that hyperscalers and the Australian government continue to work together to address the challenges of cloud computing in standards-setting bodies.

The government should also continue promoting development of sovereign cloud solutions owned and operated by Australian entities. This will ensure that our data remains within Australian jurisdiction and under our control.

Third, continued investment in cybersecurity capabilities is vital. We must invest in advanced cybersecurity technologies, threat intelligence and workforce development to counter evolving cyber threats.

Finally, international cooperation is not just beneficial; it's essential. Australia should continue its commitment with Five Eyes partners and other like-minded nations to establish common standards and frameworks for data sovereignty and cloud security. This collective effort will help foster a more secure and resilient global digital ecosystem.

As Australia continues to navigate the complexities of a digital future, the challenge of data sovereignty must be a priority.

Published on 28 October 2024, https://www.aspistrategist.org.au/mitigating-australias-cloud-computing-risks-is-still-work-in-progress/

Not just government: cloud system security is everybody's responsibility

Justin Bassi

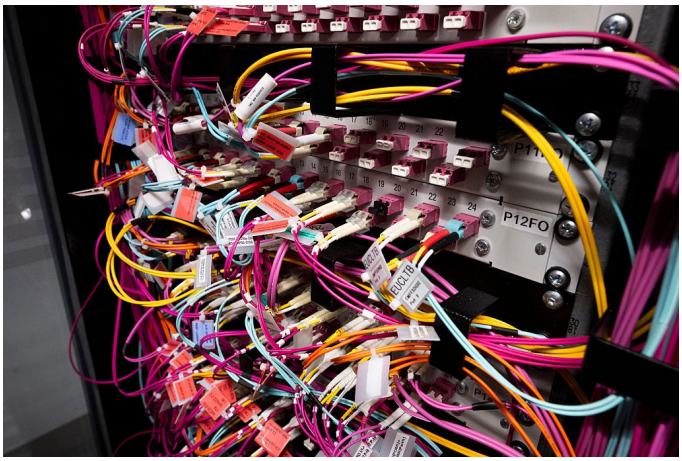


Image: Boris Roessler/picture alliance via Getty Images.

Australia's move to cloud-based technologies can't afford to repeat the mistakes of the early adoption of the internet and social media. At first, those earlier developments were not seen as critical infrastructure or technology that needed protection to defend a nation's citizenry, security and sovereignty.

Reaping the innovative benefits of cloud computing in a way that does not leave the nation less safe requires a clear and enforceable model of shared responsibility for cloud security. Individual roles should be well-defined, obligations understood and accountability embedded at every level.

Cloud computing, and other such tech, is a necessary part of our growing artificial world but naturally introduces new threat surfaces, systemic risks and critical vulnerabilities across government, industry and civil society. These risks can temporarily affect our economic security, but mismanagement will erode public trust and, therefore, more permanently threaten our national resilience and sovereignty.

Democratic governments' early unwillingness to interfere with innovation has led the internet and social media to be dominated by authoritarians that have been all too willing to stick their fingers in, exploiting the technologies for propaganda and interference. China and Russia are the main culprits in this.

We must not keep making the same mistakes. For a start, we should consider how providers, customers and governments each contribute to individual benefit and collective security.

Too many cloud users operate under the assumption that the provider alone is responsible for security; conversely, providers and users too often remain complacent, believing that the government will step in during a crisis.

Providers should be held accountable for securing the infrastructure layer, physical data centres, networks and virtualisation platforms. Customers remain responsible for securing their data, configuring systems properly, managing user access and maintaining operational readiness. And governments should use minimal regulation to protect the integrity of the infrastructure, specifically from foreign adversaries.

A shared model isn't optional; it's the only way to reduce risk in modern cloud environments. Failing to uphold these responsibilities has already led to serious breaches, including exposed credentials, unsecured databases and inadequate incident responses.

Failure to develop national policies has also led to inconsistent regulation of critical infrastructure and technologies. This has seen China dominate too many sectors on which society depends, such as renewable energies and batteries. We never gave Moscow control of our technology during the Cold War, so why are we so readily allowing Beijing to do so now?

The director of the US's Cyber Defence Agency, Jen Easterly, argues that systems need to be secure by default, meaning they're configured with maximum-security settings at the time of delivery. Furthermore, secure-by-design—in which security is architecturally embedded—cannot just be a mantra but should be a fundamental default principle.

Although cybersecurity is an ongoing process, protections such as encryption, system isolation and automated patching must be embedded during the design and deployment phases rather than being added after systems are live. Retroactively securing an environment leaves too many gaps and effectively means endlessly responding to one threat after another.

This requires cloud providers to be able to demonstrate, through independent audits and transparency, that their platforms are secure, resilient and capable of withstanding sophisticated and evolving attacks, including being able to recover quickly. Customers must be confident that the infrastructure supporting their data is not just compliant but protected and resilient.

