

The Mobile Economy Asia Pacific 2026



GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at [gsma.com](https://www.gsma.com)

GSMA Intelligence

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

Contents

Executive summary	2
1. The economic impact of the mobile industry	7
1.1 Macroeconomic outlook	8
1.2 Mobile's contribution to the economy	10
2. Trends shaping the mobile industry	14
2.1 AI emerges as a monetisation engine for 5G	15
2.2 Trust by design becomes a strategic priority for operators	19
2.3 Resilience takes centre stage amid greater global uncertainty	23
3. Mobile industry impact	28
3.1 Turning connectivity into digital participation	29
3.2 Enabling local economic value creation	30
3.3 Empowering the green transition	31
3.4 Supporting disaster management and emergency response	32
4. Policies to enable innovation and growth	33
4.1 Closing the usage gap	34
4.2 Optimising spectrum access for future services	35
4.3 Embedding digital trust into policy frameworks	38
4.4 Strengthening multi-stakeholder collaborations	40

Executive summary

Sustaining industry impact

The impact of mobile connectivity in Asia Pacific¹ is both substantial and far-reaching. No longer limited to just enabling access to the digital ecosystem, it has become a core driver of economic growth, social development and broader digital participation, connecting individuals and businesses to the wider digital economy. The scale of its contribution is significant: the mobile sector accounts for \$1 out of every \$17 of economic value generated across the region. Operators in Asia Pacific support nearly 2.7 billion connections, including close to 1.8 billion unique mobile internet users (equivalent to over 60% of the population).

Mobile networks provide the foundational infrastructure for integrating AI and other emerging technologies into everyday life and business operations, supporting digital transformation across society. As a result, operators in Asia Pacific are expanding their role beyond connectivity to offer trusted local compute, cloud and secure data services amid geopolitical realignment and the shift towards sovereign AI reshape digital infrastructure needs. This is reflected in rising investment not only in advanced mobile networks, but also in cloud and broader digital infrastructure. By 2030, mobile operators in Asia Pacific will invest more than \$200 billion in capex to meet growing demand for advanced connectivity, localised AI workloads and new digital applications.

Inclusion, trust and resilience will remain central to sustaining the mobile industry's impact in Asia Pacific as mobile networks become increasingly integral to societal well-being. While significant progress has been made in reducing the coverage gap in Asia Pacific to around 2% on average, the usage gap still exceeds 1 billion people, including nearly 700 million adults, underlining the urgency for stakeholders to accelerate efforts to address this. At the same time, the proliferation of multi-dimensional online harms is elevating digital trust from a compliance requirement to a strategic priority for operators. Meanwhile, network resilience is evolving beyond coverage and capacity to focus on sustaining service continuity amid disruption and cost pressures.

\$1tn 

In 2025, mobile technologies and services generated \$1 trillion in economic value, projected to grow at a CAGR of 6.1% to reach \$1.4 trillion by 2030

18m 

The mobile ecosystem supported nearly 18 million jobs in 2025, including 12 million direct jobs

1. Asia Pacific in this report excludes Greater China unless otherwise stated.

Key trends shaping the mobile ecosystem

5G monetisation through AI

From selling connectivity to monetising AI-ready infrastructure and services

As AI moves from experimentation to deployment, operators in Asia Pacific are expanding across the AI value chain. This includes securing AI-ready infrastructure, developing orchestration layers to make distributed compute programmable and packaging AI applications for enterprise use.

Digital trust and cybersecurity

Trust by design is becoming a societal necessity and a commercial growth market

As scams and other online threats intensify, and AI makes fraud harder to detect, operators are shifting from reactive protection to prevention by design. The focus is no longer only on post-incident response, but on reducing risk earlier, embedding cyber defence across networks, services and governance, and collaborating with ecosystem partners.

Network resilience

The operator agenda is shifting from building coverage to engineering continuity

Network resilience is becoming the defining test of digital infrastructure. In a more fragmented and shock-prone environment, connectivity must remain reliable even when power systems, supply chains or terrestrial networks are disrupted. For operators in Asia Pacific, the focus is shifting from expanding coverage to ensuring continuity.



Policies for growth and innovation

Sustaining digital innovation and economic growth remains a priority for governments and stakeholders across Asia Pacific. Given the region's diverse digital landscape and the growing importance of digital trust, policy priorities should focus on closing the usage gap, strengthening trust as a foundation for advanced digital economies and deepening multi-stakeholder collaboration. Addressing these interconnected priorities will help build a more resilient and inclusive digital ecosystem while attracting the investment needed to finance and de-risk the next phase of digital development.

Optimising spectrum management is also essential to support efficient infrastructure rollout. Spectrum roadmaps help ensure sufficient capacity for rising demand from consumers and new technologies. Greater clarity on future spectrum availability enables operators to plan investment, secure financing and prepare deployment strategies across different technologies. Across Asia Pacific, several countries have published roadmaps, setting out timelines for access to core bands, including the 2.6, 3.5 and upper 6 GHz bands. While 6 GHz is expected to play an important role in meeting future connectivity needs, World Radiocommunication Conference 2027 (WRC-27) studies are also examining other mid-band options, including spectrum in the 4.5 GHz and 7–8 GHz ranges.



The Mobile Economy Asia Pacific



State of mobile internet connectivity

2024

Asia Pacific's coverage gap has narrowed to just 2%, reflecting sustained operator investment and shifting the challenge to last-mile connectivity. Action is needed on affordability, access, skills and relevant content to address the larger usage gap, to make meaningful digital inclusion a foundation for social welfare and enterprise growth.

Usage gap

35%

Coverage gap

2%

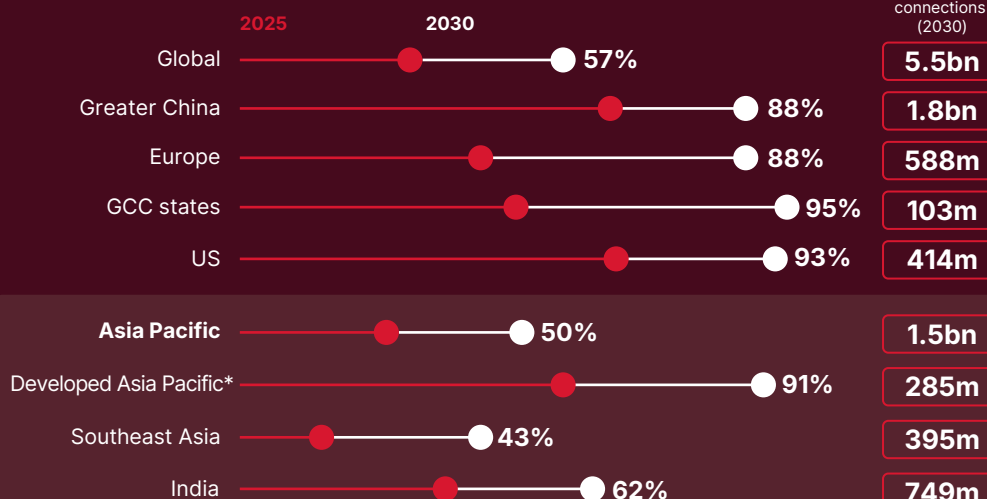


Connected
63%



5G as a share of total connections

Percentage of total connections (2030)



Total 5G connections (2030)

5.5bn

1.8bn

588m

103m

414m

1.5bn

285m

395m

749m

50%

5G adoption in Asia Pacific is set to nearly double by 2030, accounting for 50% of total connections in Asia Pacific.

However, regional disparities will remain: developed Asia Pacific is expected to exceed 90% adoption by 2030, while growth elsewhere will depend on sustained investment in coverage, spectrum, affordability and device availability.

* Australia, Japan, New Zealand, Singapore, South Korea



Operator revenues and investment

Revenues

2025

\$201bn

2030

\$224bn

Investment

Capex for the period 2025–2030

\$213.7bn



Operator adoption of GSMA Open Gateway APIs

2025

28 operators

Representing

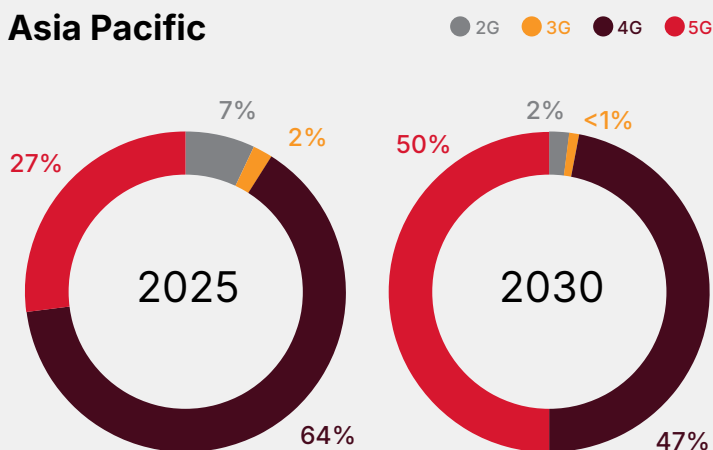
32%

December 2025

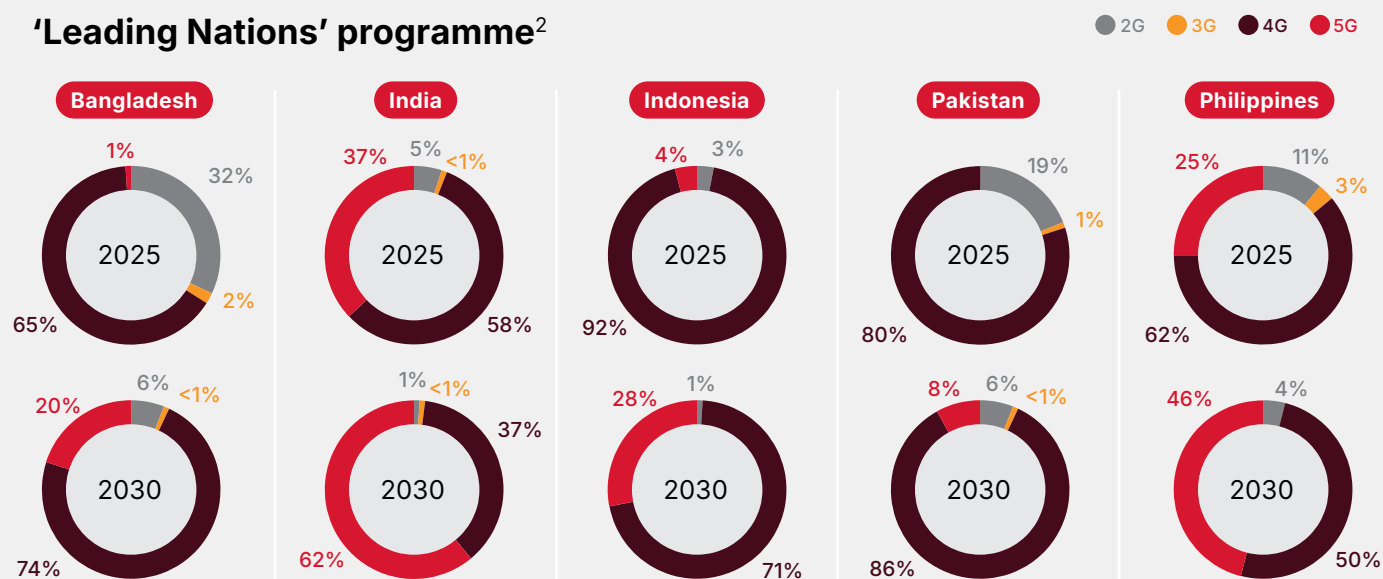
of global mobile market share by connections

Mobile technology trends for key markets*

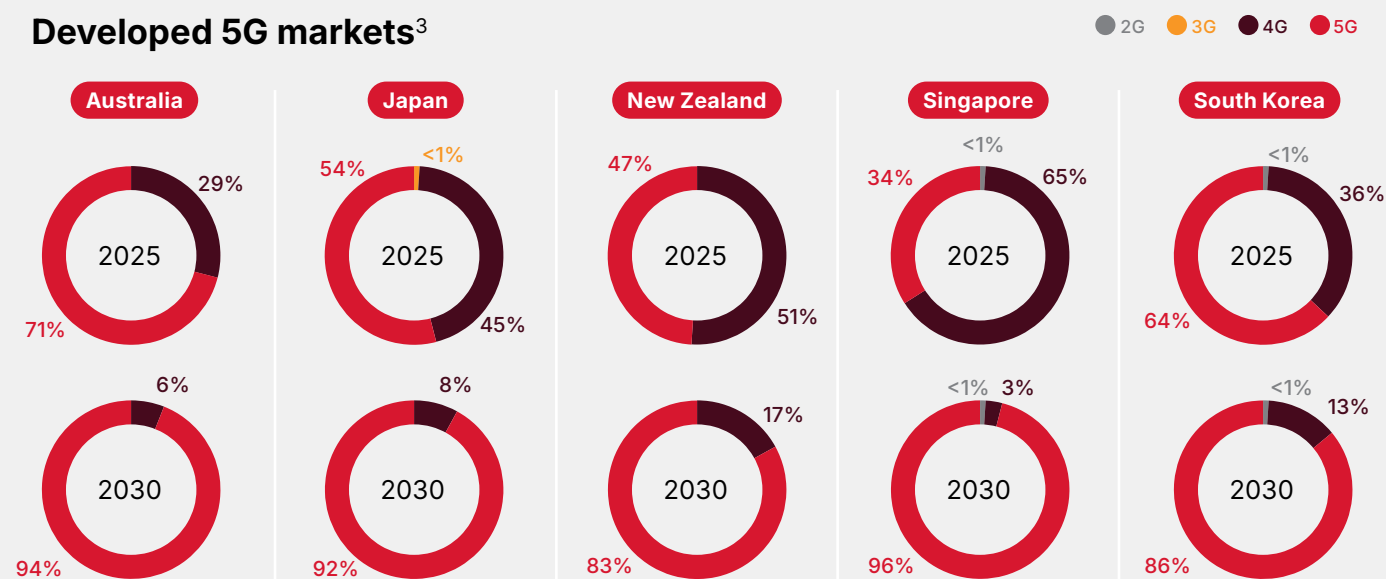
Asia Pacific



'Leading Nations' programme²



Developed 5G markets³



* Percentage of total connections

2. The GSMA Leading Nations engagement (comprising Bangladesh, India, Indonesia and Pakistan) seeks to accelerate the growth of the digital economy and advance the mobile industry's sustainability by lobbying for regulatory modernisation with relevant stakeholders.

