GSMA

The Mobile Economy 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**

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

Moving beyond connectivity

The mobile industry underpins global connectivity, enabling seamless communication, real-time data exchange and an expansive ecosystem of consumer and enterprise applications. Today, it supports 8.8 billion wireless connections, including 5.8 billion unique subscribers – around 70% of the global population – who rely on mobile services for communication, commerce and access to digital platforms. While extending ubiquitous connectivity through advanced 4G and 5G networks remains a core priority, the industry is also entering a new era shaped by intelligent, adaptive and value-added digital services. This shift is being enabled by next-generation mobile networks, such as 5G standalone architectures, and the rapid integration of AI and other transformative technologies across consumer applications and enterprise solutions.

These developments mark a shift from a connectivity-centric model to one driven by advanced digital platforms and data-enabled innovation. To support this transition, the mobile industry is leveraging core network assets, such as network slicing and open APIs, to deliver differentiated services. It is also investing in new capabilities and forming partnerships across the digital ecosystem to scale up offerings beyond connectivity and open up new revenue streams.

This evolution is already reshaping the global economy. The contribution of mobile technologies and services to global GDP is projected to rise from $7.6 trillion in 2025 (6.4% of GDP) to $11.3 trillion by 2030 (8.4%). In 2025, the industry supported 50 million jobs worldwide and generated more than $800 billion in public revenues, underscoring its role as a major economic and fiscal driver.

8.8bn

The industry supports 8.8 billion wireless connections, including 5.8 billion unique subscribers

50m

In 2025, the industry supported 50 million jobs worldwide and generated more than $800 billion in public revenues

$11.3tn

The contribution of mobile technologies and services to global GDP is projected to rise from $7.6 trillion in 2025 (6.4% of GDP) to $11.3 trillion by 2030 (8.4%)

Key trends shaping the mobile ecosystem

AI monetisation

45% of operators see AI-enabled revenue streams as a strategic priority

Operators are increasingly repositioning AI from a cost-optimisation tool to a core driver of new revenue. In a GSMA Intelligence survey, 45% of operators identified AI-enabled revenue streams as a strategic priority. AI monetisation spans a broad spectrum, from core and private-cloud deployments to enterprise and device-level edge applications, with distinct technical and commercial trade-offs at every stage.

Network security

90% of operators report using multi-layered defence architecture

Safeguarding network integrity, ensuring service continuity and meeting regulatory standards are fundamental to maintaining trust and competitiveness. Over 90% of operators in a GSMA Intelligence survey report using multi-layered defence architectures, while 80% have formal incident-response plans. AI is a double-edged sword, as it strengthens security capabilities but also creates new vulnerabilities. This makes robust governance, continuous monitoring and a skilled workforce essential for tackling AI-enabled threats.

Device innovation

Shifting from hardware-centric innovation to experience-led value creation

Consumer value is increasingly defined by how well a device anticipates user intent, adapts to real-world context and integrates into a broader multi-device ecosystem – rather than by its standalone technical specifications. This marks a shift from hardware-centric innovation to experience-led value creation, with AI emerging as the primary driver of device differentiation. AI capabilities now play a significant role in shaping purchase decisions and influencing upgrade cycles.

eSIM momentum

By 2030, eSIM will account for 42% of all SIM technologies

Once limited to premium smartphones, eSIM has become standard across mid-range devices, wearables and an expanding array of connected products, simplifying activation and reducing dependence on physical SIM cards. Beyond improving customer experience and reducing operational friction, eSIM creates direct monetisation opportunities by enabling seamless multi-device connectivity and supporting new, flexible service models. GSMA Intelligence projects that eSIM-enabled smartphone connections will reach 2.5 billion by 2028, with eSIM accounting for 42% of all SIM technologies by 2030.

Enterprise digital transformation

Enterprises plan to allocate 10% of revenues to digital transformation in 2025–2030

Enterprises plan to allocate around 10% of revenues to digital transformation between 2025 and 2030, underscoring a shift in perception from digitalisation as a cost centre to a core driver of long-term value creation. This investment wave is widening the B2B opportunity landscape for technology providers, with operators well positioned to capitalise on this opportunity as they evolve from traditional connectivity suppliers into full-stack technology partners by leveraging their network assets, enterprise relationships and emerging platform capabilities.

The impact of the mobile industry

By expanding access to affordable networks, devices and scalable digital services, the mobile industry is helping to close long-standing gaps in public-service access, particularly for marginalised communities. It is also reducing the carbon intensity of connectivity and enabling more efficient digital operations across sectors, supporting large-scale decarbonisation and progress towards net-zero goals. In parallel, the sector plays a vital role in disaster preparedness and response, providing resilient communication networks that underpin early-warning systems, real-time information flows and coordinated humanitarian efforts.

Policies for growth

While 5G deployments continue, the mobile ecosystem is already working with governments to plan spectrum for 6G, which is expected to come into use in the 2030s. Channel sizes will expand significantly, from 100 MHz in the 5G era to 200–400 MHz, reflecting the higher performance requirements of next-generation networks. Although widespread 6G rollout is unlikely before the 2030s, spectrum harmonisation efforts in bands such as 4.5 GHz and 7 GHz are well underway. The World Radiocommunication Conference 2027 (WRC-27) will examine these and other mid-band ranges, including 7–8 GHz, as candidates for the next phase of mobile evolution. Because these bands already host incumbent services and given the long lead times for international harmonisation, equipment development and network deployment, regulators and policymakers must begin planning now to meet future mobile spectrum needs.

Combatting fraud has become a priority for governments, regulators, the mobile industry and the wider digital ecosystem, underscoring the need for coordinated, cross-sector action. The global financial cost of cybercrime, including fraud, is projected to rise from $9.22 trillion in 2024 to $15.63 trillion by 2029. For consumers, the consequences can be severe, ranging from financial loss to emotional distress and a loss of trust in digital services, which in turn hinders the adoption of beneficial technologies. Human behaviour remains a critical vulnerability, with criminals increasingly using social engineering to extract the information needed to commit online crimes.

The Mobile Economy

State of mobile internet connectivity

2024

As mobile internet adoption continues to grow faster than network expansion, the usage gap is falling. However, it remains almost 10 times larger than the coverage gap.

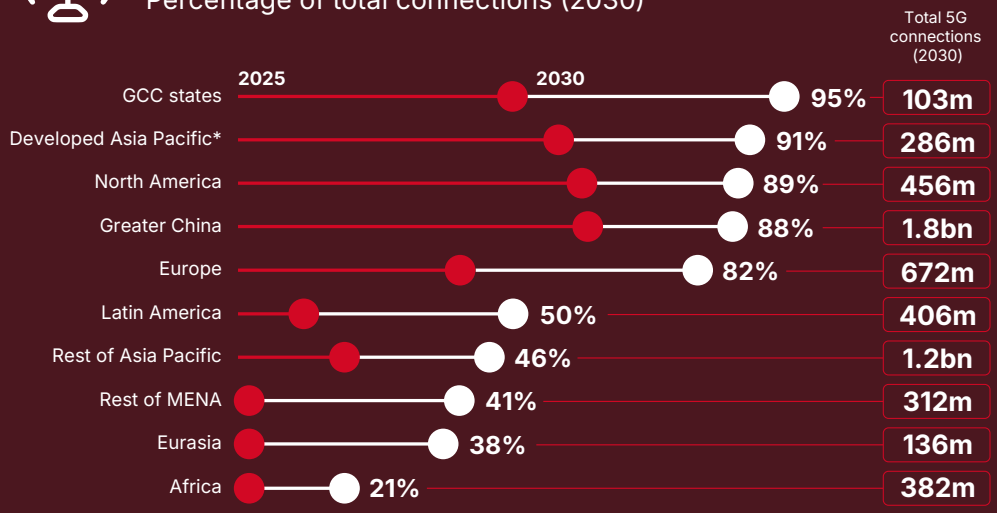
Coverage gap
4%

Usage gap
38%

Connected
58%

5G as a share of total connections

Percentage of total connections (2030)



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

2030

57%

of all mobile connections are forecast to be on 5G by 2030

while legacy 2G and 3G networks will fall to just 1% and 5% of connections respectively, marking a near-universal transition to advanced networks.