Strong security governance is essential. The Department of Home Affairs' Hosting Capability Framework is a certification scheme for datacentres and cloud suppliers that provides users with protections and assurance of security, including relating to foreign ownership, control or influence risk, at both the infrastructure and platform layer. Cloud providers must also have clear, operational frameworks aligned with recognised standards, such as the Infosec Registered Assessors Program run by the Australian Signals Directorate or the International Organization for Standardization's ISO 27001. And they must be able to show how those controls are implemented in practice.

With governance and regulation in place, customers need to apply their policies for how data is handled, how access is granted and how workloads are managed. Most cloud breaches still result from users failing to apply basic governance and control measures. Resilience depends on customer readiness. Organisations need to design for failure, ensuring they have backup systems, recovery plans, continuity procedures and communications plans that have been tested under realistic conditions. The question is not whether disruption will occur but whether systems are ready to recover when it does.

Sensitive data should be encrypted by default, both at rest and in transit. Organisations should know where their data is stored, which jurisdiction's laws apply to it and who has the ability—legal or technical—to access it. This is particularly important in national security or critical infrastructure contexts, and any providers unable to offer this level of transparency and control should not be entrusted with such high-risk workloads.

The physical layer supporting cloud environments cannot be ignored. The ephemeral-sounding 'cloud' is formed by

physical infrastructure—data centres, cabling, hardware and energy systems. For Australia, government policy on critical infrastructure systems should, by default exclude providers whose supply chains create a risk of China accessing or controlling data and platforms. Then, providers must have strict physical security measures in place: controlled access, surveillance, layered perimeters and staff vetting. These controls must be demonstrable. If a provider cannot meet basic physical security requirements, it should not be hosting sensitive data or services.

Security doesn't stop at the perimeter. Cloud environments must be continuously monitored for anomalies and threats. Providers should offer real-time monitoring, automated threat detection and built-in response capabilities. And customers have a responsibility to configure and monitor their environments and to act quickly when alerts are triggered.

Access control remains the most frequent point of failure in cloud environments. In the absence of a physical perimeter, identity becomes the new security boundary. Providers must enforce multi-factor authentication and role-based access controls. Customers must manage identities carefully—granting only the minimum necessary access, rotating credentials regularly and auditing behaviour for anomalies. A single compromised identity can compromise an entire environment.

As cloud use becomes more complex—spanning public, private, hybrid and multi-cloud systems—security oversight needs to evolve. Fragmented cloud environments create blind spots. Visibility, accountability and control must extend across the full cloud landscape.

Australia's digital future depends on having reliably secure and resilient digital systems. That future cannot be delivered without shared responsibility. Government, providers and customers each have clear roles, and each needs to be accountable. Trust in cloud systems must be earned and continuously verified. Security as a secondary afterthought only puts the entire nation last.

Published on 23 July 2025, https://www.aspistrategist.org.au/not-just-government-cloud-system-security-is-everybodys-responsibility/

2 Hyperscale cloud sovereignty and security in the Indo-Pacific

States vulnerable to foreign aggression embrace the cloud: lessons from Taiwan

Jocelinn Kang

Image: created with DALL.E image generator

Taiwan is among nations pioneering the adoption of hyper-scale cloud services to achieve national digital resilience.

The island faces two major digital threats: digital isolation, in which international connectivity is intentionally severed or significantly degraded (for instance, if all submarine cables are cut), and digital disruption, in which local infrastructure, such as data centres, is inoperable.

To counter this, Taipei is shifting critical public systems and government data to global cloud platforms, and turning global cloud providers Microsoft, Google, and Amazon into partners in national resilience. But this reliance on foreign tech giants raises questions about sustained sovereignty in times of crisis.

Taiwan has learned from Ukraine's digital survival before and right after Russia's full-scale invasion in 2022. When threats to Ukraine's physical and digital critical infrastructure escalated, the government in Kyiv rushed through amendments to its data protection law, permitting government data to be stored on public cloud platforms. This amendment allowed Ukraine to shift critical data and services to cloud infrastructure across

Europe. So essential government functions, public services and important private sector functions remained available even when its local physical infrastructure was under siege.

Building on these insights, Taiwan in 2023 launched a four-year, NT1.34 billion ($65.7 million) plan to transition 18 critical civilian government information systems to the cloud in 2023. This includes services such as national health insurance, vehicle management and border control systems. The effort is intended to ensure continuity of essential digital services during disasters and emergencies and to enable swift operational recovery in the case of outages.

According to a press release, this involves 'cryptographic splitting and data backup mechanisms'. Although details are scarce, the Taiwanese government is presumably distributing encrypted backups of critical national data offshore stored across various cloud providers and retaining exclusive access to the decryption key. As part of this effort, former minister of the Ministry of Digital Affairs Audrey Tang suggested Taiwan would conduct contingency drills that would involve rerouting operations to alternative locations, such as Japan or Australia.