3. Markets in Asia Pacific with the highest 5G penetration

01

The economic impact of the mobile industry



1.1

Macroeconomic outlook

Economic growth in Asia Pacific remained strong in 2025 at 4.2%, outperforming the global average of 3.1%. Although growth has moderated from the rapid post-pandemic recovery, Asia Pacific continues to be one of the world's most dynamic economic regions. However, its diversity means growth prospects vary significantly across countries, with strong momentum in emerging markets and more moderate growth in advanced economies.

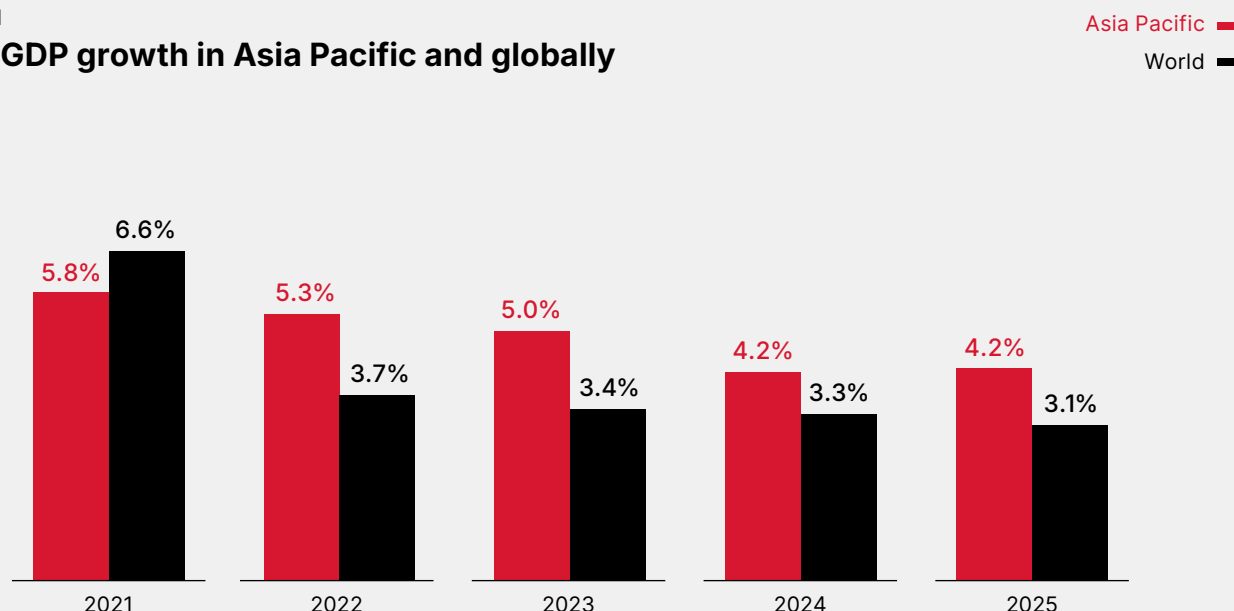
Recent growth has been supported by robust consumption, investment and services activity, particularly in emerging economies across South and Southeast Asia. Rising incomes, urbanisation and a growing middle class continue to support domestic demand, while many economies benefit from their integration into regional and global supply chains. Meanwhile, inflationary pressures have eased across much of the region, allowing monetary conditions to stabilise and support economic activity.

Looking ahead, Asia Pacific faces an increasingly complex global environment. Rising trade tensions, geopolitical uncertainty and energy-market disruptions pose risks to growth, particularly for highly open economies that depend on international trade. Productivity growth has also slowed in several markets, highlighting the need for continued structural reforms, investment in human capital and improvements in the business environment to sustain long-term economic expansion.

Nevertheless, Asia Pacific remains well positioned to capture the benefits of digital transformation. The region combines some of the world's fastest-growing digital economies with large-scale investment in connectivity, cloud infrastructure, AI and advanced manufacturing. The task now is to turn this investment base into practical gains for businesses: faster technology adoption, stronger local innovation ecosystems and a larger pipeline of higher-value services and advanced manufacturing activity.

Figure 1

Real GDP growth in Asia Pacific and globally



Source: GSMA Intelligence using WEO-IMF October 2025 data



Technology investments underpin economic growth

Technology investments have become essential for sustained long-term economic growth, with digitalisation reshaping how value is created, traded and captured across economies.

In Asia Pacific, investment in digital infrastructure, cloud capacity, data centres and AI computing continues to accelerate, reflecting the region's role as a major hub for digital adoption and technology-enabled growth. Across markets such as Australia, India, Indonesia, Japan, Malaysia and South Korea, public- and private-sector investments are expanding the capacity needed to support AI, cloud services, digital platforms and advanced connectivity.

Recent announcements highlight the scale of this shift. Microsoft announced a \$17.5 billion investment in India over four years to expand cloud and AI infrastructure, training and operations. In Southeast Asia, Malaysia has attracted major cloud and data-centre commitments, including Microsoft's first cloud region in the country and Oracle's planned investment of more than \$6.5 billion to establish its first public cloud region in Malaysia.

Overall, while Asia Pacific faces risks from trade fragmentation, geopolitical tensions and energy market volatility, it remains well positioned to leverage digital investment as a driver of productivity and competitiveness. Sustained investment in advanced connectivity, cloud infrastructure and AI capabilities will be critical to supporting innovation, strengthening resilience and enabling the region to maintain its role as one of the world's most dynamic growth engines.

1.2

Mobile's contribution to the economy

Mobile technologies contributed \$1 trillion of economic value in 2025

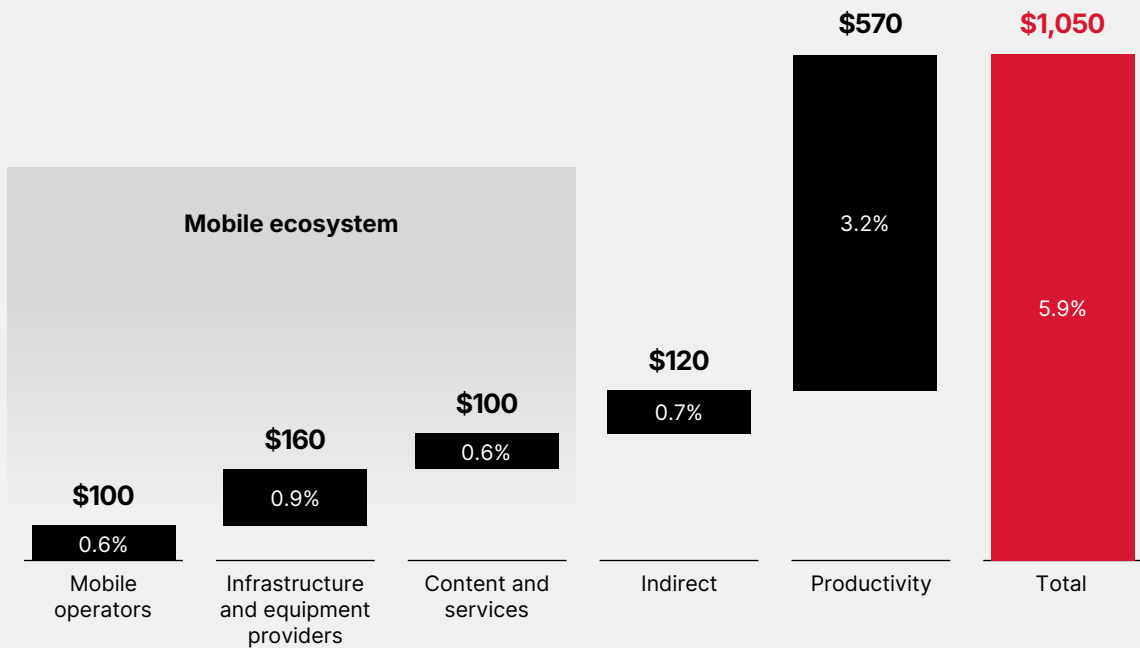
In 2025, mobile technologies and services generated 5.9% of GDP in Asia Pacific, a contribution that amounted to \$1 trillion of economic value added. The greatest benefits came from the productivity effects reaching \$570 billion, followed by the direct contribution of the mobile ecosystem generating \$360 billion.

The impacts of mobile technologies include connectivity and digital transformation. Connectivity refers to the use of mobile technologies, while digital transformation involves the integration by enterprises of advanced mobile technologies such as 5G, IoT and AI.

The mobile ecosystem is formed of three categories: mobile operators; infrastructure and equipment; and content and services. The infrastructure and equipment category encompasses tower companies, network equipment providers, device manufacturers and IoT suppliers. Meanwhile, the content and services category comprises content, mobile application and service providers, distributors and retailers, and mobile cloud services.

Figure 2
Asia Pacific: economic contribution of mobile, 2025

Billion, percentage of GDP

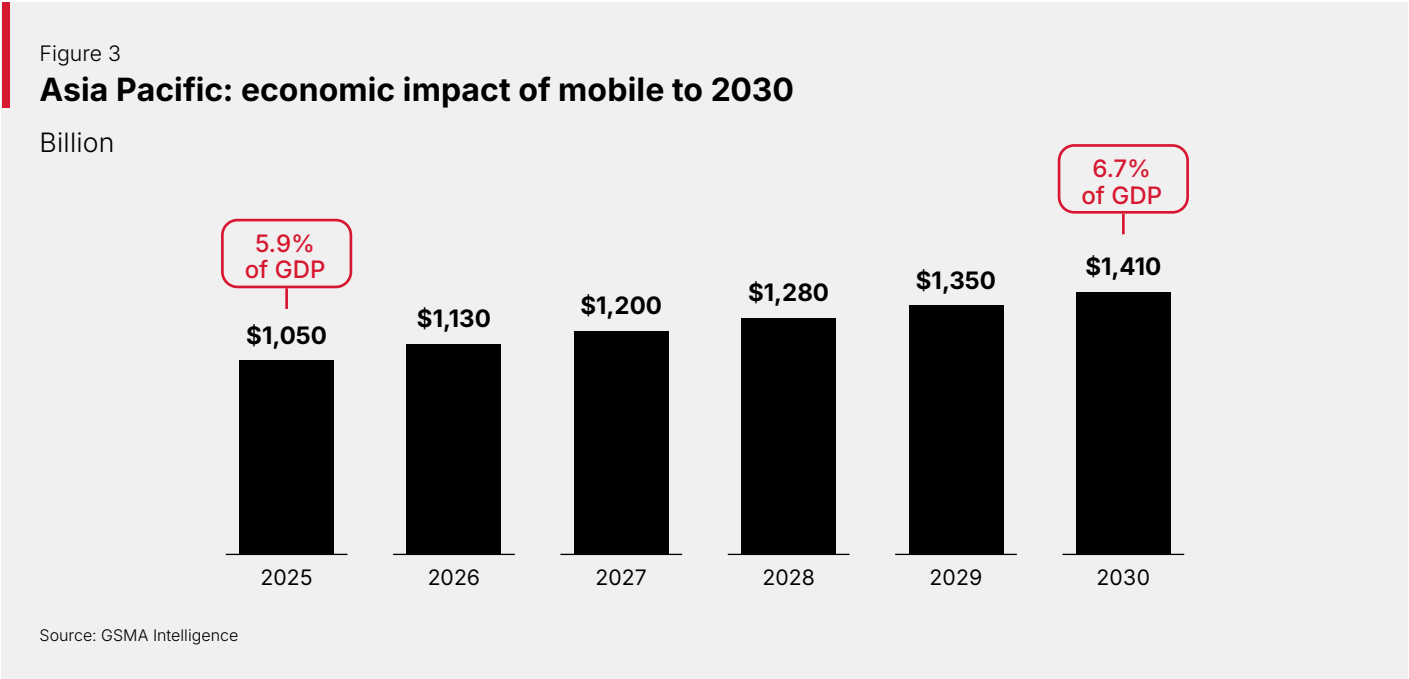


Note: Totals may not add up due to rounding.
Source: GSMA Intelligence

Mobile's economic contribution will reach \$1.4 trillion by 2030

By 2030, mobile's economic contribution in Asia Pacific will reach \$1.4 trillion, driven by the improvements in productivity and efficiency brought about by the continued expansion of mobile services and the growing adoption of digital technologies, including 5G, IoT and AI. By 2030, mobile's contribution is expected to grow at a CAGR of 6.1%, outpacing the overall regional GDP growth (CAGR of 3.5%).