Operator revenues and investment

Revenues

2025 **$1.19tn**

2030 **$1.36tn**

Investment

Capex for the period 2025–2030

$1.2tn

Operator adoption of GSMA Open Gateway APIs

2025 **79 operators**

Representing

77% **of global mobile market share**

December 2025

01

The economic impact of the mobile industry

1.1
Macroeconomic outlook

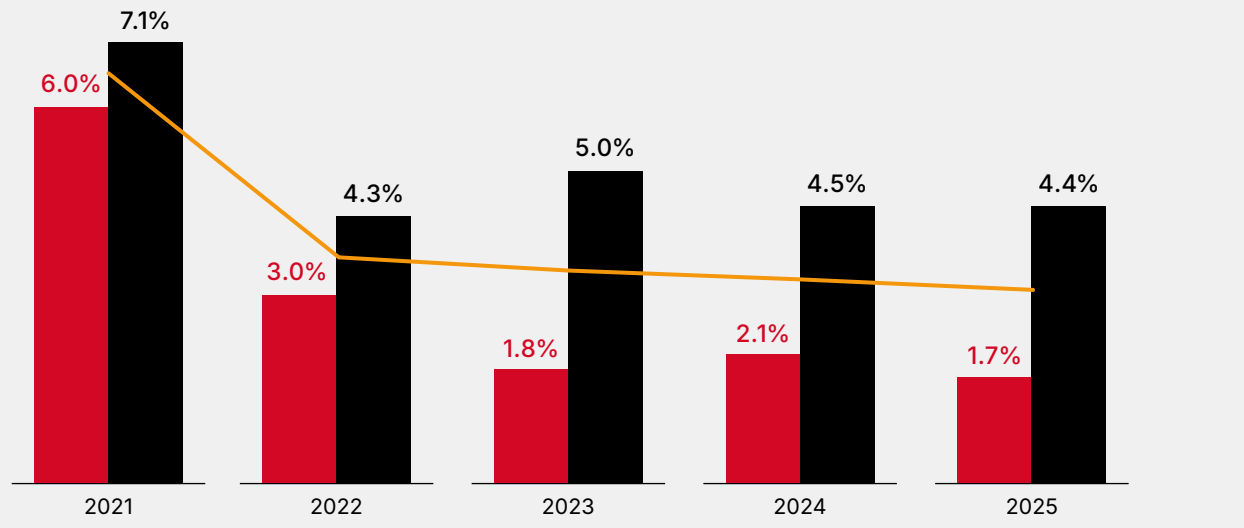
The global economy has sustained solid growth in recent years, with real GDP rising by 3.2% in 2025.[1] Despite risks early in 2025 from trade restrictions and tariff disruptions, businesses and economies have adapted. The primary engine of growth in 2025 was investment in AI, including for data centres, AI chips and the associated surge in energy demand. These investments have invigorated markets, particularly in advanced economies, with productivity gains expected to diffuse globally over time.[2]

However, there are risks to the outlook. A key concern is the potential overvaluation of the AI investment boom if spending fails to translate into productivity-enhancing products and profitable services. Additional vulnerabilities stem from mounting disruptions to global value chains, especially if geopolitical tensions escalate and further fragment trade flows.

Figure 1

Real GDP growth by income level, 2021–2025

Percentage of population



Source: GSMA Intelligence using WEO-IMF October 2025 data

1. In January 2026, the IMF updated the GDP growth in 2025 to 3.3%.
2. World Economic Outlook Update, IMF, January 2026

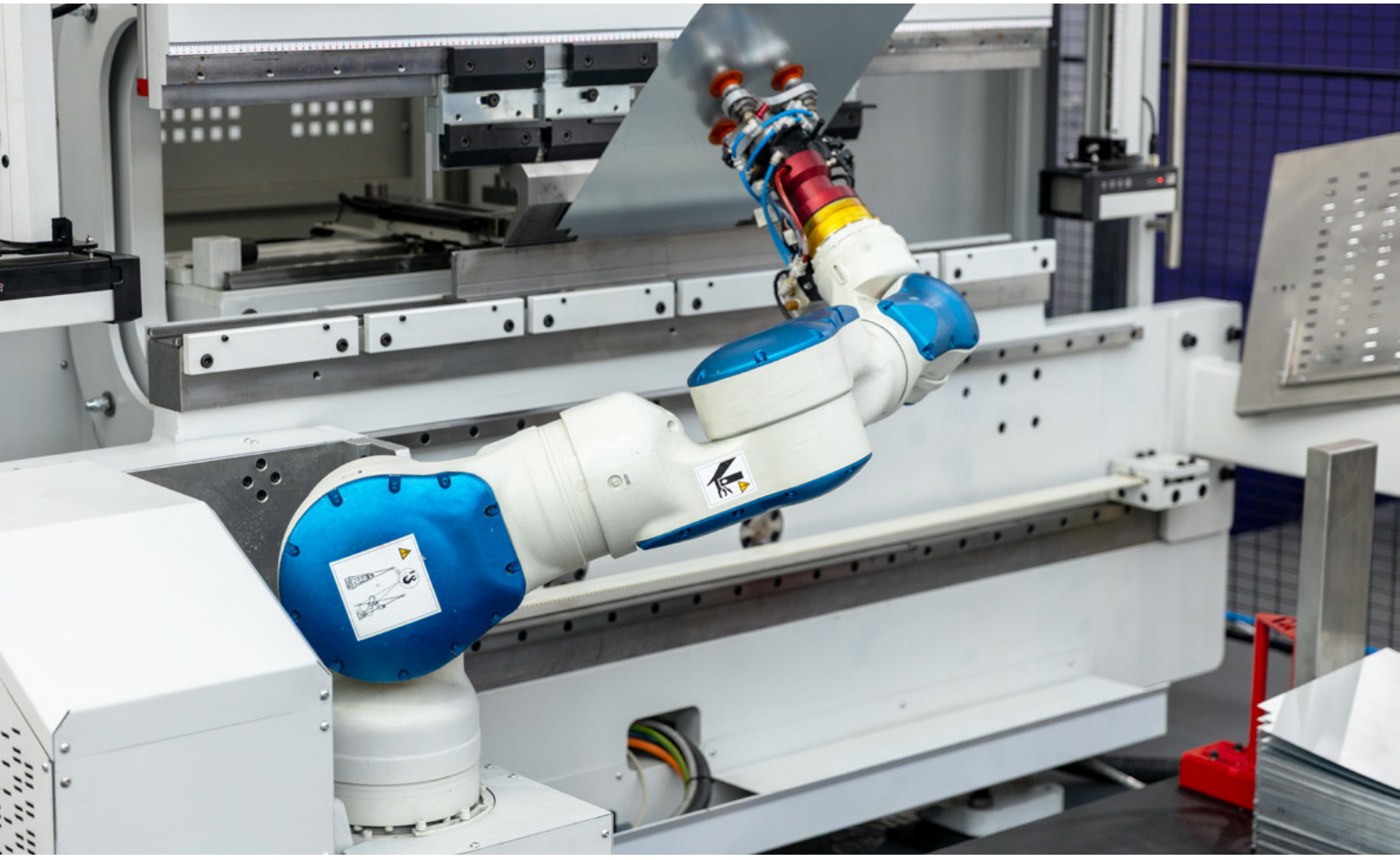
Technology investments underpin economic growth

Technology investment has become essential for sustaining long-term economic growth. For high-income countries (HICs), it offers a pathway out of the sluggish growth seen between 2022 and 2025 by enabling the creation of new products and services that raise living standards. For example, Microsoft, Alphabet, Amazon and Meta collectively increased their capex to more than $300 billion in 2025,[3] driven largely by investments in AI infrastructure and compute capacity. In parallel, the Stargate Project – led by OpenAI, Microsoft, Oracle and SoftBank – has committed up to $500 billion over four years to build advanced data centres across the US.[4]

For low- and middle-income countries (LMICs), which are expanding at faster rates, digital technologies provide an opportunity to accelerate development, improve quality of life and narrow the digital divide.

For example, in December 2025, Microsoft and Amazon pledged more than $50 billion to expand India's cloud and AI infrastructure, while Intel also announced plans to manufacture chips in India to tap into rising PC demand and rapid AI adoption. Separately, Google had already committed $15 billion to build new data-centre capacity for an AI hub in southern India.[5]

Within this context, the mobile sector can play a transformative role by delivering fast, reliable connectivity that underpins the development and deployment of emerging technologies and supports diversification across industries. Enhanced connectivity will boost efficiency and raise productivity for consumers and enterprises alike, enabling access to the latest wave of digital technologies, including 5G, IoT and AI, across all sectors of the economy.