While hyperscale cloud services offer resilience against cyber and physical threats, they prompt questions around data sovereignty and personal data protection: how can a government keep control over data and services managed through foreign commercial infrastructure? How can privacy laws be enforced when data is outside of a nation's physical jurisdiction?

Taiwan has taken a pragmatic approach, allowing data-holding entities to use foreign cloud infrastructure as long as they can strictly adhere to Taiwan's privacy requirements. For instance, in 2023 the Financial Supervisory Commission amended its rules to allow the financial industry to use foreign cloud platforms for some operations, provided they met information security regulations, particularly regarding de-identification processes and personal data protection.

Cloud providers are acutely aware of contentions around digital sovereignty and have responded by offering 'sovereign hyperscale cloud' solutions. These involve security controls specifically implemented to meet local regulations and requirements, such as restricting data access and management to security-cleared local personnel operating from their national jurisdiction. The Australian Department of Defence is one enterprise that intends to implement sovereign hyperscale cloud, alongside sovereign cloud from domestic cloud providers as part of its cloud strategy. The willingness of global hyperscale cloud providers to adapt their offerings reflects their increasing role in national security.

In Taiwan, the Ministry of Digital Affairs is taking advantage of this adaptability. They have worked to bring the three major cloud providers (Google, AWS, Microsoft) into Taiwan and are actively encouraging them to build local partnerships with the satellite communication vendors to create locally resilient systems that can switch to satellite communications during emergencies and prioritise essential data transmission. These measures are particularly important for a country that imports 98 percent of its energy and faces regular challenges from natural disasters, such as earthquakes and typhoons, as well as military and hybrid threats. By establishing redundant systems through cloud and satellite infrastructure, Taiwan can maintain critical government functions even when local systems are compromised.

Cloud providers face operational risks when supporting nations vulnerable to aggression. When AWS and Azure took over the hosting of Ukraine's critical systems and data, their cloud infrastructure became a target of state and non-state cyberattacks. Yet this exposure provides valuable cyber threat intelligence, which is then used to improve security products, benefitting other customers.

The deepening integration of technology in national security and digital resilience introduces new dynamics to the relationship between states and global technology providers. These companies are no longer just technology providers; they are custodians of critical national assets. This shift demands a mature framework of collaboration: one that considers tech companies as potentially essential partners in national resilience, including as part of the digital supply chain. This inherently comes with mutual commitments centred around trust, accountability, oversight and responsibility that are sustainable during times of crisis.

Taiwan's integration of hyperscale cloud into their national resilience strategy shows how nations can leverage leading global technological capabilities while maintaining oversight over their critical systems and

sensitive data. This model may well define strategic autonomy in an age where digital resilience depends on foreign-provider infrastructure.

Published on 28 February 2025, https://www.aspistrategist.org.au/states-vulnerable-to-foreign-aggression-embrace-the-cloud-lessons-from-taiwan/

Strengthening South Korea's national security by adopting the cloud

Afeeya Akhand

Image: Gije Cho/Pexels.

To improve its national security, South Korea must improve its ICT infrastructure. Knowing this, the government has begun to move towards cloud computing.

The public and private sectors are now taking a holistic national-security approach that includes the country's military capability and cybersecurity. Success in this approach will require an improved competitive edge across emerging technologies to project and defend national power.

Cloud-based ICT infrastructure provides scalable computing capacity by managing vast quantities of data and adapting to varying workloads. From a defence perspective, flexible computing capacity enables rapid scaling during different mission phases.

Beyond modernising internal ICT infrastructure and military readiness, increasing South Korea's cloud uptake could improve the country's military interoperability with regional partners by facilitating real-time sharing of data at lower levels of classification and sensitivity.

Such information sharing is particularly important considering the international growth of South Korea's defence industrial base, which includes Hanwha's facility in Australia and Korea Aerospace Industries' ongoing support to the Philippine Air Force to enhance its air combat capabilities. Furthermore, if South Korea participates in specific AUKUS Pillar 2 projects, a common federated cloud-based platform could foster secure information-sharing, advancing collaborative development of advanced technological capabilities.

The South Korean government has introduced initiatives and policies to catch up on cloud adoption, including the 2015 *Act on the Development of Cloud Computing and Protection of its Users*, the 2022 Digital Strategy and a series of plans in 2024. But to improve cloud uptake in line with these policies and strengthen national security, the South Korean government must overcome several barriers.

The first of these barriers relates to the Cloud Security Assurance Program, a certification that cloud service providers (CSPs) must receive before working with South Korean government agencies. Despite a reformation in 2022, the certification process remains complex and lengthy. Australia's Certified Cloud Services List program faced similar criticism for its complexity, and was terminated in June 2020 following an independent review by the Australian Signals Directorate.