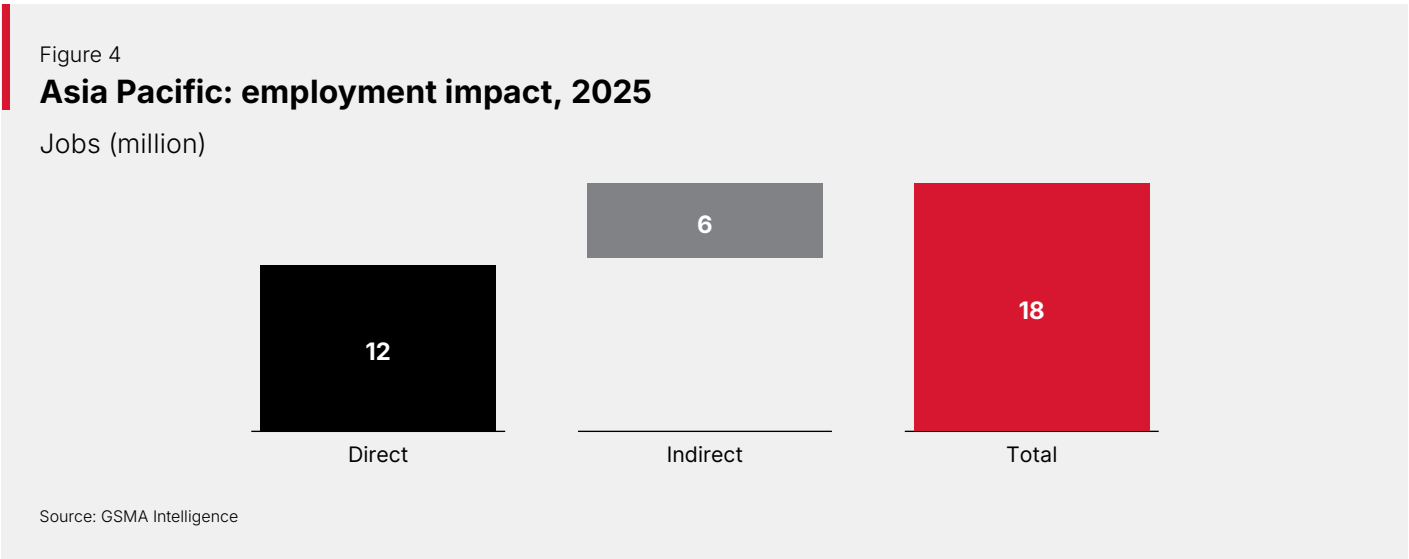
In this context, mobile technologies play an increasingly important role in supporting economic resilience and competitiveness. By enabling digitalisation across industries, they help firms improve efficiency, optimise costs and adapt to a more challenging economic environment while also supporting innovation and productivity gains over the medium term.



The mobile ecosystem supported 18 million jobs in 2025

Mobile operators and the wider mobile ecosystem provided direct employment to 12 million people in Asia Pacific in 2025. In addition, the economic activity

in the ecosystem generated 6 million jobs in other sectors, meaning that 18 million jobs were directly or indirectly supported.

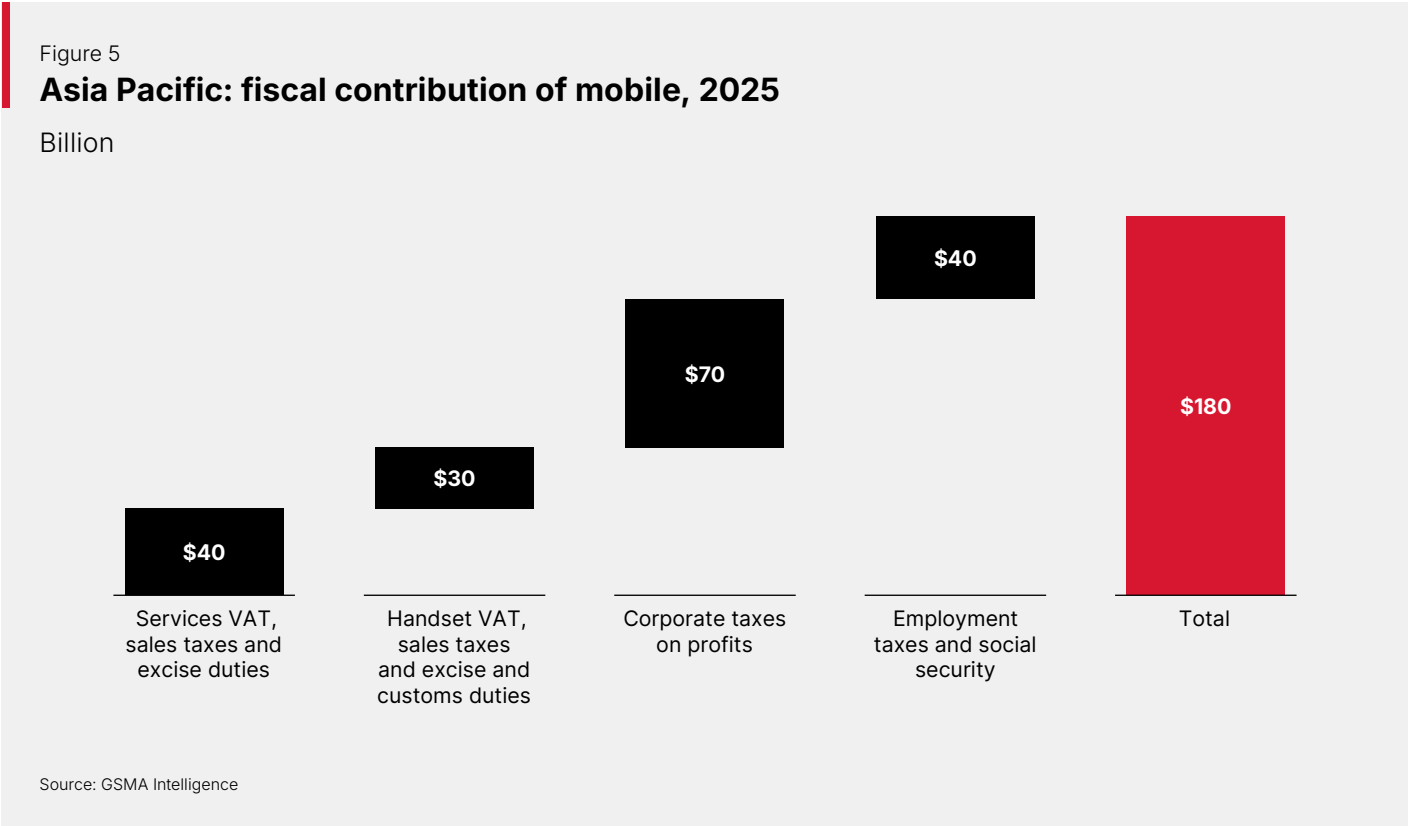


The fiscal contribution of the mobile ecosystem reached \$180 billion in 2025

Taxes constitute the major share of government revenues around the world. In 2025, tax revenues in Asia Pacific reached \$3.1 trillion, or 18% of the regional GDP, similar to the previous year.⁴ The mobile sector in Asia Pacific made a substantial contribution to the funding of the public sector, with \$180 billion raised through taxes on the sector in 2025. A large contribution was driven by corporate taxes on profits (\$70 billion). The fiscal contribution of the mobile ecosystem represented 5.7% of the total tax revenue.

Beyond its direct fiscal contribution, the mobile sector plays an important role in strengthening public finances across Asia Pacific by supporting the digitalisation of tax administration and the expansion of the digital economy. Across the region, mobile connectivity is increasingly used as a channel for individuals and businesses to access public services, including tax filing, payments and interactions with government agencies. Mobile-enabled platforms can reduce administrative costs, simplify compliance and improve the efficiency of revenue collection, particularly for small businesses and self-employed workers.

At the same time, the rapid growth of digital payments, mobile wallets and mobile money is increasing transaction traceability and supporting greater formalisation of economic activity. This is particularly relevant in emerging markets across South and Southeast Asia, where mobile financial services can help bring individuals and small firms into the formal economy. As e-commerce and platform-based services continue to expand, mobile technologies can help broaden the tax base, improve VAT and consumption tax collection, and support more stable and predictable public revenues. For governments, this reinforces the role of mobile not only as a direct contributor to public finances, but also as an enabler of more efficient and inclusive fiscal systems.



4. Source: IMF Fiscal Policies: World Revenue Longitudinal Database

The contribution of 5G and its ecosystem

As 5G networks expand and complementary technologies such as AI continue to mature, the scale of impact will be shaped not only by infrastructure availability, but also by investment in digital skills, innovation capacity and the integration of advanced technologies into production processes.

The economic value of digital transformation will come from two main channels:

- **External value creation:** The creation of new revenue streams and business models that expand markets and stimulate additional demand.
- **Internal value enhancement:** Measurable gains in productivity, cost efficiency and operational performance within firms.

The balance between these channels will vary across sectors, reflecting differences in digital readiness, capital intensity and the ability to adopt and scale up advanced technologies. Between 2025 and 2030 in Asia Pacific, manufacturing and services are projected to account for the largest shares of the economic impact attributable to 5G and its

ecosystem. This reflects the importance of industrial production, trade, logistics and services across the region, as well as the capacity of these sectors to adopt 5G-enabled solutions such as automation, connected devices, AI-driven analytics and smart supply chains.

Construction and real estate, public administration and agriculture also make significant contributions. In construction, 5G can improve project coordination and asset management, while in public administration it can support more efficient digital government services. In agriculture, 5G, IoT and data-driven tools can help improve productivity, resource efficiency and market access, which is particularly relevant for emerging economies across the region.

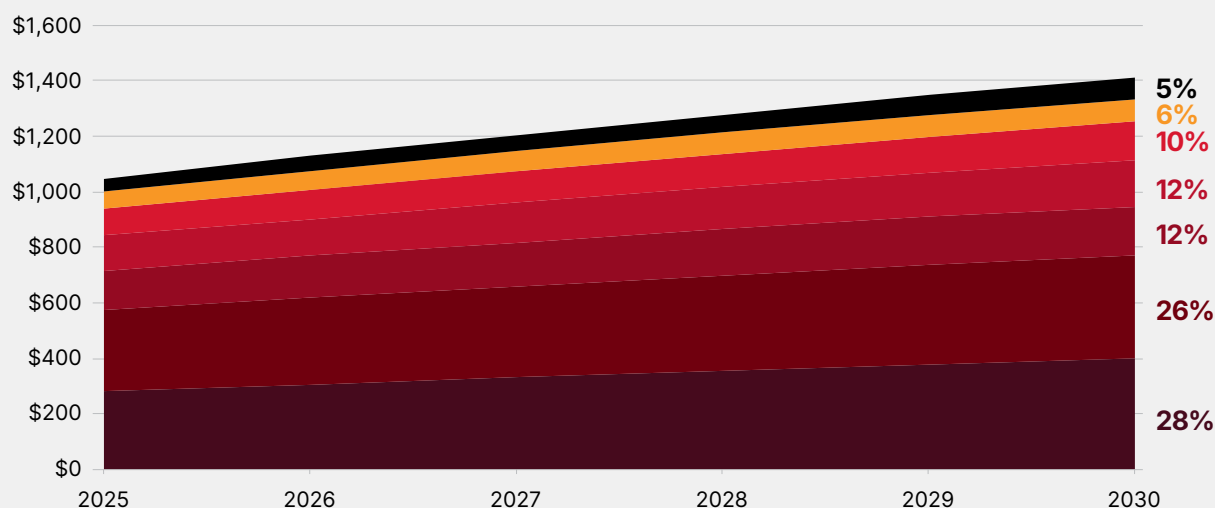
The information and communication sector accounts for a smaller share of total impact, but this reinforces the wider role of 5G as an enabling technology. Its greatest value comes not only from growth within the digital sector itself, but from supporting productivity gains across traditional industries.

Figure 6

Asia Pacific: mobile's contribution to GDP by industry, 2025-2030

Billion

Information and communication
Finance
Agriculture
Public administration
Construction and real estate
Services
Manufacturing



Source: GSMA Intelligence

02

Trends shaping the mobile industry



2.1

AI emerges as a monetisation engine for 5G

As 5G deployment matures across Asia Pacific, the strategic focus is shifting from network rollout to value creation. AI is becoming central to this transition by improving network performance, expanding operators' roles across infrastructure and applications, enabling programmable network

capabilities through APIs and strengthening sovereign digital capacity. For operators, the opportunity is not a single AI revenue stream, but a broader platform position across connectivity, compute, cloud, data, security and enterprise services.