3. "Inside the relentless race for AI capacity", Financial Times, July 2025
4. "Tech giants are putting $500bn into 'Stargate' to build up AI in US", BBC, January 2025
5. "Over $50 billion in under 24 hours: Why Big Tech is doubling down on investing in India", CNB, January 2026

1.2
Mobile's contribution to the economy

Mobile technologies contributed $7.6 trillion of economic value in 2025

In 2025, mobile technologies and services generated 6.4% of global GDP, a contribution that amounted to $7.6 trillion of economic value added. The greatest benefits came from productivity effects reaching $4.8 trillion, followed by the direct contribution of the mobile ecosystem generating almost $2 trillion.

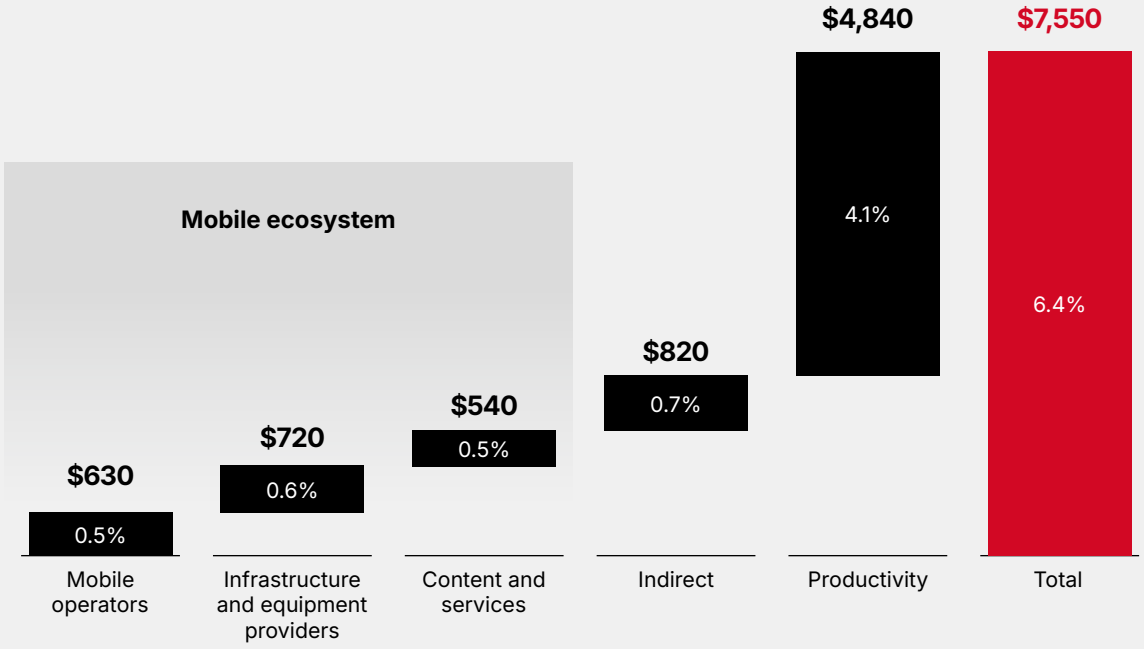
The impacts of mobile technologies include connectivity and digital transformation. Connectivity refers to the use of mobile technologies, while digital transformation involves the integration by enterprises of advanced mobile technologies such as 5G, IoT and AI.

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 encompasses content, mobile application and service providers, distributors and retailers, and mobile cloud services.

Figure 2

Total economic contribution of mobile technologies, 2025

Billion



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

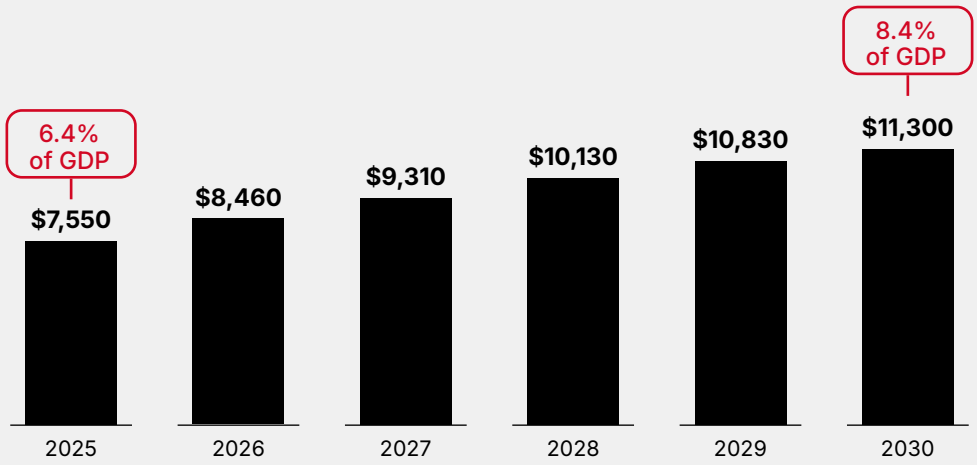
Mobile's economic contribution will exceed $11 trillion by 2030

By 2030, mobile's contribution to the global economy will reach $11.3 trillion, or 8.4% of GDP, driven by the improvements in productivity and efficiency brought about by the continued expansion of the mobile services and the growing adoption of digital technologies, including 5G, IoT and AI. Towards the end of the decade, mobile's contribution is expected to grow at a CAGR of 8.4%, three times the expected growth in global GDP for 2026–2030 (CAGR of 2.6%). This highlights the importance of mobile and digital technologies as key components in promoting innovation, shaping the future of the digital economy and serving as a means of development and progress for the least developed countries.

Figure 3

The economic impact of mobile through to 2030

Billion



Source: GSMA Intelligence

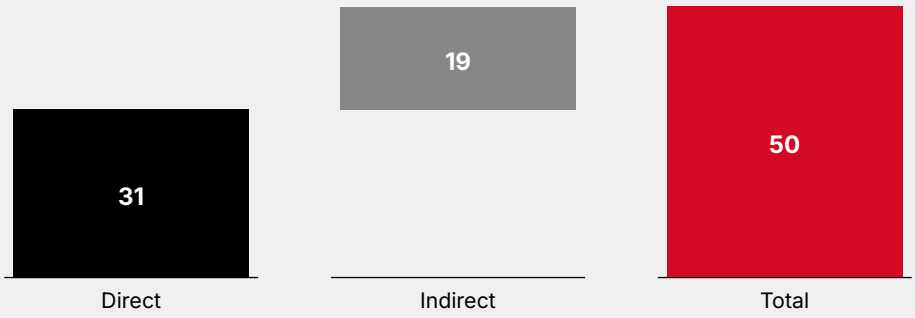
The global mobile ecosystem supported 50 million jobs in 2025

Mobile operators and the wider mobile ecosystem provided direct employment to 31 million people across the world. In addition, economic activity in the ecosystem generated around 19 million jobs in other sectors, meaning that 50 million jobs were directly or indirectly supported.

Figure 4

Employment impact of mobile, 2025

Jobs (million)



Source: GSMA Intelligence

The fiscal contribution of the mobile ecosystem reached $810 billion in 2025

Taxes constitute the major share of government revenues around the world. In 2025, global tax revenue reached $23 trillion, an increase of 2.3% compared to the previous year. The biggest contribution came from HICs at $17 trillion, representing 23% of their GDP, while LMICs contributed almost $6 trillion, representing 14% of their GDP.