ASD's review into Australia's cloud services list outlined a need for greater industry engagement, for example through co-designed cloud security guidelines and the establishment of industry consultative mechanisms. In South Korea, regulatory reform processes—sparked by uptake challenges in the public sector—must engage CSPs to better meet provider needs.

This will require a careful balancing act. Although international CSPs can now serve government agencies, their ability to support public systems managing sensitive or private data—labelled as mid-risk and high-risk tier segments—is limited. Conversely, domestic CSPs have argued that the entry of international CSPs into the government market threatens their survival.

While market competition is healthy, the concerns of domestic CSPs mustn't be understated—the government plays an important role in the success of domestic tech

companies, such as Samsung and Naver, which are now points of national pride.

To meet the commercial interests of both international and domestic CSPs, international-domestic collaborations must continue to be brokered in South Korea. One recent example is between KT Corporation and Microsoft Corporation, which involves the development of a sovereign cloud solution to drive cloud and AI innovation in the public sector and regulated industries.

The second barrier to cloud uptake is the country's relatively low level of necessary expertise. Cloud-specific skills are required for organisations to assess the benefits of implementing cloud services. Despite the country's technologically advanced status, a 2021 OECD report stated that less than 15 percent of South Korean small and medium enterprises provided general ICT education to employees.

The third barrier, also linked to inadequate cloud expertise, is perceived security concerns. South Korean enterprises are conscious of the risks that cyberattacks pose, such as those that North Korea's Lazarus group has been conducting since 2009.

Many leading CSPs offer cyber protections through mitigation as well as response and recovery at scale, which would become particularly important in major combat operations near the Korean Peninsula, such in the South China Sea. However, organisations with limited cloud expertise often stick to existing systems due to misconceptions around cloud security and the perceived burden of data protection under the shared responsibility model.

To overcome these final two barriers, ICT professionals must upskill. Beyond government-led initiatives, such as a 2021 plan to nurture a talent pool of 10,000 cloud-trained professionals, CSPs are taking the lead. For example, Amazon Web Services Korea offers free cloud-computing education to South Korean jobseekers.

South Korea's slow adoption of cloud computing presents a gap in its national security and technological competitiveness. The government has recognised cloud infrastructure as essential to strengthening national power and interoperability with allies and partners—ultimately supporting defence, economic growth and emerging technologies. This has pushed South Korea to develop uptake strategies, but regulatory hurdles, low digital literacy and security concerns are persistent challenges. Encouraging collaboration between CSPs and improving digital literacy will only become more important as cloud technology becomes central to South Korean security.

Published on 11 April 2025, https://www.aspistrategist.org.au/strengthening-south-koreas-national-security-by-adopting-the-cloud/

The Philippines must consider security of hyperscalers

Gatra Priyandita

Image: inkoly/Getty Images.

The Philippines is embracing digital technology to drive economic growth and tackle socioeconomic challenges. Hyperscale cloud solutions—far larger than typical cloud service providers—promise robust cybersecurity and operational stability to protect critical data. But their adoption raises serious concerns about data sovereignty and dependence on foreign providers.

The Marcos government has articulated an ambitious digital transformation agenda, aiming to improve internet connectivity, expand e-governance platforms, and achieve universal digital ID registrations by the end of 2025. With the government's data collection and the country's broader data economy rapidly expanding, cloud adoption has also emerged as a priority.

The Department of Information and Communication Technology (DICT), the lead agency for cybersecurity and digital infrastructure, has pushed for the replacement of siloed legacy systems across government with more modern, integrated cloud-based solutions. These new platforms are intended to enhance interoperability

between agencies and improve delivery of public services. Under the current strategy, cloud services are developed as hybrids, blending on-site infrastructure with accredited third-party cloud providers. This allows for agency-level flexibility while maintaining essential control over sensitive data.

Security is a key criterion in accrediting cloud service providers. The DICT advises that government agencies move to accredited providers, as they regularly update their software. However, as government systems are increasingly targeted by state-sponsored cyber operations, the case for working with hyperscale cloud providers becomes more compelling. These providers claim to offer stronger defences for critical systems and national datasets than many government agencies can build in-house.

Without robust cybersecurity measures, the benefits of digital transformation risk being undermined, particularly in a country that remains highly vulnerable to cybercrime and foreign cyber intrusion. Other countries facing similar threats, such as Taiwan, have already turned to hyperscale cloud platforms as a means of ensuring digital resilience.

The scale of the challenge is substantial. In 2024, the cybersecurity firm Surfshark reported that more than 24 million Philippine accounts were compromised in data breaches, placing the country sixth in Asia for cyber incidents. High-profile attacks have hit both public and private sectors.

In October 2023, the Philippine Health Insurance Corporation suffered a ransomware attack that exposed the data of more than 42 million people. In early 2024, China-linked hackers made unsuccessful attempts to breach the president's office and maritime security agencies. This followed an earlier breach in which sensitive military data was exfiltrated, allegedly by Chinese state-sponsored actors.