The synergy between 5G and AI remains critical

Asia Pacific is forecast to reach almost 1.5 billion 5G connections by 2030, accounting for more than a quarter of the global total. But while mature markets in the region are expected to reach 91% 5G adoption by then – with some already operating extensive 5G standalone (SA) networks – markets elsewhere in the region are continuing to build foundational coverage and capacity.

At the same time, the mobile industry is increasingly focused on monetising 5G investments and delivering broader societal benefits with the technology. AI–5G synergy is therefore becoming a strategic priority. Use cases that deliver clear gains in productivity, service quality or resilience can strengthen the case for further investment in spectrum, sites, fibre, cloud and edge infrastructure. A key route is using AI to extract more value from 5G networks. For instance, in December 2025, KT and Samsung validated AI-RAN optimisation on KT's commercial network, using user-level AI configurations to predict and reduce service disruption. Meanwhile, in early 2026, KDDI and Ericsson completed a large-scale live network trial using Ericsson AI rApps⁵ to optimise uplink interference across 4G and 5G cells, improving throughput, signal-to-interference-and-noise ratio and progress towards greater network autonomy. These examples show how AI is shifting network operations from static optimisation to more user-aware, self-optimising performance.

A related priority is positioning advanced 5G networks as platforms for AI deployment in the economy. As industrial and public-sector AI use cases increasingly depend on processing data closer to its source, edge AI and edge–cloud coordination are becoming central to network strategy. This will require continued investment in low-latency transport, edge computing, cloud-native network functions, 5G SA and 5G-Advanced capabilities, enabling networks to support real-time inference, secure data handling, service assurance and differentiated quality of service.

Private 5G offers a key route to adoption by providing secure, high-performance and low-latency environments tailored to enterprise and industrial needs. Across Asia Pacific's manufacturing clusters, ports, logistics hubs, hospitals and smart city settings, private 5G gives large enterprises, small and medium-sized enterprises (SMEs) and startups controlled environments to develop, test and scale up AI-driven use cases. The strategic challenge is to shift 5G from general-purpose connectivity to programmable, industry-specific infrastructure that supports AI-enabled productivity and public-service outcomes.

Operators deploy solutions across the AI value stack

As AI moves from experimentation to deployment, operators are expanding across the AI value stack. In Asia Pacific, this includes securing AI-ready infrastructure, creating orchestration layers to make distributed compute programmable and packaging AI applications for enterprise use.

The aim is to reposition network, cloud and data-centre assets as scalable enterprise AI platforms rather than standalone connectivity services.

5. Intelligent, AI-powered software applications designed to automate, optimise and heal telecom networks, particularly the RAN

Table 1

Asia Pacific: major operator moves across the AI value stack

Layer	Details
AI infrastructure	AI demand is rising in Asia Pacific. This is pushing operators to invest in AI facilities and to position local data-centre assets as part of national and regional AI infrastructure. Major operator moves • Airtel's data-centre arm, Nxtra, secured \$1 billion in March 2026 to expand its data-centre infrastructure, building on its October 2025 partnership with Google to develop a gigawatt-scale AI hub in Visakhapatnam. • Singtel agreed to acquire full control of STT Global Data Centres, together with KKR, giving Singtel exposure to a platform with approximately 2.3 GW of design capacity across 12 major markets. Singtel's data-centre brand, Nxera, opened its 58 MW Tuas data centre in 2026, increasing Singtel's Singapore data-centre capacity to 120 MW. Strategic impact The growing investment in AI infrastructure gives operators a stronger claim on the first layer of AI demand: the need for secure, scalable and energy-intensive infrastructure for training, inference and cloud workloads. It also improves their relevance to hyperscalers, large enterprises and regulated sectors that need local capacity, data-centre resilience and trusted hosting options.
AI cloud OS and orchestration	Enterprises in Asia Pacific are moving from raw compute demand to managed AI environments that can orchestrate workloads across data centres, cloud, edge and network resources. AI cloud OS is therefore becoming the software layer that makes distributed operator infrastructure programmable. Major operator moves • SoftBank launched Infrinia AI Cloud OS in January 2026 to orchestrate graphics processing units (GPUs), network functions and Kubernetes-based container environments. In March 2026, its AITRAS work with Nokia showed how spare AI-RAN capacity could support third-party workloads, including Mitsubishi Heavy Industries' industrial edge use cases. • SK Telecom is building a managed AI infrastructure stack for GPU partitioning, workload management and lifecycle control, showcasing its AIDC Infrastructure Manager and AI Inference Factory in March 2026 to scale up data-centre operations and inference workloads. Strategic impact This layer turns AI infrastructure investment into a 5G monetisation engine. With this layer, AI data-centre scale and AI applications are bridged, helping operators monetise network intelligence and turning network assets into monetisable AI infrastructure.
AI applications and marketplaces	Enterprise AI demand is shifting towards packaged applications for specific business processes, especially among SMEs that seek faster deployment and lower implementation risk. This favours operators with existing enterprise reach, cloud, security and managed ICT capabilities. Major operator moves • Telkom Indonesia has signed an MoU with ZTE to advance cloud computing, next-generation connectivity and AI-enabled enterprise solutions. The company also operates an AI Centre of Excellence focused on enterprise and government use cases. • KT focuses on enterprise AI-agent enablement, unveiling Agentic Fabric and Agent Builder to help enterprises configure and deploy AI agents across workflows, using reusable templates and no-code tools to reduce custom development complexity. Strategic impact Packaged AI applications bring operators closest to enterprise demand and measurable outcomes. Instead of selling infrastructure only, operators can offer ready-to-deploy agents, workflow tools and sector solutions that address specific business pain points. These offerings also drive upselling of existing cloud, security, data and managed ICT services, making AI the front end of broader packaged enterprise revenue for operators.

Source: GSMA Intelligence

Telco APIs as the programmable layer for agentic AI

As operators expand into AI platforms and enterprise applications, network APIs are becoming the link between AI services and telecoms capabilities. Agentic AI increases this need, as enterprise agents will require programmable access to network context, performance assurance and edge resources to operate reliably, decide where workloads should run and respond to changing device or connectivity conditions.

Operators are well placed to expose API capabilities to meet growing demand for stable, accurate and adaptable connectivity. Their networks provide real-time control points through which connectivity, mobility and service quality are managed. By standardising access to these assets, operators can make network capabilities easier for AI developers and enterprise platforms to use, positioning APIs not only as a monetisation channel but also as an enabling layer for agentic AI services. GSMA Intelligence found that 16 out of 17 major operators focused on network APIs at MWC Barcelona 2026, while enterprises ranked network performance, quality optimisation and fraud prevention among the most important API use cases for 2026. In particular, APIs in the following areas are likely to see the most immediate demand as the agentic AI economy scales up:

- **Context and mobility APIs provide the situational-awareness layer for agentic AI.** As AI systems become embedded in vehicles, robots, field operations and connected assets, reliable action will depend on verified information about location, reachability and movement. The Device Location Verification API can confirm whether a SIM-based device is within a defined area – Asia Pacific operators have a strong presence in this API category, relative to operators in other regions. Over time, Device Information APIs could extend this role by adding device status and reachability, helping agents adapt as assets move, disconnect or become unavailable.

- **Quality and performance APIs address the assurance needs of agentic AI services.**

Applications such as video analytics, remote equipment control, mobile robotics and immersive interfaces are sensitive to latency, throughput and service continuity, making programmable performance increasingly important. APIs such as Quality on Demand (QoD) allow developers to request stable latency or prioritised throughput from the network. KDDI offers a useful Asia Pacific example: in August 2025, it outlined technical work on QoD implementation as part of a broader effort to expose 5G network functions to applications.

- **Edge discovery and compute APIs support the execution layer of agentic AI.** As inference becomes more distributed, applications will need to match each workload to the most suitable processing environment, balancing latency, reliability, data locality and resource availability across devices, enterprise sites, operator edge nodes and central cloud. The Simple Edge Discovery API is strategically important because it helps applications identify the nearest suitable edge cloud zone, reducing latency and improving reliability for time-sensitive AI services. Singtel Paragon, for example, provides a 5G edge platform that helps enterprises provision low-latency applications across network and cloud environments.

Over the longer term, regional coordination will be critical to scaling up this opportunity. The Bridge Alliance API Exchange builds on the GSMA Open Gateway and CAMARA standards by adding a federation layer for Asia Pacific, giving enterprises unified integration, simplified commercial frameworks and common operating support across markets. Its expansion to Indonesia, Malaysia, Taiwan and Thailand in November 2025 shows how the region is working to reduce fragmentation and make network APIs a more scalable revenue layer.

Sovereign AI creates new strategic opportunities for operators

In Asia Pacific, sovereign AI is shifting from policy ambition to infrastructure and enterprise execution. For operators, it creates a role beyond connectivity, turning local compute, trusted cloud, secure data handling and model localisation into platforms for national AI capacity and regulated-sector adoption.

Compute and infrastructure sovereignty

AI sovereignty begins with access to local compute. Across Asia Pacific, AI-driven demand is turning data centres, GPUs, power supply and cloud-network connectivity into strategic infrastructure. The region will have 4.8 GW of new data-centre supply added by 2027, with 78% already pre-leased, according to JLL.⁶

This trend is also putting pressure on the supporting infrastructure needed to operate AI data centres, including power, cooling, water, fibre and grid connections. KPMG estimates that AI training and inference could increase data-centre power demand in Asia Pacific by 165% by 2030.⁷ Johor, Malaysia's southern state and one of Southeast Asia's fastest-growing data-centre hubs, illustrates the infrastructure constraint. As data-centre demand surged, local authorities reportedly rejected nearly 30% of applications to protect power and water resources.⁸

Data and cloud sovereignty

Beyond access to compute, sovereign AI in Asia Pacific also depends on trusted environments for storing, processing and governing sensitive data. Regulatory expectations are tightening: India's 2025 Digital Personal Data Protection Rules operationalise data-protection obligations, while Australia's CPS 230, effective since July 2025, raises requirements for operational resilience and service-provider risk management in regulated sectors.

This has led to unmet demand for sovereign cloud platforms that keep AI workloads local, auditable and secure, supported by cybersecurity capabilities and enterprise reach. Operators can help fill this gap. For instance, SoftBank launched sovereign cloud and AI services in April 2026 using Oracle Alloy from Japan-based data centres, ensuring data and systems are managed domestically. Separately, Airtel partnered with IBM in 2025 to enhance Airtel Cloud with AI-ready servers and capabilities tailored to regulated sectors.

For operators, sovereign cloud creates a higher-value enterprise pathway, deepening relationships with governments and regulated sectors while expanding recurring revenue across cloud, security, data-centre connectivity and AI services.

Model sovereignty

Model sovereignty, which is the ability to develop proprietary foundation models, remains limited to selected Asia Pacific markets and operators with sufficient compute, data, talent and policy support. Sovereign foundation models can strengthen domestic-language capability, sector knowledge and controlled deployment while improving cost discipline through smaller or operator-optimised models. These can help operators manage inference economics and capture value above compute and cloud. Recent launches of sovereign foundation models include the following:

- In March 2026, **Viettel** partnered with Nvidia to help build Vietnam's sovereign AI ecosystem, including Vietnamese foundation models, reinforcing the link between telecoms capabilities and national AI capacity.
- In December 2025, **SK Telecom** launched A.X K1, which is designed for Korean-language and industry-specific AI workloads. It also serves as a 'teacher model' for smaller, specialised models.
- In October 2025, **SoftBank** integrated SB Intuitions' Japanese-language Sarashina model into its large telecoms model, enabling end-to-end domestic AI processing for network operations.
- In July 2025, **Indosat Ooredoo Hutchison**, through its subsidiary Lintasarta, launched an Nvidia-powered sovereign AI cloud, offering Blackwell GPUs and advanced large language models such as Sahabat.ai for Bahasa speakers.

For smaller and less mature markets, a full sovereign AI stack may remain challenging in the near term. The priority may not be frontier-model development, but rather trusted regional or national AI operating environments. Strategic partners can invest alongside local operators, creating shared enterprise value while strengthening local AI ecosystems through secure connectivity, edge-cloud partnerships, data-governance support and public-sector delivery channels.

6. Asia Pacific Data Centre Report Year-end 2025, JLL, 2025

7. The Asia Data centre landscape, KPMG, 2025

8. "Johor rejects nearly 30% of data centre applications to protect local resources", The Straits Times, November 2024



2.2

Trust by design becomes a strategic priority for operators

As digital services become more embedded in daily life, business operations and public-service delivery, trusted access to the online environment is becoming increasingly important. Simultaneously, exposure to scams, fraud and cyberattacks is on the rise. For consumers, this challenge is most visible in digital safety. The GSMA ASEAN Consumer Scam Report found that the share of consumers who reported having ever been scammed rose from 31% in 2024 to 45% in 2025, while recent scam victimisation also increased.⁹ Scam activity remains closely linked to communications channels, with victims most often citing over-the-top (OTT) messaging, voice calls and social platforms as contact points, while SMS and email remain relevant in some markets.