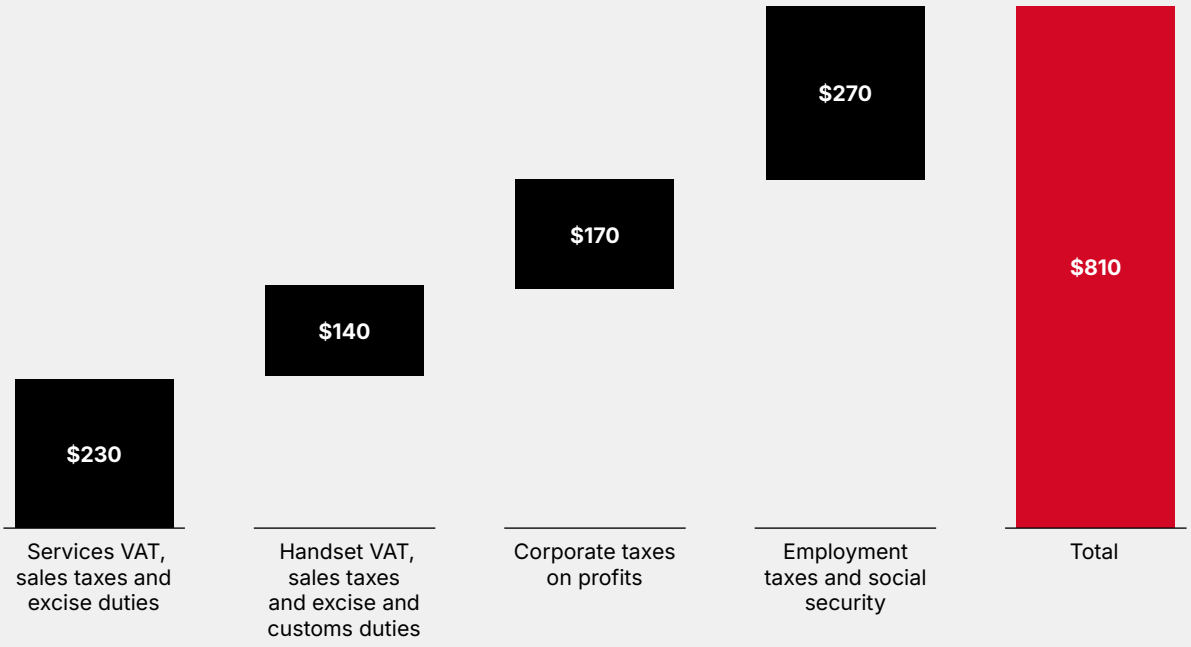
In 2025, the mobile sector made a substantial contribution to the funding of the public sector, with more than $800 billion raised through taxes on the sector. The largest contribution was from employment, taxes and social security ($270 billion). The fiscal contribution of the mobile ecosystem represented 3.5% of the total tax revenue.

Beyond its direct contribution, the mobile sector can enable a more efficient collection of tax revenue by enhancing tax processes across the economy. Digital payments represent one channel for achieving this. Another method involves leveraging mobile platforms for tax filing and payment. High compliance costs are a significant barrier discouraging individuals and small and medium-sized enterprises (SMEs) from paying taxes. In response, governments are rolling out mobile apps for filing and paying taxes to reduce friction and improve compliance rates.

Figure 5

Fiscal contribution of mobile, 2025

Billion



Source: GSMA Intelligence

The contribution of 5G and its ecosystem

The economic impact of mobile technologies will increasingly come from the pace and depth of technology adoption among consumers and enterprises. Countries equipped with advanced digital infrastructure, a highly skilled workforce and sustained investment in emerging technologies are positioned to benefit the most from 5G and AI. In contrast, developing regions are likely to experience more gradual but broad-based benefits as mobile technologies diffuse across their economies. Realising these gains, however, depends on complementary policy frameworks – particularly in spectrum allocation, taxation and service-quality regulation – that support ICT capital formation and enable firms to develop new digital products and services.

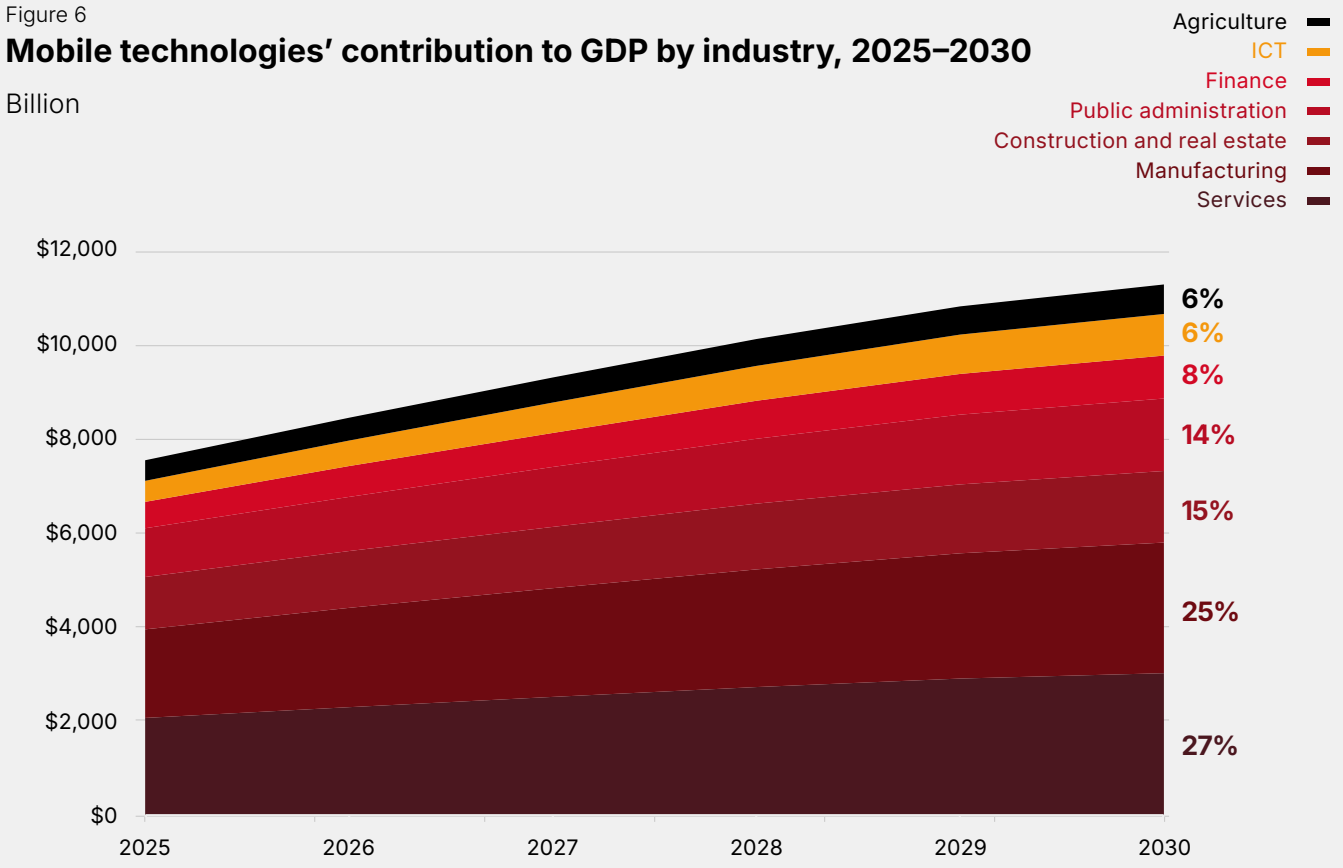
While mobile technologies will influence all sectors, the scale of impact will vary according to each industry's capacity to integrate 5G, IoT and AI into production processes. The economic value of digital transformation will arise from two primary channels:

- the creation of new revenue opportunities and business models that expand markets and generate additional demand (external value creation)
- the measurable improvements in productivity, cost efficiency and operational performance within firms (internal value enhancement).

Between 2025 and 2030, the services and manufacturing sectors are projected to account for roughly half of all growth attributable to mobile-enabled technologies, reflecting their relatively high readiness to absorb and deploy advanced digital tools.