As the Philippines develops key sectors, such as electronics, and deepens its role in regional security issues, it also becomes more exposed to intellectual property theft and digital coercion.

One of the strongest arguments for adopting hyperscale cloud services is their superior security features. Unlike traditional on-site infrastructure, hyperscalers offer AI-powered threat detection, continuous monitoring and automated incident response. Their infrastructure is designed with redundancy and geographic distribution in mind, making them well-suited to the Philippines, as a disaster-prone country. The ability to preserve data integrity and maintain services during crises is particularly valuable.

There is also a security logic to the adoption of hyperscalers. The Philippines is deepening its cyber cooperation with partners such as the United States and Australia, including through enhanced defence cooperation and increased collaboration on critical technologies.

Meaningful integration into allied defence networks will require the Philippines to meet high interoperability and cybersecurity standards. Hyperscale cloud platforms, if properly governed and secured, provide the critical foundation for secure information sharing, joint operational planning and rapid response capabilities with allied forces.

However, these benefits do not come without strategic trade-offs.

Currently, the Philippines relies heavily on foreign cloud vendors, with such major vendors as Huawei, Alibaba and Amazon Web Services operating in the country. This reliance—particularly on Chinese companies, given the two countries' disputes in the South China Sea—poses serious risks to national sovereignty and operational security. It also underscores the urgent need for a more comprehensive regulatory framework to govern cloud security and ensure digital sovereignty.

National security, not cost, must guide decisions about cloud providers. While hyperscale cloud platforms offer extraordinary capabilities, the Philippines must ensure that accredited providers meet strict sovereignty and cybersecurity requirements. The *Data Privacy Act* provides some protections, but it does not fully address the complexities of managing sensitive military and national security data across multinational platforms. The DICT should move quickly to enforce rigorous compliance standards for hyperscale adoption in defence, including mandated end-to-end encryption, strict physical and logical access controls, independent audits, and clear restrictions on foreign jurisdictions' legal claims over data.

To future-proof its digital transformation and secure its place as a credible regional partner, the Philippines must treat hyperscale cloud adoption as a strategic enabler—not just of administrative efficiency, but of national defence and sovereignty. This means embedding cybersecurity and geopolitical risk assessments in every stage of cloud policy, while building a regulatory environment that protects sensitive data and ensures operational continuity in times of crisis.

Hyperscale platforms, when governed by strong safeguards and aligned with trusted international partners, offer the Philippines a rare opportunity to bridge its digital infrastructure gap and reinforce its security architecture. The choice is not whether to adopt hyperscale cloud, but how to do so on the country's own terms.

Published on 19 June 2025, https://www.aspistrategist.org.au/the-philippines-must-consider-security-of-hyperscalers/

Digital dai-ichi: with right balance, Japan can shape its hyperscale future

Nishank Motwani

Image: metamorworks/Getty Images.

Japan's digital rise hinges on adopting hyperscale cloud computing without ceding strategic autonomy—a balance it has yet to strike.

Japan's hyperscale strategy must walk a tightrope—balancing the immense benefits of cloud infrastructure with the imperative of national control. The solution is not isolation, but integration: fusing trusted foreign hyperscalers with sovereign policy, secure design and a workforce capable of defending it.

Japan's ambitions, from the Society 5.0 vision to regional tech leadership, depend on hyperscale infrastructure. Society 5.0 aims to solve domestic social challenges through innovation and this infrastructure underpins the nation's push to transform governance, stimulate innovation and ensure economic resilience. But opportunity brings risk: foreign dependency, lagging domestic capacity and intensifying cyber threats expose structural vulnerabilities.

Additionally, Japan's digital transformation hinges on a critical enabler: energy. Data centres—especially hyperscale facilities—are energy intensive. Japan's projected doubling of data centre capacity from 2.0 gigawatts in 2024 to 4.0 gigawatts by 2030 highlights the importance of reliable energy supply to meet AI-driven computing demand.

The government's Vision for a Digital Garden City Nation and GovCloud initiatives aim to modernise public services, enable AI-driven governance and enhance national crisis response. These strategic platforms are already operationalising that vision: tools such as Spectee Pro harness hyperscale cloud to deliver real-time disaster insights, while GovCloud lays the foundation for scalable, secure digital infrastructure across ministries. Together, these capabilities strengthen Japan's domestic resilience and serve Japan's soft power, positioning it as a model for digital governance in the Indo-Pacific.

Foreign investment has rapidly followed. Microsoft has committed US$2.9 billion for AI and cloud infrastructure in Japan, Oracle plans to spend more than US$8 billion for AI and cloud computing services and Google has announced US$1 billion to expand subsea cable connectivity through the Pacific Connect initiative.

However, this promising growth faces friction. Substation capacity shortages in data centre hubs including Inzai could delay deployment for up to a decade. Land scarcity, rising construction costs and a limited contractor base, including for data centre construction and maintenance, further constrain expansion.