The AI era is making this risk more severe. Generative AI (genAI) can help scammers create more convincing messages, impersonate trusted organisations, produce synthetic identities and scale up personalised social-engineering attacks. The GSMA report also identifies AI-enabled scams, including voice cloning, deepfake customer-service chats and real-time one-time password (OTP) relay attacks, as an emerging risk.

The financial impact of this is already substantial. In Singapore, scam and cybercrime losses amounted to SGD913.1 million (\$706 million) in 2025,¹⁰ while Australia reported more than AUD2 billion (\$1.38 billion) in scam losses in 2025.¹¹ However, the impact of scams extends beyond direct monetary loss. The same GSMA report found that 68% of scam victims in 2025 lost money, but around 45% also reported time and effort spent resolving the incident, in addition to emotional distress and ongoing anxiety. These multi-dimensional harms erode the confidence needed for digital inclusion, mobile payments, digital identity, enterprise digitalisation and public-service access. As a result, operators are increasingly investing in cyber defence and anti-scam capabilities, not only as providers of digital access but also as part of the trust surface through which consumers are contacted, authenticated, warned and protected.

These trends are changing the role of operators in digital trust. The priority is moving from responding after harm occurs to reducing risk earlier, embedding cyber defence into networks, services and governance and working with partners in the wider ecosystem. This creates three related shifts: operators are embedding stronger security controls into their own infrastructure; turning these capabilities into enterprise-facing services; and deepening collaboration across sectors where scams and cyber risks unfold.

9. [ASEAN Consumer Scam Report 2025: Victims Rising, Defences Under Strain](#), GSMA, 2026

10. Annual scam and cybercrime brief 2025, Singapore Police Force, 2026

11. "Continued action critical to combat fraud as annual scam losses exceed \$2 billion", ACCC, March 2026

Digital trust moves from response to anticipation

The first shift is internal. Operators in Asia Pacific are building detection, filtering and risk-scoring capabilities more directly into their networks and customer channels, allowing suspicious traffic, identities and behaviours to be identified earlier and at greater scale. GSMA Intelligence survey data suggests the region is relatively advanced: around two thirds of surveyed Asia Pacific operators have adopted a proactive security approach, compared with 53% globally.¹² As networks become more software-defined, cloud-based and AI-enabled, digital trust will increasingly depend on continuous exposure management, AI-enabled scam and threat prevention, cross-domain visibility, and stronger governance and accountability.

Continuous exposure management

Preventative security depends on a continuous cycle of identifying weaknesses, testing exposure, remediating risks and keeping reporting channels open. For example, Telkomsel conducts Cyber Patrol, a regular programme of proactive monitoring and inspection on cyber risks, and vulnerability assessments across IT and telecoms networks, while KDDI provides a more integrated model, combining vulnerability scans with risk-based patching, configuration changes, 24/7 log monitoring and dedicated incident-response teams. Several other operators, including Singtel, Telstra, Optus, StarHub, Maxis and AIS, operate public vulnerability disclosure programmes, enabling external researchers to report issues privately. This helps reduce the window in which exposed system weaknesses can be exploited.

AI-enabled threat prevention

AI is becoming central to preventative security, enabling operators to turn network, call and messaging data into real-time risk signals that support earlier detection, instant warnings and automated intervention.

At the network layer, SK Telecom upgraded ScamVanguard, its anti-scam protection system, in 2025 with AI capabilities for bait-message detection, phishing-chat detection, voice-phishing call-pattern analysis and suspicious-identity-use detection. During 2025, it blocked around 1.1 billion attempted cases of voice spam, voice phishing and scam text messages, up 35% year on year.¹³ Meanwhile, Maxis has deployed an AI-powered firewall for voice and SMS traffic since January 2026 to screen international traffic and block scam calls, spoofed numbers and malicious messages.

At the user-facing layer, AI is being embedded into call-protection services. At MWC Barcelona 2026, SK Telecom showcased its A. Phone for real-time call safety, KT demonstrated AI-based voice-phishing detection and LG Uplus highlighted ixi-O Pro as a proactive AI call assistant with anti-phishing capabilities. In February 2026, Airtel launched Fraud Alert, which warns users when a banking OTP is received during a potentially risky call.

Network-wide threat visibility

As threats span IT systems, telecoms networks, edge nodes, cloud functions and enterprise environments, operators require detection capabilities that go beyond traditional enterprise security monitoring. Extended detection and response (XDR) tools can help address this by correlating signals across network assets and reducing detection and response times.

Globe Telecom, for example, has deployed an AI-powered XDR solution with Vectra AI to strengthen detection and response across its mobile network, enhancing protection for more than 80 million subscribers. Other Asia Pacific operators, including StarHub, Telstra and Telkomsel, are also adopting XDR tools to improve cross-domain visibility and response.

Governance and security accountability

Embedding trust across networks and services requires security to be built into people, processes and accountability structures, rather than simply leaving this to specialist teams. GSMA Intelligence research highlights the operator security gap in Asia Pacific: 68% of surveyed operators have security-awareness and training programmes, compared with 87% globally, and only 35% conduct role-specific training.¹⁴

This points to the need for stronger operating discipline, including threat-intelligence sharing, regular policy review, structured incident response and continuous employee training. SoftBank demonstrates this approach, with information security governance led by a chief information security officer and supported by a group security committee, enabling coordinated oversight, threat sharing and incident response across affiliated companies.

12. [Telco security governance and strategies: Asia Pacific](#), GSMA Intelligence, 2026

13. "SKT blocked 1.1 billion voice phishing and spam cases last year utilising AI technology", Maeil Business Newspaper, January 2026

14. [Telco security governance and strategies: Asia Pacific](#), GSMA Intelligence, 2026

Digital trust is emerging as one of the fastest-growing digital markets

Digital trust is moving from an internal defensive requirement to an externally addressable growth market. As enterprises digitise operations, adopt AI and face tighter regulatory expectations, spending on cybersecurity, identity, privacy and trust-enabling services is rising quickly across Asia Pacific. The IDC forecasts cybersecurity spending in Asia Pacific to reach \$60.6 billion by 2028, growing at a CAGR of 10.6% from 2025.¹⁵ Market-level forecasts point to the same momentum: information-security spending is expected to grow in 2026 by 11.7% in India¹⁶ and 9.5% in Australia,¹⁷ with faster growth in managed security services, security software, application security, data security and privacy.

Demand is also broadening. Enterprises need protection for cloud and AI workloads, identities, fraud risks, privacy obligations and digital-customer journeys, while AI is making threats such as deepfakes, synthetic identities and automated social engineering more sophisticated. For smaller businesses, the need is simpler but urgent: affordable protection for connectivity, devices and online transactions. This gives operators room to productise established security capabilities for the wider ecosystem.

Managed security as a service

Managed security is one of the most direct paths to commercialise digital trust, with operators packaging cyber defence beyond internal security operations centre and network protection into enterprise-grade services. In May 2026, Airtel Business launched Airtel Secure Workforce, a fully managed zero-trust-architecture platform designed to protect users, devices, networks, applications and data across hybrid work environments. Similarly, KDDI and its cybersecurity subsidiary LAC expanded their global security services, combining security monitoring, governance assessment and incident-response capabilities for enterprises with international operations.

Critical-infrastructure cyber defence

Critical-infrastructure cyber defence extends this model into highly trust-sensitive sectors such as transport, energy and public infrastructure, where service continuity and public confidence are central to national resilience and economic stability. In June 2026, SoftBank launched 'patching as a service', developed with OpenAI, to support vulnerability assessment and remediation for Japan's critical infrastructure. In India, Airtel Business secured a multi-year contract in 2025 to provide advanced cybersecurity services for Indian Railways' Security Operations Centre, covering sensitive systems such as ticketing, train tracking, freight, signalling, customer data and payments.

AI productisation

AI productisation is also emerging as operators embed AI into commercial security offerings. In September 2025, StarHub partnered with Vectra AI to launch an AI-powered threat-detection service for enterprises in Singapore, making the Vectra AI Platform available as part of StarHub's cybersecurity services. The offering combines Vectra's network detection and response technology with StarHub's hybrid IT capabilities to help enterprises detect, investigate and respond to sophisticated threats across modern digital environments.

15. "Security in an uncertain world: Tackling AI threats and trade pressures in Asia/Pacific", IDC, July 2025

16. "Gartner forecasts information security spending in India to total \$3.4 billion in 2026", Gartner, March 2026

17. "Gartner forecasts information security spending in Australia to reach over \$7.5 billion in 2026", Gartner, March 2026

Ecosystem collaboration is essential to deliver digital trust

Scams and cyber risks cannot be addressed by operators in isolation. Fraud chains increasingly span communications networks, financial services, digital platforms, device ecosystems and public reporting channels, while many scams also operate across borders. This is emphasised by the GSMA APAC Cross-Sector Anti-Scam Taskforce's (ACAST) anti-scam framework, pointing to the need for structured collaboration, peer learning, intelligence sharing and coordinated action across the wider digital ecosystem. This is becoming more important, as GSMA Intelligence research shows that 56% of Asia Pacific operators view supply-chain attacks as a significant threat.¹⁸ Building cyber resilience, and sustaining digital adoption, therefore depends on trust across the end-to-end service journey rather than only within the mobile network.

Public-private collaboration to support SMEs and national cyber resilience

SMEs are often disproportionately exposed to cyber risk yet lack the resources to adopt advanced protection. This creates a clear role for public-private models that combine policy reach with deployable operator capabilities. Singtel's Cyber Protect Programme, launched in October 2025 in partnership with Enterprise Singapore and the Infocomm Media Development Authority, illustrates this approach. The programme provides SMEs with 12 months of complimentary 'Mobile Protect' and 'Broadband Security', helping secure business mobile lines, broadband connections and connected devices against threats such as phishing, malware and ransomware.

Meanwhile, Axiata Group's August 2025 memorandum of understanding (MoU) with Cambodia's Ministry of Post and Telecommunications points to a broader form of collaboration. The partnership focuses on cybersecurity talent development, coordinated threat response and resilience building through a public-private framework, reinforcing the role of ecosystem cooperation in strengthening cyber resilience.

Cross-operator collaboration on defence technology

Some trust challenges require shared capability development, particularly where fraud patterns, voice intelligence and AI-enabled attacks evolve across markets. Syntelligence AI, which was incorporated in August 2025 and introduced publicly at MWC Barcelona 2026, provides a useful example. Backed by Deutsche Telekom, e&, Singtel, SK Telecom and SoftBank, the joint venture focuses on telco-grade AI solutions spanning scam and fraud detection, voice intelligence, automation and operational efficiency. This reflects a broader shift from standalone operator tools towards shared, reusable capabilities developed at the ecosystem level.

Trusted technical infrastructure for ecosystem collaboration

As highlighted by the GSMA ACAST anti-scam framework, cross-sector collaboration needs to extend beyond policy coordination to include technical cooperation, intelligence sharing and interoperable response mechanisms. Nearly three years after the launch of the GSMA Open Gateway – with several Asia Pacific operators among its initial signatories – authentication and fraud-prevention APIs remain central to the network API agenda. Building on this foundation, operators are now expanding common technical frameworks to support cross-sector trust. In March 2026, Spark, One NZ and 2degrees signed the GSMA Open Gateway MoU to develop compatible, cross-network APIs in New Zealand, initially focused on Number Verification and SIM Swap to enable real-time fraud prevention.

18. [Telco security governance and strategies: Asia Pacific](#), GSMA Intelligence, 2026



2.3

Resilience takes centre stage amid greater global uncertainty

Network resilience is becoming a strategic priority as operators navigate a more fragmented global environment. Geopolitical shocks, technology competition, emerging-market ambitions and pressure on trade routes, energy systems and critical infrastructure are all reshaping investment, technology access and supply-chain reliability.

For operators, resilience is no longer just about coverage or capacity; it is also about sustaining service continuity amid disruption, cost pressures and geopolitical risk. Across Asia Pacific, this is reflected in three responses: energy resilience, supply-chain diversification and hybrid connectivity as resilience architecture.

Energy resilience becomes part of network resilience

As operators in Asia Pacific expand 5G and prepare for more advanced connectivity demands, energy consumption is becoming closely linked to network resilience. Growth markets face expanding coverage needs and rising traffic, while leading markets must support denser, software-defined and industrial-grade networks that are driving higher energy intensity across mobile infrastructure. This comes at a time when power supply, tariffs and fuel availability are becoming more volatile in some markets amid growing global uncertainty. In response, operators are shifting beyond sustainability reporting towards operational resilience. This includes diversifying power sources and back-up systems, using AI and automation to improve energy efficiency and securing cleaner energy to support long-term infrastructure growth.

Power continuity as an immediate resilience priority

In markets facing acute energy stress, operators are prioritising layered power continuity within broader resilience strategies, such as in the Philippines and Japan:

- **Philippines:** PLDT and Smart registered 153 sites under the Retail Aggregation Program with Meralco's Mpower in July 2025, pooling demand to improve procurement flexibility and manage supply costs. In March 2026, during national energy-emergency conditions, Globe activated a layered continuity plan, which involved prioritising network performance, reducing non-essential energy use, securing generator fuel and reserving batteries as a last line of back-up.
- **Japan:** In May 2026, KDDI, SoftBank, Rakuten Mobile and NTT Group signed a joint agreement with seven manufacturers to secure portable batteries. Effective from 1 June 2026, the agreement enables rapid deployment to evacuation centres and affected areas during outages. In a market exposed to natural disasters, this strengthens the telecoms sector's role in maintaining connectivity when grid power fails, reinforcing energy continuity as both a network and societal resilience priority.