Figure 6

Mobile technologies' contribution to GDP by industry, 2025–2030



Source: GSMA Intelligence

02

Trends shaping the mobile industry

2.1
Operators poised to capture new AI revenue opportunities

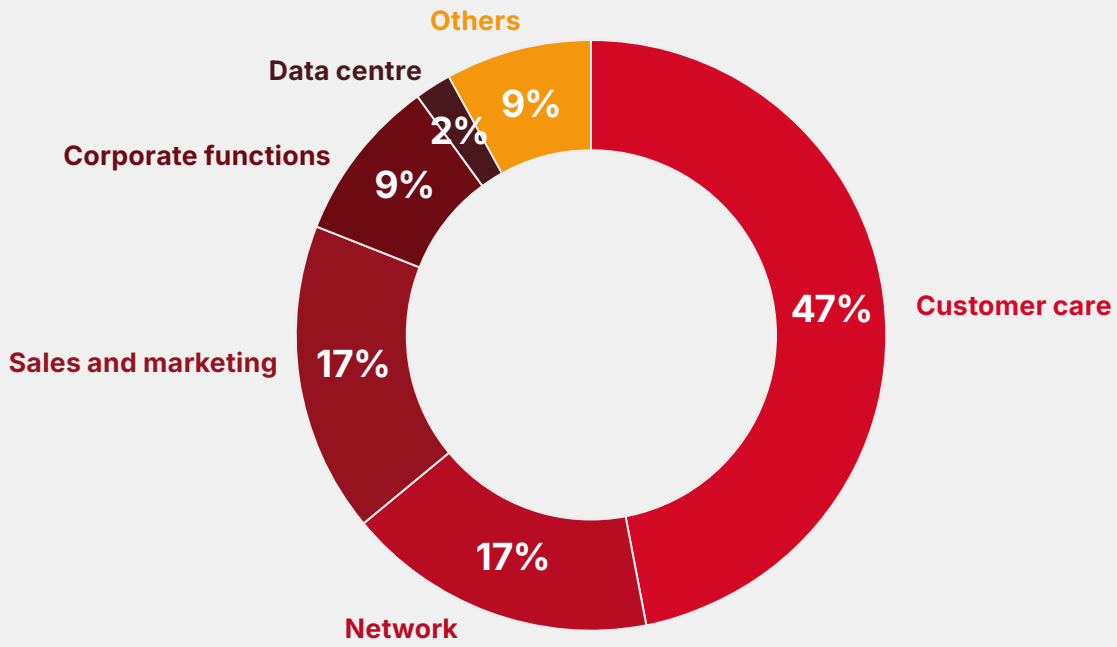
GSMA Intelligence research[6] shows that operator activity in AI continues to gravitate towards low-risk, easy wins, where functions can be automated through AI agent stacks. In 2025, customer care alone accounted for almost 50% of deployments, with AI for networks at just under 20%. Operator cost savings remain an imperative in a low-growth environment and amid continued pressure from data traffic and energy usage. AI deployments reflect this, with approximately 80% primarily targeting internal efficiencies.

However, operators are now looking to AI as a central pillar of revenue growth strategies as well. They are increasingly moving beyond just internal AI uses, such as predictive maintenance and chatbots, towards developing external AI opportunities – including partnerships with hyperscalers, cloud providers and data centre companies – to monetise AI capabilities.

Figure 7

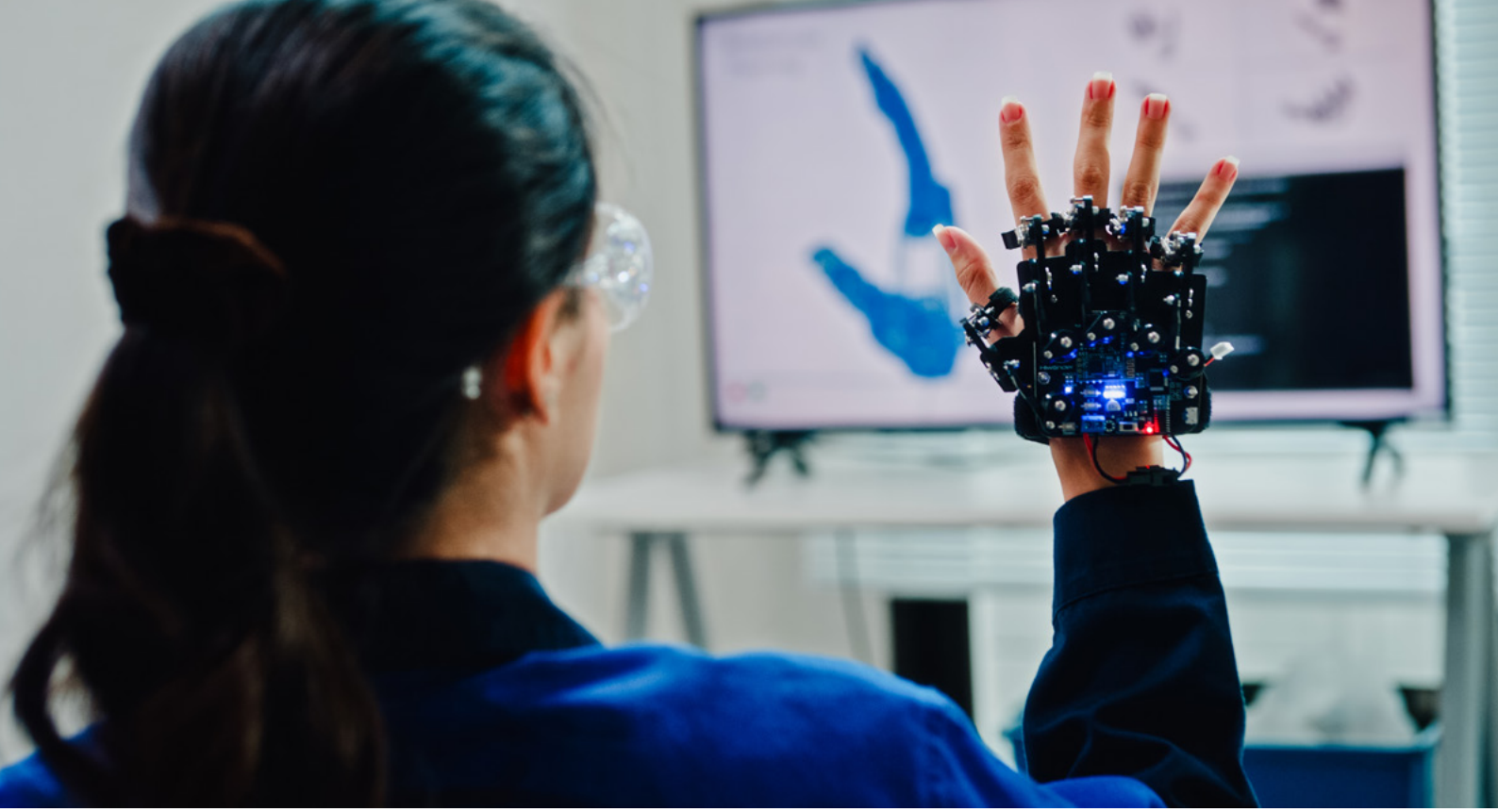
Telco AI adoption: prioritising easy wins while shifting towards revenue growth opportunities

Percentage of telco AI deployments



Source: GSMA Intelligence

6. Telco AI: State of the Market, Q3 2025, GSMA Intelligence, 2025



Emerging AI revenue models

Traditionally, telecoms operators have occupied the infrastructure layer of the digital value chain. More recently, there has been a structural shift upwards into high-value service domains, with the expansion of activity in GPU as a service (GPUaaS), AI platforms, IoT and cloud gaming. This vertical expansion reflects a strategic response to slowing connectivity revenues and the need to capture a greater share of emerging AI-driven value pools. However, this is also reshaping the competitive landscape. As operators enter domains historically dominated by hyperscalers and enterprise IT vendors, they face intensified competition, higher innovation requirements and greater execution risk.

The economics are also more complex: while AI-enabled services offer superior margin potential, they require significant investments in compute, software ecosystems and specialised talent.

AI monetisation can be viewed as a spectrum, extending from core and private clouds to enterprise and device-level edge deployments. Each position along this spectrum presents distinct trade-offs between capital intensity, revenue potential, latency performance and strategic considerations such as data sovereignty and compliance with sovereign AI requirements.

These dynamics are pushing the industry towards partnership-led models. Collaboration with hyperscalers, AI platform providers and IT vendors reduces time to market, mitigates capital risk and allows operators to differentiate through integration, localisation, data sovereignty and network-embedded capabilities, rather than attempting to compete directly with global cloud providers. Key emerging models are outlined in Table 1.