Decentralisation via the Digital Garden City Superhighway may help rebalance workloads, but coordinating regional resilience at scale introduces new policy and resource challenges.

Japan's cloud market is dominated by foreign hyperscalers. Domestic providers (NEC, IDC, and NTT)

together hold a market share of only about 30 percent. This raises concerns of vendor lock-in and exposure to foreign policy decisions compelling prioritisation of home country needs, especially during geopolitical strain.

The Economic Security Promotion Act (ESPA) seeks to mitigate these risks by designating cloud infrastructure as a critical asset and directing approximately US$500 million to support sovereign cloud and AI compute capabilities. Yet this pivot introduces a policy paradox: aggressive self-reliance could slow the adoption of globally advanced tools, including those vital to next-generation AI development.

Bridging Japan's hyperscale ambition with operational reality demands more than a policy shift. It requires a national effort leveraging strengths in advanced manufacturing, industry leadership, and research and development. The challenge for Japan's government is to enable, not direct, fostering an environment where industry can innovate at speed and scale. To translate digital ambition into secure, resilient outcomes, Japan will need to consider coordinated measures across cybersecurity, infrastructure, talent, architecture and legislative reform.

The sheer size of hyperscale systems makes them high-value targets for state-sponsored cyberattacks, cybercriminals and hacktivists. For example, in 2023 Japan's space agency, JAXA, suffered a series of cyberattacks seemingly linked to China. Consequently, to fully leverage hyperscale systems Japan will also need to prepare for the evolving cyberthreat landscape.

This will require deep visibility into supply chains, software dependencies and global data flows. Japan's recent legislative reforms—notably the Active Cyber Defense Bill, which was passed in early 2025 and will be effective from 2027—and inauguration of a dedicated position of economic security minister in 2021, signal integrated enhancement of its national capabilities to pre-empt threats at their source rather than solely focusing on mitigating their domestic consequences.

This involves expanding ESPA's scope to audit critical cloud infrastructure components and promote diversified sourcing. Redundancy needs to be built into supply chains domestically and through partnerships with trusted allies, enhancing resilience against external shocks.

Japan's national cybersecurity strategy calls for trust-building with cloud providers and integration of intelligence flows, yet public-private cooperation remains fragmented. Without a legal framework for information sharing and liability protections, incident response will likely stay reactive and inconsistent.

To build a resilient hyperscale ecosystem, Japan must accelerate energy and zoning approvals—particularly in regions outside Tokyo where power and land constraints are less acute. Incentives should also support regional hubs through targeted subsidies and regulatory coherence across prefectures.

Addressing the nation's cyber talent shortage is equally crucial. Japan faces a shortfall of 200,000 cybersecurity professionals by 2025. Years of outsourcing have weakened its domestic capabilities, constraining hyperscale ambitions. Japan (and others, such as South Korea) should consider investing in national cyber academies, vocational training and public-private university partnerships to grow specialised talent at scale.

Architecturally, Japan should adopt a sovereign-by-design cloud model that blends foreign and domestic cloud providers in a hybrid ecosystem with robust legal and technical safeguards. Strong encryption, access controls and enforceable data governance standards must be foundational to ensure operational sovereignty and compliance with national security objectives.

Legal frameworks should also be updated to enable structured information sharing between government and industry, including protections for liability. Without these guardrails, real-time threat intelligence will remain siloed and under-utilised.

By investing in infrastructure, talent and digital sovereignty, Japan can shape a hyperscale future that strengthens—not compromises—its economic security and alliance credibility. As cloud becomes contested terrain, Japan must lead like a digital power prepared to defend its digital frontier.

Published on 26 June 2025, https://www.aspistrategist.org.au/digital-dai-ichi-with-right-balance-japan-can-shape-its-hyperscale-future/

Whose cloud is it, anyway? Rethinking sovereignty in the shift to

cloud infrastructure

James Corera and Jason Van der Schyff

Image: blackred/Getty Images.

Cloud infrastructure is now the backbone of everything from social services and emergency response to critical industry operations and defence. The shift has been fast, and often invisible to users. What began as a convenience to save costs and increase flexibility has quietly become a question of national resilience. As more government systems migrate to commercial cloud platforms, the issue is no longer just where the data lives, but who holds real control over the systems that support it.

High-profile breaches at Qantas, revealed last week, and Optus and Medibank in 2022 have highlighted the consequences of poor data governance—not just for the organisations attacked, but for the individuals whose information was exposed. These events reinforce the need to secure datasets that carry real-world consequences. But the risks don't stop at the consumer level. They also affect us as citizens. Public discussion of data sovereignty often focuses on geography. The assumption is that if data is stored within national borders, sovereignty is intact. But this framing misses the larger issue. Control isn't just about the data centre postcode. It's also about the equipment and supply chains behind these services: who designs, manages and secures the infrastructure; who can observe or collect system-level activity; and who sets the rules for access.