Innovating for lower energy intensity

Operators are also reducing the energy cost of capacity growth through software, automation and network design:

- In May 2026, Rakuten Mobile and KDDI launched a joint R&D project, backed by Japan's New Energy and Industrial Technology Development Organization, aimed at reducing data centre and RAN power consumption by around 40% by 2030.¹⁹
- In February 2026, Rakuten Mobile reached Level 4 validation in a live open RAN network, using cloud-native architecture and AI-driven automation to deliver around 20% energy savings in the RAN.²⁰
- In December 2025, Globe Philippines reported that AI and machine learning deployed across network and facility assets delivered savings of more than 11.3 million kWh over the year.²¹
- In November 2025, True Corporation achieved Level 4 validation for RAN energy efficiency. It is scaling up AI-based energy management across more than 10,000 base stations.²²

Cleaner power as a long-term resilience hedge

To reduce exposure to energy volatility, operators are securing cleaner power as part of network cost control and infrastructure resilience. By the end of 2025, Telstra reported renewable generation equivalent to more than 120% of its electricity consumption,²³ while True Corporation is targeting 49 MWp of clean energy capacity by 2026 through continued solar deployment across network sites and data centres.²⁴ Meanwhile, Globe aims to power more than 3,000 cell sites with renewables by 2028.²⁵

19. "Rakuten Mobile and KDDI selected by Japan's NEDO for R&D project to optimize virtualized infrastructure for sustainable telco", KDDI, May 2026

20. "Rakuten Mobile receives world first Level 4 autonomy validation for energy efficiency optimization in a live open RAN network from TM Forum", Rakuten Mobile, February 2026

21. "Globe cuts over ₱125M in energy costs through AI-powered efficiency", Globe, December 2025

22. "True corporation achieves Level 4 autonomy validation for 5G services assurance with Ericsson AI solutions", Ericsson, November 2025

23. "Target achieved: powering more renewable energy generation than we use", Telstra, 2026

24. True corporation sustainability-linked financing framework, True, 2025

25. "Globe to shift over 3,000 cell sites to renewable energy", ACEN, July 2025

Supply-chain fragmentation is a challenge for network resilience

Global technology supply chains are becoming more fragmented as strategic competition, export controls and industrial-policy priorities reshape access to critical digital infrastructure. Advanced technology markets are competing for leadership in AI, semiconductors and next-generation networks, while growth markets are placing greater emphasis on sovereign capability, data security and domestic value creation. These different strategic priorities are tightening the link between network resilience and technology resilience.

AI-driven infrastructure demand is adding further pressure: semiconductor revenues worldwide are expected to exceed \$1.3 trillion in 2026, with AI semiconductors accounting for around 30% of the total,²⁶ driven by AI infrastructure, memory and hyperscaler investment. This points to rising cost and supply pressures around semiconductors, high-bandwidth memory, accelerators and networking equipment, all of which are also relevant to operators' advanced connectivity, cloud, edge and automation plans. In response, operators in Asia Pacific are placing greater emphasis on diversified sourcing, trusted suppliers, local capability building and more efficient use of existing network assets.

Diversified and trusted sourcing

In Asia Pacific, vendor diversification is increasingly about reducing exposure to a single supplier, geography or closed technology stack while maintaining rollout speed, interoperability and cost discipline. Open RAN remains one of the clearest technical routes, as open interfaces can reduce dependence on closed vendor stacks while enabling multi-vendor integration. Examples of ongoing developments include the following:

- In April 2026, Japan's METI also selected Rakuten Symphony to trial virtualised open RAN across seven countries, including Indonesia, Vietnam, Malaysia and India, with around 100 virtualised base stations targeted in each market and funding support of up to JPY8 billion (\$50 million). This points to potentially broader adoption of open and software-led network architectures across the region.
- In June 2025, MobiFone and Rakuten Symphony signed an MoU to deploy a 4G/5G open RAN pilot, positioning MobiFone as one of Southeast Asia's early movers in this architecture.

Localisation and domestic capability

Over the long term, network resilience increasingly depends on the depth of domestic capability behind network deployment. This is especially important for fast-growing 5G markets that face a dual challenge: expanding coverage and capacity quickly while building the local technology base needed to sustain those networks over time. The infrastructure deployed today will serve as a long-term digital foundation, so supply assurance, software control, upgradeability and local integration are becoming part of resilience planning.

India has a clear plan in this regard. Under the Atmanirbhar Bharat agenda, BSNL is deploying an indigenously developed 4G stack that is technically upgradeable to 5G. By January 2026, more than 97,000 sites had been installed, with over 95,000 already live. This approach links rural and national coverage expansion to a broader strategic objective: strengthening domestic integration, enhancing software and upgrade capabilities and improving long-term supply assurance.

That said, for some 5G growth markets with large coverage needs, cost constraints and still-developing domestic technology ecosystems, the more practical route to supply resilience is phased and hybrid localisation. Rather than replacing global suppliers immediately, operators can build domestic capabilities progressively while maintaining access to mature technologies, competitive costs and faster deployment. This approach helps balance long-term strategic control with near-term network requirements, provided localisation is supported by predictable procurement rules, interoperability testing, supplier development and skills investment.

26. "Gartner forecasts worldwide semiconductor revenue to exceed \$1.3 trillion in 2026", Gartner, April 2026

Software-led capacity efficiency

Supply uncertainty, rising infrastructure costs and higher prices for embedded components are making network expansion a more selective investment decision. This is especially relevant to 5G growth markets, where operators must continue expanding coverage, improving quality and supporting traffic growth. In this context, resilience is not only about securing additional hardware, but also about extracting more value from existing assets. Software, automation and cloud-native architectures are becoming important tools to improve capacity and service quality with lower fixed infrastructure intensity, easing the component demand, capex burden and opex pressure associated with future network growth.

Cloud-native core is one pathway. While latency-sensitive and mission-critical functions will continue to require controlled private or dedicated environments, selected core network workloads can benefit from cloud elasticity, automation and on-demand scaling. NTT Docomo and NEC's commercial 5G core on AWS, launched in February 2026, illustrates this logic by allowing capacity to flex during traffic surges and scale back when demand normalises, reducing the need for permanent over-provisioning at the core-network layer.

Carrier aggregation provides another route at the radio and spectrum layer. By combining separate spectrum bands into a wider effective data pipe, operators can improve throughput and reliability from already deployed assets. Since May 2025, Telstra and Ericsson have deployed automated carrier aggregation across Telstra's 5G-Advanced sites in North Sydney, showing how real-time system intelligence can select optimal carrier combinations and improve spectrum efficiency. Similarly, Optus and Ericsson validated 180 MHz carrier aggregation across 2.3 and 3.5 GHz on a live 5G SA network in May 2026, demonstrating how smarter use of existing spectrum and radio assets can support capacity growth alongside targeted densification.



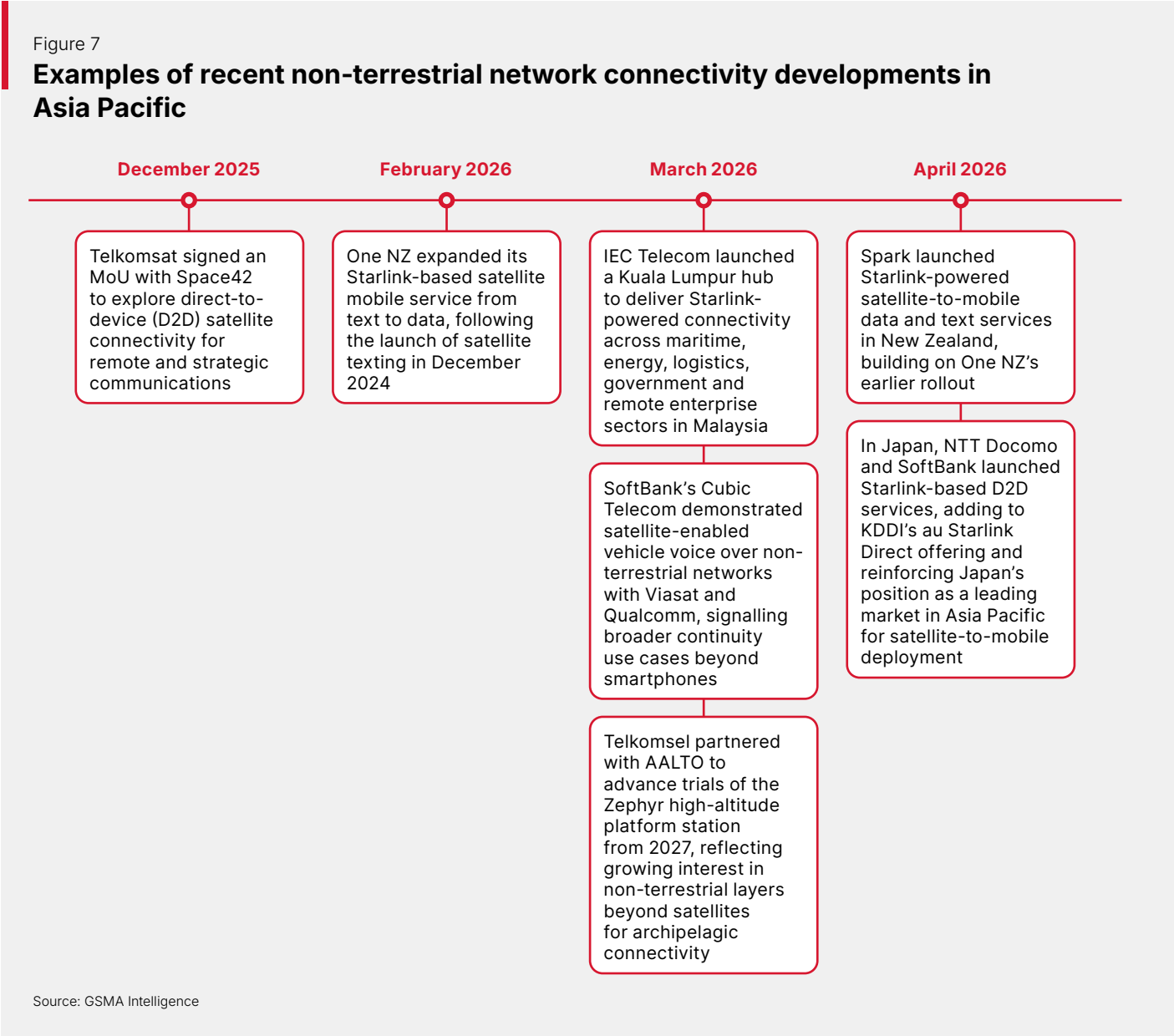
Hybrid connectivity: from a redundancy layer to resilience architecture

Resilient connectivity is increasingly defined by operators’ ability to maintain stable service under uncertain or adverse conditions, including remote geographies, maritime environments, transport corridors and disaster-response scenarios. Across Asia Pacific, these requirements are shifting hybrid terrestrial and non-terrestrial connectivity from a strategic concept to an emerging commercial reality. Recent operator activity suggests this transition is accelerating (see Figure 7).

For some remote island markets in Asia Pacific, the connectivity challenge is more acute, with network expansion relying on a mix of international technology providers, financing partners and local capabilities, making partner governance, trusted sourcing and long-term maintainability central to resilience.

In addition, geography, population dispersion and limited market scale constrain the economic and operational viability of terrestrial networks. In this context, hybrid connectivity plays a broader role than redundancy alone.

The Solomon Islands illustrates this. The partnership between Our Telekom and Intelsat uses managed satellite capacity to extend 3G and 4G coverage across remote and underserved communities spread over six major islands and more than 1,000 smaller islands. This highlights how satellite can enable coverage expansion where terrestrial rollout is constrained by geography, scale and cost. In such markets, hybrid connectivity is not just a back-up, but a practical foundation for scalable and sustainable network coverage.



03

Mobile industry impact



3.1

Turning connectivity into digital participation

Through sustained operator investment, Asia Pacific’s mobile broadband coverage gap narrowed to 2% by 2024. The remaining gap mostly comprises remote villages, mountainous areas, island communities and low-density rural markets. The inclusion challenge is therefore becoming more targeted and demand led.

Yet coverage alone is not enough. As such, operators are increasingly focused on adoption barriers, including devices, affordability, digital skills, localised content, trust, AI access and connected public services.

Democratising digital and AI access

As AI becomes a stronger driver of productivity, operators are leveraging their scale, apps and service bundles to extend access beyond early adopters.

Emerging activity highlights three priorities: widening access to premium tools; developing affordable and localised service models; and building the skills needed for confident use (see Table 2).