Table 1

Emerging AI revenue models for operators

Model	Description	Examples
AI connectivity provider	This involves leveraging high-capacity networks, edge infrastructure and data centres to deliver low-latency, secure and sovereign connectivity optimised for AI workloads. The revenue strategies centre on value-based models that go beyond traditional usage fees, such as network slicing for AI-specific performance, connectivity as a service (CaaS) and edge-based AI processing.	• Singtel's Paragon platform unifies private 5G, edge computing and service orchestration, using Nvidia's accelerated computing and AI enterprise stack to power AI- and graphics-intensive workloads. • Reliance Jio's enterprise connectivity portfolio (including multiprotocol label switching VPNs, SD-WAN and leased lines) underpins Reliance Industries and Meta's joint enterprise AI offering.
AI compute provider	This involves repurposing cloud and connectivity infrastructure to deliver GPU-powered compute, sovereign AI clouds and high-performance processing tailored to enterprise and industrial AI workloads. Revenue models include offerings such as GPUaaS, on-demand compute reservation, and subscription-based access to AI infrastructure.	• In November 2025, Deutsche Telekom launched the Industrial AI Cloud, a €1 billion AI-factory investment that delivers GPU-powered compute for industrial applications, large language model (LLM) development, digital twins and robotics. • In August 2025, SK Telecom launched its sovereign GPUaaS platform, Haein, which includes more than 1,000 Nvidia B200 GPUs, to provide enterprise and government customers with on-demand access to high-performance GPU capacity.
AI solutions partner	This involves collaborating with hyperscalers, AI platform providers and enterprise software vendors to co-develop, co-innovate and jointly deliver end-to-end AI solutions tailored to specific industries. Revenue models include joint go-to-market offerings, revenue-sharing on bundled services, consulting and integration fees, managed AI solutions and ecosystem-based marketplaces.	• KDDI provides infrastructure design, development, operations and maintenance, together with partners such as liret (an AWS Premier Tier Services Partner), to help local businesses adopt generative AI (genAI) products. • China Telecom's Xingchen LLM has been deployed across more than 50 industries, including government affairs, healthcare and education. • Reliance Jio offers JioBrain, a comprehensive AI platform that enables businesses to deploy genAI tools and advanced analytics. JioBrain helps enterprises to train and deploy custom LLMs with supporting models from OpenAI (GPT), Claude, Llama and others.

Source: GSMA Intelligence

2.2
Telco security: from network safety to strategic differentiation

The security threat landscape for telecoms operators is undergoing rapid structural change. Economic volatility, geopolitical tensions, accelerated digitisation, the rise of AI and the shift towards software-defined, cloud-native networks are collectively expanding both the scale and sophistication of cyber risks. More than 90% of operators now rate the threat level as high or very high – a view that has remained consistent over the past two years, underscoring the persistence and intensity of the challenge.[7]

As networks evolve into distributed, software-centric platforms deeply integrated with enterprise and consumer digital ecosystems, security and privacy have become core strategic imperatives. Telecoms infrastructure carries vast volumes of sensitive data and underpins national critical systems, making it an attractive target for state-aligned actors, cybercriminal groups and supply-chain attacks. Ensuring network integrity, maintaining service continuity and meeting increasingly stringent regulatory requirements are therefore essential not only for compliance but also for sustaining customer trust and long-term competitiveness.

Addressing this environment requires a holistic, multi-layered security strategy spanning prevention, detection and response. This includes advanced threat intelligence, automated monitoring, zero-trust architectures, resilient cloud and edge environments, and rapid incident-response capabilities. Equally important are skilled cybersecurity teams and mature organisational processes.

Strengthening defences through security best practices

Organisational cybersecurity can be understood through two complementary lenses. The first is prevention: identifying potential threats and deploying controls that minimise the likelihood of an incident occurring. The second is detection and response: acknowledging that no environment is fully secure and ensuring the capability to identify breaches quickly, contain their impact and restore services with minimal disruption.

Prevention

GSMA Intelligence survey data shows that operators have made significant progress on preventive measures. More than 90% report using multi-layered defence architectures, combining overlapping controls so that weaknesses in one layer can be offset by protections in another. Most operators have also invested in security awareness and training programmes, reflecting the persistent role of human error as a major source of cyber risk.

However, adoption gaps remain, particularly around next-generation prevention frameworks. The majority of operators have yet to implement zero-trust security models, highlighting the complexity, cost and architectural change required, especially for legacy systems not designed for continuous verification or granular access control. Despite these barriers, momentum behind zero trust is accelerating. Standards bodies such as the 3GPP and regulatory frameworks, including the EU's NIS2 Directive, increasingly recommend or require zero-trust principles, signalling their growing relevance in countering modern threat vectors and strengthening the resilience of telecoms networks.

7. Staying one step ahead: telco security in 2025, GSMA Intelligence 2025

Detection and response

Operator readiness for detection and response is comparatively stronger, but there is still significant variation. More than 80% of operators report having incident-response plans and procedures in place – an essential foundation for containing breaches and accelerating service restoration. However, these plans require continuous refinement to keep pace with evolving threat behaviours, new attack surfaces and the increasing complexity of cloud-native network environments.

Adoption of advanced detection techniques is still limited. Less than 40% of operators currently use threat-hunting practices, according to GSMA Intelligence survey data. Threat hunting plays a key role in uncovering stealthy or early-stage intrusions, such as reconnaissance activity or initial access attempts that traditional monitoring tools may miss, highlighting the need for operators to address this gap. Adoption is expected to increase as network equipment vendors and security providers embed threat-hunting capabilities more deeply into their platforms, lowering the operational barriers for telecoms operators and enabling more proactive security postures.

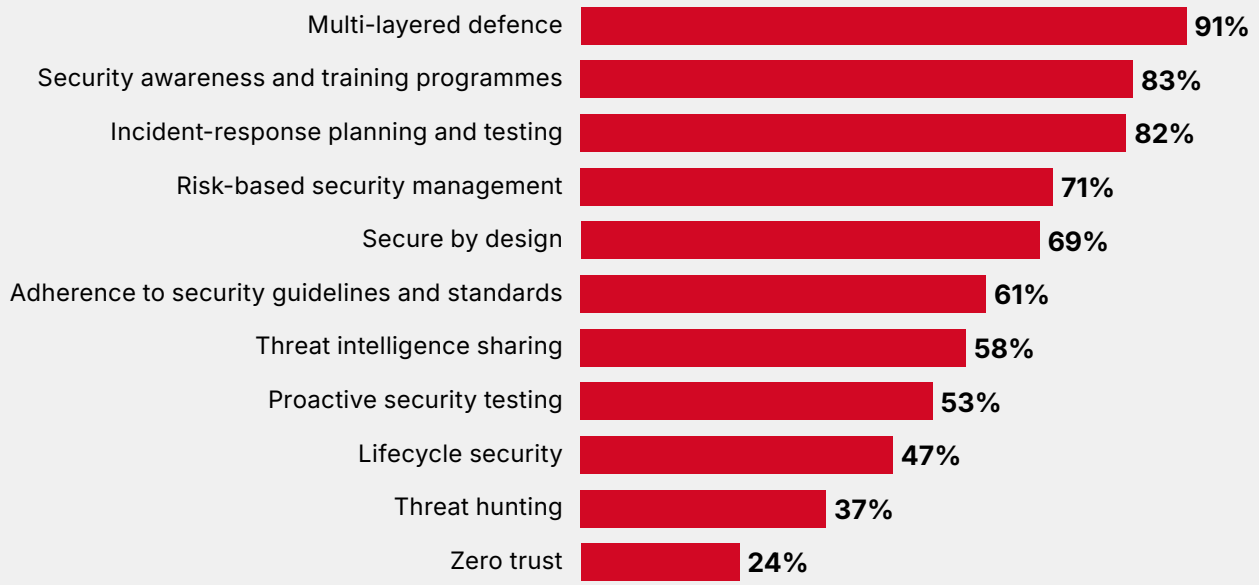
The skills imperative

Security challenges extend well beyond technology. Telecoms operators face a persistent shortage of specialised network-security talent, driven by the need to maintain ageing legacy systems while simultaneously building expertise in cloud-native, virtualised and AI-enabled environments. Closing this skills gap requires sustained investment in workforce development, including continuous training, upskilling and competitive compensation to attract and retain highly specialised professionals.

Figure 8

Security approaches among telecoms operators

Which of the following security approaches has your organisation adopted? (Percentage of operators)



Source: GSMA Intelligence Operators in Focus Security Survey July 2025

The impact of AI

AI and machine learning have long supported telecoms security, particularly in anomaly detection, fraud prevention and traffic analysis. But the emergence of genAI has materially expanded what can be automated. GenAI allows operators to process far larger and more complex datasets, correlate insights across multiple security domains and present findings through intuitive, text-based interfaces. This shifts security operations from manual, reactive investigation towards faster, more accurate and more proactive decision-making.