These distinctions matter, but they're part of a more complex picture. Data residency refers to the physical location of storage, while data sovereignty refers to who holds legal and operational authority over data and systems.These are important dimensions, but sovereignty in the cloud era involves more than geography or governance. It includes: assurance of supply chains and the extent to which enabling technologies can be controlled or directed by a foreign government; visibility into infrastructure; and the ability to adapt service architectures as risks evolve. Responding to this requires more than technical specifications or regulatory clauses; it demands a layered, ongoing approach to risk, resilience and control.

Estonia offers a useful model. Through its 'digital embassy' in Luxembourg, it stores copies of critical government data offshore while retaining sovereign control. The legal structure treats the data as Estonian territory under international law. Ukraine has taken a different approach during wartime, shifting sensitive systems into public cloud environments under frameworks designed to preserve operational continuity.

Commercial cloud architecture is complex, often deliberately so. Many government clients have limited visibility into how workloads are scheduled, where failover systems reside, or who can access logs and metadata. Even when such information is available, procurement and policy teams often lack the technical capability to interrogate it effectively. This limits their ability to identify risks, challenge vendor assumptions or make informed comparisons. Services labelled as 'sovereign' or 'local' may still rely on offshore elements—such as software updates, control planes and management consoles—that sit outside domestic oversight. This fragmentation creates blind spots that regional hosting alone cannot resolve.

There's also a risk of structural dependency without understanding the implications. Sovereignty in the digital era is a systems question, not just a legal one. When governments can't inspect or govern the infrastructure that delivers their services, they rely on opaque assurances and private trust relationships. That might be acceptable in peacetime. It becomes a vulnerability in crisis or conflict.

Some argue this is the trade-off for accessing secure, scalable infrastructure. But that view is misleading. Security and sovereignty are not mutually exclusive. Adopting modern cloud capabilities doesn't require surrendering visibility, control or policy independence. What's missing is not technical feasibility, but strategic intent.

If Australia wants to retain authority over how its systems operate during disruption, it will need to prioritise infrastructure that supports operational independence. This means demanding transparency in service delivery, auditability of privileged access, and enforceable constraints on data movement and administrative control. It also means building scalable in-house capability for continuous compliance monitoring so agencies can assess, manage and, where necessary, disengage from platforms that no longer meet sovereign requirements.

This is not an abstract policy debate. Cloud platforms underpin essential government functions, from border security and defence logistics to law enforcement databases and infrastructure monitoring. They are embedded in daily public operations. A failure—whether from misconfiguration, cyberattack or coercion—would have widespread consequences. As reliance deepens and infrastructure becomes more concentrated, the risk only grows.

Policy responses must be forward-looking and principled. Governments should not be passive recipients of whatever commercial offering is available. Instead, they should shape requirements around a clear articulation of sovereign interest. That includes a willingness to invest in architectural resilience, even at the cost of slower procurement or higher upfront expense. Sovereign capability is not always efficient, but it's often essential.

The key shift is from passive consumption to deliberate control, defined not just by initial oversight, but by the ability to scale and adapt governance as threats evolve. This requires frameworks that are dynamic, not static, with the flexibility to respond to vendor behaviour, changing risks or the needs of missions. Contracts and compliance frameworks are no substitute for verifiable and enduring authority over systems.

Leading on sovereign cloud adoption is not about reinventing the wheel; it's about making deliberate choices that align with national interests and setting clear expectations for transparency, control and resilience. That requires a mindset shift—from treating cloud as a commodity to seeing it as strategic infrastructure. Convenience cannot be the organising principle. In a contested and uncertain world, the systems we build should be governed with clarity, not outsourced by default.

Published on 7 July 2025, https://www.aspistrategist.org.au/whose-cloud-is-it-anyway-rethinking-sovereignty-in-the-shift-to-cloud-infrastructure/

Conclusion

Jason Van der Schyff

As the Indo-Pacific's digital transformation accelerates, hyperscale cloud infrastructure has emerged not only as a cornerstone of economic modernisation but as a strategic asset tied to sovereignty, alliance trust and regional resilience. This *Strategist* series shows that cloud adoption is no longer a technical choice; it's a geopolitical act.

Across Japan, South Korea, Taiwan and the Philippines, we see shared imperatives, including the need to modernise public digital infrastructure, build resilience against cyber threats and reduce dependence on foreign technology ecosystems. Each country faces different challenges, such as power constraints, skills shortages, regulatory friction and legacy systems. But the pattern is clear: hyperscale cloud is becoming the backbone of state capacity.

This holds true for Pacific island nations as well. Though smaller in scale, they sit on the frontlines of climate shocks and natural disasters, where resilient digital services and real-time situational awareness are vital. Hyperscale cloud, supported by secure connectivity and trusted partnerships, offers a pathway to leapfrog legacy infrastructure. For many, it is the first viable route to sovereign digital capability and a safeguard against high-risk vendors embedded in outdated systems.