Table 2
Activities for digital and AI democratisation

Activity	Examples
Access to AI tools	• In 2025, Airtel partnered with Perplexity to offer 12 months of Perplexity Pro free to its customers – a high-value subscription worth INR17,000 (\$198). It extended this approach in January 2026 by bundling one year of Adobe Express Premium worth INR4,000 (\$47), expanding access to AI-enabled creative tools. • Reliance Jio offered eligible Unlimited 5G users 18 months of Google AI Pro, valued at INR35,100 (\$399).
Affordability and localisation	• In May 2026, Globe introduced AI Fiesta in the Philippines, bundling multiple AI platforms into an affordable service for students, creators, SMEs and entrepreneurs. • In 2025, Dialog Axiata launched a data-free, trilingual AI portal in Sri Lanka that supports Sinhala, Tamil, English and hybrid-language use. • In the same period, LG Uplus launched U+Pick AI in South Korea, offering a flexible subscription model that combines multiple AI tools.
Skills, confidence and accessibility	• Telstra’s Being Digital programme expanded across South Australia in 2025, delivering free training on device use, online safety, digital banking and AI to more than 4,000 residents. • In November 2025, PLDT and Smart launched AI-in-a-Box to support teachers working with students with disabilities. • In October 2025, CelcomDigi trained over 150 teachers across 134 inclusive schools, equipping them to deliver STEM and digital skills programmes to more than 10,000 students with disabilities.

Source: GSMA Intelligence

Extending participation into essential services

The inclusion agenda is moving from connectivity availability to service enablement, with operators using networks, apps, AI tools and hybrid connectivity to translate access into learning outcomes, welfare gains and more inclusive participation, as highlighted in the examples below:

- **Philippines:** PLDT and Smart partnered with Ateneo de Zamboanga University to launch literacy apps for Chavacano and Tausug communities, supporting local-language learning and cultural inclusion.
- **Sri Lanka:** Dialog Axiata's trilingual AI portal helps students summarise, translate and practise writing while supporting teachers with lesson plans and simplified learning materials.
- **South Korea:** LG Uplus added Science Donga AiR as a genAI tutor for science and maths, while KT's mobile KT AI Station is bringing AI-based learning experiences to middle schools.
- **Malaysia:** In November 2025, CelcomDigi and Hospital Pengajar Universiti Malaysia Sarawak launched MediRover and MediDoc in Sarawak, combining 5G and satellite connectivity with virtual consultations, AI diagnostics and remote monitoring to improve rural healthcare access. In December 2025, CelcomDigi also partnered with Universiti Malaya Medical Centre on a 5G-enabled AI 'holomedicine' initiative to support live surgical training and cross-border clinical collaboration.
- **Japan:** NTT Docomo has introduced AI-driven health services that use smartphone data (subject to user consent) to assess health risks and deliver personalised lifestyle guidance via platforms such as 'd Healthcare' and 'Health Mileage'.
- **South Korea:** SK Telecom's AI Care service supports vulnerable users, including older individuals and those at risk of isolation. Its AI Care Centre uses AI speakers and calls to detect anomalies and trigger follow-up support, connecting users to counselling, human care or emergency services when needed.

3.2

Enabling local economic value creation

Operator-led inclusion is also enabling more active participation in commerce. Digital finance is central to this shift, allowing individuals to transition from basic access to formal economic activity through mobile payments, credit, savings and insurance. JazzCash illustrates the scale of this, as the operator reported 29.2 million active users and PKR16.8 trillion (\$59.7 billion) in transaction value over the 12 months to March 2026, up 56% year on year.²⁷

In addition, operators are providing capital, merchant tools, AI-enabled support and data insights to help small businesses formalise their operations and build capabilities for sustainable participation in the digital economy, such as the following:

- **Indonesia:** Telkomsel launched QRIS Soundbox, SiteSense and Savia in August 2025, combining payments, location intelligence and customer engagement tools to integrate telco data and AI into enterprise and merchant operations.
- **Malaysia:** Axiata's Boost ecosystem uses e-wallet data to enable lending for SMEs with limited credit histories. By May 2025, Boost Bank had disbursed nearly MYR150 million (\$35 million), with plans to expand into a broader SME platform covering payments, operations and financial management.²⁸
- **Philippines:** Globe and GCash are digitising public markets, starting with Lucena Public Market, providing free Wi-Fi and enabling cashless payments. The model expanded to Maypajo in May 2026, adding access to digital credit, insurance and bookkeeping tools.
- **Sri Lanka:** Dialog Axiata has introduced AI tools for SMEs to generate invoices, cash-flow templates, business plans and multilingual content, as well as to summarise government circulars, reducing the reliance on specialist services.

27. VEON 2026 Q1 earnings release, 2026

28. "Boost Bank reaches SME financing milestone: close to RM 150 million disbursed to hundreds of SMEs", Boost Bank, May 2025



3.3

Empowering the green transition

In the wider climate context in Asia Pacific, the urgency for the green transition is becoming harder to ignore. Data from the World Meteorological Organization shows that Asia is warming nearly twice as fast as the global average,²⁹ while natural-disaster losses in Asia Pacific reached around \$73 billion in 2025, 11% above the 10-year average of \$66 billion, with only \$9 billion insured.³⁰ Beyond direct losses, pressure is also growing on power, transport, data-centre and telecoms infrastructure due to rising heat, flooding and extreme weather. This is adding urgency to reducing the sector's energy intensity, emissions and resource footprint, as highlighted by the following examples:

- **Energy efficiency:** Singtel invested SGD335 million (\$259 million) in 2025 across Singapore and Australia to improve energy efficiency, reduce emissions and strengthen network resilience. Telstra's 2025 annual report showed a 44% reduction in Scope 1 and Scope 2 emissions and a 43% reduction in Scope 3 emissions from its 2019 baseline. Axiata also cut energy intensity by 7.7% in 2025 through solarisation, expanded fibre backhaul and energy-efficiency investment.
- **Green energy:** Singtel consumed 65.1 GWh of renewables-backed electricity across Singapore and Australia in 2025 (roughly equivalent to the annual electricity use of 14,000 Singapore four-room HDB households) and made its Malaysia operations 100% renewables-backed through Renewable Energy Certificates. In 2025, Globe expanded its renewables-energy footprint to 358 sites (having set a target to shift more than 3,000 sites to renewable energy by 2028) and reduced Scope 1 and 2 emissions by 15.13% year on year.
- **Circularity:** Singtel and Optus diverted 100% of used mobile devices collected through take-back schemes from landfill or incineration in 2025, while SK Telecom's 'RE' strategy focuses on reducing waste and improving reuse, recycling and resource efficiency across network equipment, devices and operations.

29. State of the climate in Asia 2025, World Meteorological Organization, 2026

30. Climate change presses on: Devastating wildfires and intense thunderstorms exacerbate losses for insurers", Munich Re, January 2026

3.4

Supporting disaster management and emergency response

As global warming intensifies, Asia Pacific's disaster-resilience agenda is operating in an increasingly volatile multi-hazard context. The region continues to face high-impact earthquakes, destructive rainfall, flooding, heat and drought. Its island, coastal, mountainous and remote communities remain especially exposed to disruption. As extreme weather becomes more frequent and less predictable, mobile connectivity is being elevated from a post-disaster recovery tool to a part of public-safety infrastructure, supporting early warning, emergency connectivity and coordinated recovery:

- **Last-mile public warning:** Operators have a specific role in early warning because mobile networks are often the widest-reaching real-time communication channel available to the public. This is especially important in disaster-prone island and coastal markets, where alerts must reach residents, visitors and vulnerable communities quickly, without relying on app downloads, mobile data or individual phone numbers. In 2025, the Solomon Islands showcased a cell-broadcast-based early warning system, with local operators Our Telekom and Bmobile involved alongside disaster-management and meteorological agencies.
- **Emergency fallback connectivity:** The ability to stay connected during and immediately after a disaster is becoming a life-saving resilience measure. It allows people to receive critical information, contact family members, seek assistance and reduce panic through trusted information flows. Following the 2026 Mindanao earthquake in the Philippines, operators and government agencies deployed satellite-backed emergency connectivity, free Wi-Fi, charging stations and emergency communications services. Globe also activated Starlink-enabled satellite-to-mobile support in affected areas, offering free satellite data and SMS while network restoration continued.
- **Coordinated recovery and roaming resilience:** Operators are also moving from ad hoc support to more structured recovery coordination. In Mindanao, Globe restored services in affected municipalities while providing free calls, charging and Wi-Fi sites. Japan illustrates a more system-level model: in 2026, the country's five mobile carriers launched the 'Japan Roaming' service, allowing users to temporarily connect to another carrier's 4G network if their own service is disrupted by a large-scale disaster or major outage. These examples show how mobile operators are becoming core resilience partners in disaster-prone Asia Pacific markets.

04

Policies to enable innovation and growth



Sustaining digital innovation and economic growth remains a key objective for governments and stakeholders across Asia Pacific. While the region stands out as one of the world's most dynamic digital markets, it continues to face persistent challenges – many rooted in its diversity – including uneven connectivity and rising threats to digital trust.

4.1

Closing the usage gap

Across Asia Pacific, sustained investment in mobile broadband infrastructure, particularly 4G, has reduced the coverage gap to low single digits in percentage terms over the past decade. In South Asia, the coverage gap has fallen from around 30% to less than 5%. However, significant gaps remain in some areas, especially the Pacific Islands, where the coverage gap still exceeds 15% on average. As a result, building resilient mobile and digital infrastructure in underserved communities remains a priority for governments and industry stakeholders. India's BharatNet initiative and the growing number of telco-satellite partnerships illustrate wider ecosystem efforts to extend coverage.

Closing the usage gap is a more difficult challenge, given its scale and the complex mix of factors that limit people's ability and willingness to use mobile internet. In Asia Pacific, more than 1 billion people, including nearly 700 million adults, are covered by mobile broadband but remain offline. Key barriers include limited access to affordable smartphones, low digital skills, weak perceptions of the value of mobile internet, lack of digital trust and online safety concerns.

The size of the usage gap and the factors driving it differ markedly across the region. The usage gap is widest in the Pacific Islands and South Asia, where affordability remains a major constraint, while in developed Asia Pacific the main barrier is often limited digital skills among older users. This underlines the need for market-specific strategies rather than a one-size-fits-all approach. Policymakers and industry stakeholders should therefore start by identifying the specific barriers in their markets, so interventions can be targeted where they will have the greatest impact. The GSMA Mobile Connectivity Index³¹ provides a practical framework to guide this assessment.

Key priorities for policymakers and industry stakeholders in the region include closing the usage gap, optimising spectrum management to support efficient infrastructure rollout and maintaining high levels of digital trust as a foundation for an advanced digital economy. Enabling policies that address these interconnected priorities are essential to build a resilient and inclusive digital ecosystem and attract the much-needed investments to finance and de-risk the next phase of digital development.

Across Asia Pacific, stakeholders are using market-specific interventions to address the usage gap. In Indonesia, the Ministry of Communications and Information Technology has worked with regional partners, including East Ventures, to develop digital literacy indices and tailored curricula that address generational and gender gaps, such as digital safety and financial literacy training for rural women and small merchants. In India, the flagship PMGDISHA programme under Digital India has trained more than 64 million rural citizens, helping build foundational digital skills and support adoption of mobile internet, public services and e-commerce.³²

The next priority for policymakers is to make inclusion policies more demand-led and sustainable. This requires moving beyond one-off subsidies or training schemes towards integrated pathways that combine affordable access, capable users and essential digital services. Short-term measures such as device subsidies or temporary tariff discounts may lift adoption temporarily, but they do not guarantee lasting connectivity. Governments and industry should therefore tackle underlying cost barriers by reducing taxes and fees on entry-level smartphones and expanding innovative financing models such as micro-loans and pay-as-you-go leasing.

Policies should also help build capable and confident users while expanding services that people see as essential. This means going beyond basic digital literacy to provide targeted, ongoing support for vulnerable groups and training in practical skills, such as mobile financial services and online safety. At the same time, scaling up relevant digital services, including localised applications and support for micro-entrepreneurs, can create sustained demand. Achieving this at scale will require coordinated action across government, the industry and civil society to build an integrated digital ecosystem.

31. [GSMA Mobile Connectivity Index](#)

32. "A Decade of 'Digital India Mission': Achievements, Gaps, and the Way Forward", Observer Research Foundation, August 2025

4.2

Optimising spectrum access for future services

Harmonising spectrum for mobile evolution

Long-term access to spectrum is essential to support sustained investment in network infrastructure. Countries across Asia Pacific can support the development of mobile technologies by developing long-term roadmaps for low-, mid- and high-band spectrum into the 2030s.

For mid-bands, important ranges include 3.5 GHz, which has been used as the basis for 5G launches, and the 6 GHz band, which has also been harmonised internationally for future mobile evolution. Following its identification for IMT at the World Radiocommunication Conference 2023 (WRC-2023), the 6 GHz band offers administrations an opportunity to address longer-term spectrum needs. As demand for mobile grows and existing mid-band resources become increasingly utilised, 6 GHz can support future capacity requirements and create a pathway towards 6G. Furthermore, discussions at WRC-27 may also extend the band into 7 GHz.

Timely and adequate access to mid-band spectrum helps the development of networks so they can provide high-capacity connectivity for a variety of applications. These include expanded high-resolution video streaming, extended reality, enterprise digitalisation and AI.

Low bands, such as the 600 and 700 MHz bands, support wide coverage and help narrow the digital divide between urban and rural areas. Rural users spend twice as much time connected to low bands as urban users, making them important for improving digital inclusion.