However, AI is a double-edged sword. The same capabilities that strengthen defence also enhance offensive techniques. Attackers can now automate reconnaissance, generate highly personalised phishing content and orchestrate more sophisticated, scalable attacks. This reinforces the need for operators to pair AI-driven security enhancements with robust governance, continuous monitoring and a skilled workforce capable of understanding and mitigating AI-enabled threats.

Security as a growth opportunity

Beyond risk mitigation, security is emerging as a significant commercial growth area for operators, particularly in the business-to-business (B2B) segment. GSMA Intelligence estimates that cybersecurity represents more than 20% of the global revenue opportunity in B2B technology services beyond core connectivity, making it one of the largest adjacent markets available to telecoms.

Operators hold strong competitive positions across key security domains, including network security, identity and access management, endpoint protection and managed security services. Their deep expertise in network monitoring and traffic analysis provides a structural advantage over traditional IT and cloud security providers, especially for enterprises seeking integrated, network-embedded security solutions. This positioning aligns with broader market trends, which include rapid enterprise IoT expansion, rising demand for sovereign cloud and edge services, and increasing regulatory scrutiny around data protection and critical-infrastructure resilience. By combining security with AI, IoT and 5G capabilities, operators can move beyond connectivity to become trusted partners in enterprise digital transformation, offering differentiated, high-value solutions that address both operational risk and strategic innovation needs.

2.3
Consumer experience underpins device innovation

Devices are no longer passive endpoints on a network, but are instead evolving into AI-native platforms that span smartphones, wearables, smart home systems and even automotive environments. As a result, consumer value is increasingly determined by how effectively a device anticipates user intent, adapts to real-world context and integrates into a broader, multi-device ecosystem – rather than by its standalone technical specifications. This transition signals a shift from hardware-centric innovation to experience-led value creation. Intelligence, contextual awareness and frictionless interoperability across devices now define competitive advantage.

AI at the centre of emerging device trends

AI has become the primary axis of device differentiation for consumers and suppliers, overtaking traditional hardware metrics such as display quality, memory capacity or processor speed. AI is now embedded across virtually every device category, enabling real-time personalisation, content generation and more intuitive user interaction. This includes on-device AI powered by neural processing units (NPUs), hybrid AI models that distribute workloads across cloud and edge infrastructure, and increasingly capable embedded AI assistants. Consumer device manufacturers now showcase AI-first smartphones, AI-enhanced TVs, next-generation wearables and automotive dashboards with integrated AI assistants, illustrating that AI has become a foundational design principle rather than an incremental feature.

Rising consumer adoption is reinforcing the strategic importance of AI integration. Findings from the GSMA Intelligence Global Consumer Survey indicate that AI capabilities now play a significant role in shaping purchasing decisions and upgrade cycles.[8] Consumers across North America, Europe and Asia Pacific show strong intent to adopt AI-enhanced features in both smartphones and smart home devices. This shift signals that AI is no longer viewed as experimental; it has become a baseline expectation for premium devices and is rapidly diffusing into mid-tier segments as well.

8. Consumers in Focus: Device User Behaviour Survey Dashboard 2026, GSMA Intelligence, 2026

At the ecosystem level, devices are increasingly functioning as AI hubs, coordinating seamless experiences across smartphones, wearables, PCs, smart home systems and vehicles. This trend is particularly pronounced in advanced markets, where mature device ecosystems and platform players are accelerating the shift towards multi-device intelligence. As AI capabilities become distributed across form factors, the device ecosystem is evolving into an interconnected network in which context, personal data and real-time inference flow fluidly, enabling more unified, personalised and persistent user experiences.

Meanwhile, safety, security and privacy are becoming core pillars of device innovation. AI-driven biometrics, scam detection, fraud prevention and personal-safety tools are now built directly into devices, especially smartphones. On-device AI plays a central role by keeping sensitive data local, strengthening privacy and supporting regulatory compliance while reducing dependence on cloud processing. On-device and hybrid architectures also deliver structural advantages such as lower latency, stronger privacy controls and more resilient user experience, which are especially important in regulated markets.

Table 2

Emerging trends in device innovation

Category	Description
AI in devices	AI is increasingly running on-device or through hybrid device–cloud models, enabling real-time, personalised experiences.
Silicon and chipset innovation	Smartphone chipsets now integrate NPUs and AI accelerators to run genAI efficiently on-device.
Safety and security	Devices now use AI for scam detection, biometrics, fraud prevention and personal-safety tools.
Privacy by design	On-device AI reduces cloud dependence, strengthening data privacy and regulatory compliance.
eSIM adoption and iSIM evolution	eSIM is now standard in premium devices, while iSIM is being built directly into chipsets for IoT and lower-cost segments.
Cross-device ecosystems	Devices increasingly serve as AI hubs linking phones, wearables, PCs, homes and vehicles.

Source: GSMA Intelligence based on company announcements

Innovation in wearables: smart glasses on the rise

Among wearables, smart glasses are emerging as a key area of innovation. Although consumer adoption remains relatively low, averaging around 2% across 12 major developed markets, momentum is clearly accelerating. As of early 2025, Meta and EssilorLuxottica had sold more than 2 million units of the second-generation Ray-Ban Meta smart glasses, launched in October 2023, with plans to scale up production to 10 million units annually by the end of 2026. Google, Snap and Apple are expected to introduce competing products in 2026. This renewed interest is being fuelled by advances in genAI, particularly multimodal capabilities that combine voice, vision and contextual awareness to deliver more intuitive, hands-free experiences.

For operators, increased adoption of smart glasses opens new commercial pathways. Higher data consumption and more uplink-intensive use cases create opportunities to upsell premium mobile plans or introduce tariffs that guarantee low latency and enhanced network performance. Bundling is another strong lever: the GSMA Intelligence Global Consumer Survey finds that 40% of mobile contract subscribers either already bundle wearables with their connectivity plans or are interested in doing so. As smart glasses move closer to the mainstream, operators are well positioned to expand wearables-based bundles and drive incremental average revenue per user (ARPU) through offerings that integrate devices and connectivity.

2.4
Growing eSIM momentum

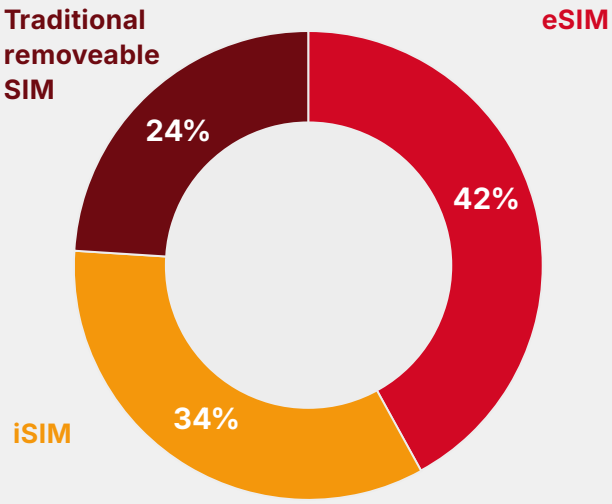
eSIM adoption is accelerating across both the consumer and enterprise segments, supported by rising awareness, improved user experience and broader ecosystem readiness. Once confined to premium smartphones, eSIM is now standard in mid-range devices, wearables and a growing range of connected products, which is streamlining activation and reducing reliance on physical SIM cards. Demand is being reinforced by the convenience of digital onboarding, easier switching between operators and plans, and the ability to manage multiple profiles on a single device. For frequent travellers, eSIM delivers clear value by enabling seamless access to local data plans without the friction of swapping SIMs.

Wearables and secondary devices are further normalising eSIM usage. Smartwatches, tablets and emerging categories such as smart glasses increasingly depend on eSIM for standalone connectivity, strengthening multi-device ecosystems. As consumers grow more comfortable managing connectivity digitally, eSIM is becoming a foundational element of the connected-device experience.