Australia has a pivotal role to play. As a trusted middle power, a digital governance leader, and a member of AUKUS and the Quad, Australia is well positioned to act as both enabler and exemplar. But leadership must be deliberate. Drawing from the insights in this volume, three priorities stand out for advancing cloud security and cooperation across the region:

1. Treat hyperscale cloud as critical infrastructure, not just commercial utility.

Cloud services underpin critical functions, including defence logistics, emergency response, financial systems and AI capability. Governments must apply a national security lens to the design, deployment and oversight of these services. This means stronger legislation like Japan's ESPA, as well as national cloud strategies and deeper coordination between infrastructure regulators, defence agencies and providers.

It also means securing supply chains, from data centre hardware to software dependencies and undersea cables. Trust at scale depends on public-private threat intelligence sharing, robust auditability and secure-by-design architectures.

2. Build regional interoperability on trusted terms.

Cloud adoption across the Indo-Pacific—from the Philippines and Indonesia to Japan, Fiji and Papua New Guinea—is shaped by fragmented standards, uneven regulatory maturity and varying levels of provider trust. Expanding access to trusted hyperscale services reduces reliance on untrusted vendors and reinforces national resilience.

While the three major hyperscalers use broadly compatible technologies, they do not make it easy to run true multi-cloud environments. This challenge can be addressed institutionally through smart architectural decisions, but doing so requires greater cloud fluency, strategic guidance and coordinated investment. That is a space where Australia is well positioned to lead.

Australia should also champion efforts to align standards, promote capacity-building, and support sovereign cloud capability where appropriate. Whether through AUKUS Pillar 2, the Quad, ASEAN digital frameworks or Pacific partnerships, Australia can help shape a cohesive regional model grounded in openness, security and sovereignty.

Initiatives such as Pacific Cyber Week, convened by Australia to promote regional cyber cooperation, offer timely opportunities to advance this agenda with Pacific island partners. The alternative is fragmentation or dependency on authoritarian infrastructure.

3. Invest in the foundations: skills, energy, and legal guardrails.

Each case study reveals structural gaps that policy alone cannot fix. Investment is needed in cyber talent—through vocational training, higher education, and migration pathways—as well as energy planning and land-use strategies that enable data centre development.

Legal frameworks must also evolve. Governments need clarity on liability, incident response protocols and rules for

secure information-sharing with trusted providers. Without these foundations, even the best cloud strategies will struggle to scale.

Cloud is not a silver bullet, but it is a force multiplier. As strategic competition unfolds across digital terrain, hyperscale platforms will shape the tempo and trust of regional decision-making. The question for Australia and its partners is no longer whether to act, but how to lead. This series offers a blueprint. The path ahead lies in connecting strategy to capability and capability to coalition.

About the authors

Afeeya Akhand is an analyst with ASPI's Cyber, Technology and Security program.

Justin Bassi is the Executive Director of ASPI.

James Corera is the director of ASPI's Cyber, Technology and Security program.

Andrew Horton is ASPI's chief operating officer.

Jocelinn Kang is a resident technical fellow at ASPI and managing director of Nodalys.

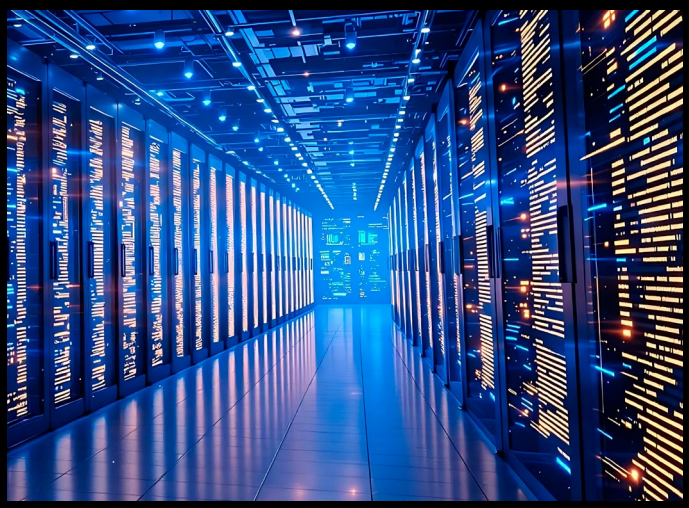
Nishank Motwani is a senior fellow and director of alliance strategy with ASPI USA.

Malki Opatha is the senior coordinator of ASPI's Cyber, Technology and Security program.

Gatra Priyandita is a senior analyst with ASPI's Cyber, Technology and Security program.

Jason Van der Schyff is a fellow with ASPI's Cyber, Technology and Security program.

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE



ISSN 2200-6648