Expanding access to low-band spectrum has multiple benefits and improves the business case for covering rural areas. For example, an additional 50 MHz of sub-1 GHz spectrum is linked to an increase of 7 percentage points (pp) in 4G coverage and 11 pp in 5G coverage.³³

Sufficient low-band capacity is an important tool for creating greater urban/rural parity. Although significant attention has recently been given to D2D for increasing connectivity, this will only provide a low-bandwidth coverage layer. Low bands will cover most rural traffic.

33. [Spectrum and rural connectivity](#), GSMA, 2025

Spectrum roadmaps

Roadmaps are an important means of ensuring there is sufficient spectrum for growing demand from consumers and new technologies. Clarity on future spectrum can help mobile operators prepare investment plans, secure financing and develop

arrangements for deploying different technologies. Across Asia Pacific, several countries have outlined spectrum roadmaps that provide time frames for access to core bands, including the 2.6, 3.5 and upper 6 GHz bands.

Case study:

A roadmap to accelerate mobile evolution in the Philippines

Mobile data traffic per connection in the Philippines reached 7.7 GB per month in Q4 2025,³⁴ reflecting sustained demand for mobile broadband. The country was the first in the Association of Southeast Asian Nations (ASEAN) to launch commercial 5G services in June 2019, providing a strong foundation for future network development.

However, further progress is required to support the nationwide rollout of high-quality 5G and 5G-Advanced services and respond to increasing traffic growth. Limited availability of large, contiguous blocks of IMT spectrum continues to constrain network performance and coverage. While recent assignments in the 2.6 and 3.5 GHz bands are positive steps, additional access to mid-band spectrum in the 1–7 GHz range will be important to support continued growth. Markets are expected to require around 2–2.5 GHz of mid-band spectrum in the 2035–2040 period, compared to approximately 845 MHz currently assigned for mobile services in the Philippines.

Building on its early leadership in 5G, the Philippines could benefit from adopting a clear and forward-looking spectrum roadmap. This would help ensure that spectrum is made available in a timely and coordinated manner, supporting investment and the continued evolution of mobile networks.³⁵ The Philippines has already started moving in this direction, with the Department of Information and Communication Technology announcing plans in 2026 to optimise spectrum use as part of its work on its new Spectrum Management Policy Framework.

Spectrum pricing

Spectrum costs can influence network investment, both at the point of allocation (e.g. upfront fees or auctions costs) and through ongoing fees and renewal charges. Governments and regulators may therefore wish to consider assignment approaches that balance revenue considerations with wider digital connectivity objectives.

Spectrum costs are an increasing burden for mobile operators. A GSMA study found that spectrum cost-to-ratio revenues in Asia Pacific rose from 3% in 2014 to 9% in 2023. Lessening this burden has a positive impact. The same study indicates that a 10 pp decrease in this ratio is associated with a 6 pp increase in coverage and an 8 pp increase in speeds.³⁶

Governments and regulators are increasingly mindful of the negative impact of high prices and poorly designed assignment mechanisms. As such, they are adopting new pricing and licensing approaches to ease the financial pressure on operators while encouraging investments in connectivity and coverage. These approaches include extending licensing terms without additional payments, helping create an investment-friendly environment for the future, and attaching coverage commitments in exchange for lower prices when auctioning or renewing spectrum. This trend is evident in Asia Pacific, where several countries, including Fiji, Indonesia, Pakistan, Papua New Guinea and Vietnam have adopted more conservative reserve prices in spectrum auctions.

34. Source: GSMA Intelligence. Based on the total number of mobile subscriptions. The average data consumption per mobile data subscription is significantly higher.

35. [Accelerating 5G and 5G-Advanced in Philippines: A Roadmap for Success](#), GSMA, 2026

36. [Global Spectrum Pricing](#), GSMA, 2026

Licence renewals

Regulators are increasingly adopting transparent processes and innovative renewal mechanisms, such as zero-cost extensions tied to coverage obligations, to align with national connectivity goals. Regulators can support the delivery of better service quality by ensuring renewal decisions are made five years ahead of the renewal date.

Continued network development is required to support growing consumer and business needs as traffic demands increase. However, operators may not invest in their networks if there is uncertainty

over future spectrum rights. Uncertainty can be reduced by creating a presumption of licence renewal except under exceptional circumstances.

To encourage network investment, spectrum fees should not be tied to historical prices, and renewal charges should be avoided as they raise costs and may ultimately impact consumers. Instead, regulators could promote efficient use through mechanisms such as spectrum trading, renewal conditions linked to investment commitments or administrative review.

WRC-27 and 6G

Asia Pacific is home to several countries that are leading the evolution of mobile technologies. Some recent examples of progress include the following:

- **India**, which published a spectrum roadmap for 6G services, has strategically outlined its long-term spectrum planning.
- **South Korea** has set out a three-year national roadmap to strengthen its position in AI, underpinned by plans for a 6G rollout in 2030.
- **Vietnam** aims to become a regional 6G leader by building on its rapid 5G deployment and using next-generation networks to support industrial digitalisation.

The discussion around future mobile spectrum is evolving. While 6 GHz is expected to play an important role in supporting growing connectivity demands, studies for WRC-27 are also examining other mid-band options, including spectrum in the 4.5 and 7–8 GHz ranges. 6G will use wide 200–400 MHz channels. To enable this, alongside the transition path for any incumbent spectrum users, long-term planning for harmonisation, equipment development and deployment will be required.

Enabling D2D

D2D describes connectivity between satellites and mobile handsets. It can supplement coverage for people who already have a mobile connection. In addition, it can offer connectivity to those that live outside terrestrial mobile coverage and can afford a device and service plan.

D2D can also expand resilience, especially during emergencies when there are terrestrial network outages. D2D's weaker signal and lower spectrum efficiency mean it cannot provide meaningful

connectivity in populated areas such as cities and towns.³⁷ Its use will therefore be limited to rural areas with very low or no population. In populated rural areas, low-band terrestrial mobile will likely remain a more efficient way of delivering mobile broadband.

WRC-27 will consider the development of D2D. A critical part of the conversation will focus on enabling D2D while ensuring that there is no harmful interference to the terrestrial mobile services that so many people rely on.

37. [The Limits of D2D: Modelling the extent of D2D connectivity](#), GSMA, 2026

4.3

Embedding digital trust into policy frameworks

Digital trust – the confidence that digital technologies and ecosystems are secure, private, reliable and well governed – is essential to digital adoption. People are more likely to use digital services when they believe their data is protected, systems will work as intended and risks such as fraud or misuse are being managed. This is especially important for sensitive or high-value services, including digital finance, health platforms and identity systems, where perceived risks can outweigh expected benefits. Strong trust frameworks covering cybersecurity, data protection, transparency and accountability can reduce these concerns, helping to increase uptake and deepen engagement.

Digital trust also shapes investment and wider economic growth. Businesses and investors are more likely to commit capital in markets with clear, predictable rules and institutions that can enforce standards on data use, competition and security. Trusted environments lower transaction costs, enable cross-border data flows and support the growth of digital business models. This creates a reinforcing cycle: trust attracts investment, while investment supports innovation and infrastructure development. These gains expand digital participation and productivity. In this sense, digital trust is more than a safeguard; it is a strategic asset for sustainable and inclusive digital growth.

As online threats escalate, governments need to embed digital trust at the centre of policy frameworks. Cyberattacks and wider digital risks impose significant costs, from financial losses and reputational damage to declining confidence in online services. Addressing these risks requires a shift from reactive measures to proactive, pre-emptive policy design. Cybersecurity and data privacy should therefore be treated as core foundations of digital policy, ensuring that e-services, AI deployment, data sharing and digital identity systems are reliable, transparent, secure and rights-respecting by design.

Across Asia Pacific, several governments are embedding digital trust more deeply into public policy frameworks. This is helping strengthen confidence in digital interactions and providing models for others to follow. Rather than relying on fragmented or reactive cybersecurity measures, these governments are taking a more holistic approach, integrating security, privacy, transparency, accountability and ethical governance into national strategies for digital identity, data sharing, AI and wider digital transformation. Australia's Trusted Digital Identity Framework, for example, sets rules and standards for safe, secure, consistent and reliable access to online government services, including privacy protections and fraud controls.

An important way for policymakers to embed digital trust is through early and sustained engagement with industry. This helps regulators understand the roles, capabilities and constraints of different sectors, supporting the design of effective and trustworthy frameworks. Early dialogue can improve policy alignment and give authorities clearer insight into operational processes, enabling more informed rulemaking. Cross-sector training and regular consultation can also help ensure that regulations are practical, achievable and aligned with industry realities while giving sectors enough flexibility to adopt approaches that fit their operating contexts.



Balancing trust and innovation

Embedding digital trust in policy frameworks brings clear benefits, but it also creates trade-offs that need careful management. Poorly designed rules can slow innovation by raising compliance costs (especially for SMEs), increasing regulatory fragmentation across borders and weakening competitiveness. Governments therefore need to protect trust while allowing innovation. Practical tools include regulatory sandboxes for supervised technology testing, modular self-assessment toolkits, voluntary certification tiers and sector-specific guardrails.

Several countries are already taking this approach by treating trust as a growth enabler rather than a constraint. Singapore combines its voluntary Model AI Governance Framework with open-source testing tools such as AI Verify, an AI governance testing framework and software toolkit, giving businesses clearer guidance without limiting development. Japan has adopted agile, non-binding guidelines supported by public-private partnerships, helping keep barriers low for smaller technology firms while reinforcing social trust and international interoperability.

4.4

Strengthening multi-stakeholder collaborations

AI, quantum computing and other advanced technologies will shape future economies and societies, creating new opportunities for growth and improving people's lives. Their deployment depends on high-performance digital infrastructure, including advanced 5G and, over time, 6G networks, as well as edge, cloud and energy infrastructure. While private investment has supported much of Asia Pacific's digital infrastructure to date, building future-ready infrastructure and the skills and innovation ecosystems needed to use it effectively will require new collaboration models.

Strengthening resilience

As critical systems become more interdependent, disruption in one sector can quickly affect others, such as when power outages disable mobile sites or connectivity failures disrupt transport, water or emergency-response systems. Governments can reduce systemic risk by connecting the operational planning of telecoms operators, utilities, emergency services and infrastructure owners to turn fragmented systems into a more coordinated resilience ecosystem. This can speed up disaster recovery, protect emergency communications when networks are congested and reduce the economic impact of prolonged infrastructure outages, as outlined in the following examples:

Governments can play a central convening role by bringing ecosystem stakeholders together around three priorities for future digital infrastructure: strengthening resilience, accelerating innovation and improving policy outcomes.

- In **Japan**, major operators, including NTT Group, KDDI, SoftBank and Rakuten Mobile, participate in the national Connect to Change project. During major earthquakes or tsunamis, competing operators can share physical assets such as refuelling stations, local business facilities and accommodation hubs to accelerate regional repair and restoration efforts.
- In **the Philippines**, telecoms operators such as Smart and Globe are integrated into the national early warning system through collaboration with the National Disaster Risk Reduction and Management Council. Using cell broadcast technology, emergency services can send localised, real-time evacuation alerts directly to mobile devices, bypassing network congestion and avoiding reliance on mobile data or individual phone numbers.

Accelerating innovation

Innovation is essential to convert emerging technologies such as AI, quantum computing and next-generation connectivity into social and economic value. A country's ability to shorten the time to market will shape how quickly it can respond to supply-chain shocks and shifting economic conditions. Governments across Asia Pacific are supporting this by convening ecosystem players through regulatory sandboxes, public-private collaboration and shared technology platforms.

Sandboxes allow SMEs and technology providers to test new solutions in live but supervised environments without immediate regulatory penalties. For example, regulators from several countries, including Singapore, Malaysia and Thailand, launched a joint AI regulatory sandbox, allowing regional tech firms to experiment with genAI models and data flows across borders under soft-law compliance guidelines.

Improving policy outcomes

Governments can improve policy outcomes by breaking down sector silos and convening a cross-industry digital ecosystem. This whole-of-society approach draws on private-sector innovation, scale and expertise while aligning activity with public goals such as inclusive service delivery and broader economic participation. By bringing together stakeholders across telecoms, banking, healthcare, education and public services, governments can support evidence-based policymaking and set standards for secure, interoperable platforms that deliver public services more efficiently.

This collaboration is becoming more important as digital and data sovereignty move up the policy agenda. Data localisation requirements, sovereign cloud initiatives and expectations for in-country infrastructure are pushing governments and private partners towards clearer, more structured models of engagement. This is giving rise to sovereignty-aligned policies that balance national priorities with private-sector innovation and efficiency. India's Digital Public Infrastructure, often referred to as the India Stack, illustrates this approach by convening telecoms operators, banks, healthcare providers, education bodies, data providers and technology innovators to deliver scalable, inclusive outcomes while maintaining national control over core digital systems.

Further reading

ASEAN consumer scam report 2025: victims rising, defences under strain

GSMA, 2026

Telco security governance and strategies

GSMA Intelligence, 2026

GSMA Open Gateway: State of the Market, H2 2025

GSMA Intelligence, 2025

GSMA Head Office

1 Angel Lane
London
EC4R 3AB
United Kingdom