Figure 9

Cellular IoT: projected market share of SIM technologies in 2030

Aggregate figures across 21 countries surveyed



Source: GSMA Intelligence

Enabling LPWAN deployments

Beyond consumer use cases, eSIM is poised to become a foundational enabler of large-scale IoT deployments, particularly those built on low-power wide-area networks (LPWAN). By digitising provisioning and connectivity management, eSIM significantly simplifies the operational complexity of deploying and scaling up IoT devices across diverse regulatory environments and network conditions.

In LPWAN-based applications – such as smart metering, asset tracking, industrial monitoring and smart city infrastructure – eSIM supports remote provisioning, lifecycle management and seamless profile switching. This reduces the need for physical maintenance after installation, which is a critical advantage for long-life, energy-efficient devices deployed in remote, hard-to-reach or cross-border locations.

As regulatory frameworks mature and eSIM standards evolve, adoption is expected to accelerate across both the consumer and enterprise IoT segments. The shift towards iSIM, which embeds SIM functionality directly into the chipset, will further reduce costs, power consumption and device footprint. This makes iSIM particularly attractive for high-volume, cost-sensitive IoT deployments, including those in emerging markets.

Strategic opportunities for ecosystem players

As connectivity becomes increasingly embedded into multi-device experiences, eSIM provides the architectural flexibility required to support diverse markets and regulatory environments. For operators, eSIM delivers clear operational and commercial advantages. It reduces the distribution and logistics costs associated with physical SIM cards and supports fully digital onboarding, lowering acquisition friction and improving conversion.

Beyond improving customer experience and reducing operational friction, eSIM unlocks direct monetisation opportunities in areas such as anti-theft services, roaming optimisation and asset and logistics tracking, reinforcing its role as a catalyst for new business models across the connectivity value chain. eSIM also enables new revenue opportunities in wearables and IoT, where flexible, software-based provisioning is essential for scalable connectivity models. For device makers and ecosystem partners, eSIM accelerates the shift towards software-defined connectivity. This supports faster product launches, simplifies global expansion and enables deeper integration between devices, networks and digital services.

Recent eSIM developments bolster the outlook for adoption

GSMA Intelligence forecasts that eSIM-enabled smartphone connections will reach 2.5 billion globally by 2028, with eSIM representing 42% of all SIM technologies by 2030, reflecting its rising strategic importance. This growth trajectory is being reinforced by several recent developments across the connectivity and devices ecosystem:

- In October 2025, China's three leading operators – China Telecom, China Mobile and China Unicom – launched trials for eSIM smartphone services, after receiving regulatory approval from the Ministry of Industry and Information Technology. With this development, eSIM is now accessible for smartphones nationwide.
- In October 2025, Oppo launched its first eSIM-enabled smartphone flagship line-up, the Find X9 series, following the approval of nationwide eSIM trials in China.
- In October 2025, AT&T and Thales introduced a standardised eSIM solution based on the SGP.32 specification, marking a significant step towards scalable IoT connectivity. The new framework enables enterprises to manage millions of devices through a centralised server, eliminating the need for individual devices to initiate manual profile 'pulls'.
- In September 2025, Apple introduced the iPhone 17 Air as its first globally released model without a physical SIM tray. While the iPhone 14 pioneered eSIM-only designs in the US in 2022, the iPhone 17 series marks a broader strategic shift, extending eSIM-only, tray-less devices to multiple international markets and signalling Apple's long-term commitment to a fully digital connectivity model.
- In August 2025, Google introduced the US models of the Pixel 10, Pixel 10 Pro and Pixel 10 Pro XL as eSIM-only devices, removing the physical SIM tray entirely.
- In March 2025, Giesecke+Devrient (G+D) partnered with AWS to shift eSIM management to a fully cloud native model, enabling more flexible, scalable and globally consistent deployments for operators and enterprises.

2.5
Digital transformation across vertical sectors gathers pace

Digital transformation within vertical industries has shifted decisively from isolated pilots and incremental upgrades to a core strategic priority. This transition reflects both technological maturation and growing pressure on organisations to redesign operations for measurable business outcomes. While digital transformation continues to mostly be driven by large enterprises in financial services, manufacturing, automotive, retail and healthcare, SMEs are increasingly investing as well, supported by modular, scalable solutions that enable phased and cost-aligned deployment.

Findings from the GSMA Intelligence 2025 Enterprise Survey,[9] which gathered responses from 5,320 organisations across 32 countries and 10 sectors, underscore the scale of this shift. Enterprises expect to allocate around 10% of revenues to digital transformation initiatives between 2025 and 2030, with anticipated returns of approximately 200% over the same period. This signals a clear expectation that digital transformation is not merely a cost centre but a driver of long-term value creation.

Security emerges as the dominant strategic imperative across industries, with organisations prioritising enhanced protection against increasingly sophisticated cyberthreats. Revenue-driven objectives, such as improving customer experience and strengthening competitive differentiation, rank closely behind. Cost-related motivations, including improved agility, operational efficiency and regulatory compliance, also play a significant role, alongside growing pressure to meet sustainability commitments.

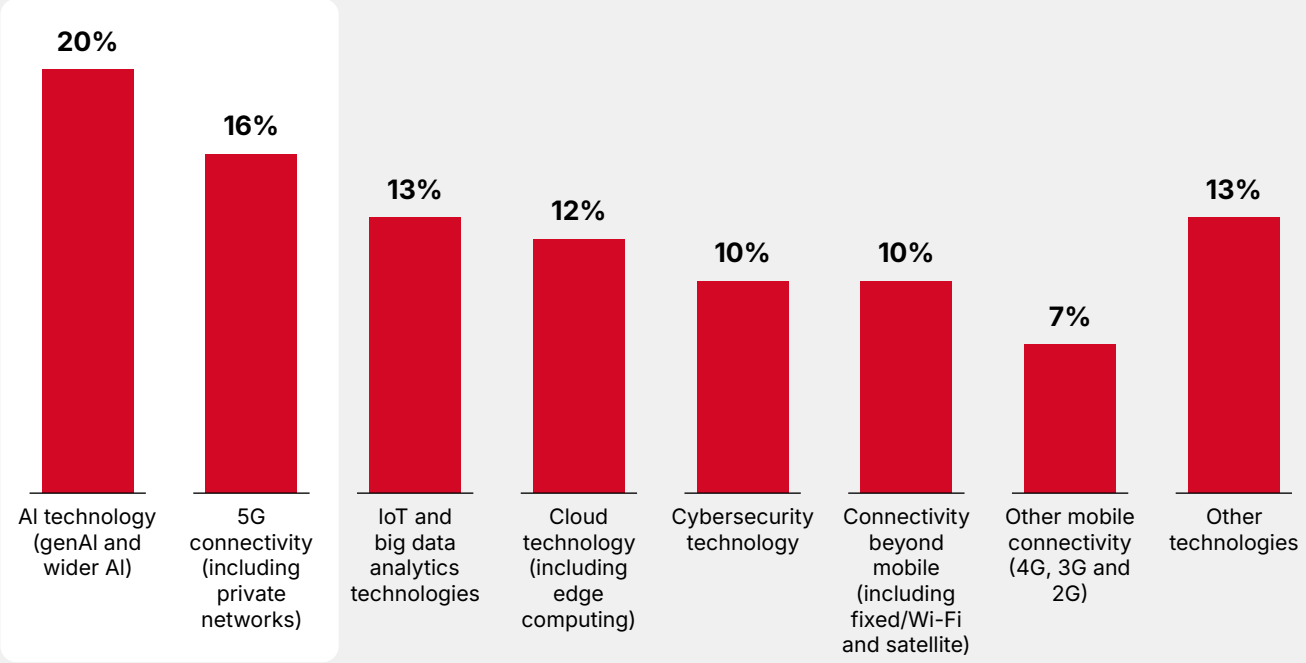
On the technology front, AI, particularly agentic AI and genAI, sits at the core of digital transformation strategies, with AI enabling autonomous decision-making, predictive insights and real-time optimisation. Advanced connectivity, including 5G and fibre, provides the foundation for large-scale IoT deployments and supports distributed AI inference at the edge. Cloud platforms continue to deliver the scalable, flexible compute environments required for these workloads, while next-generation cybersecurity solutions safeguard increasingly digital operations. Across all technologies, AI and 5G are expected to remain the primary investment priorities for enterprises through to 2030, reflecting their role as critical enablers of cross-sector digitalisation.

9. Digital transformation of vertical sectors: the new wave of B2B opportunities revealed by the 2025 global enterprise survey, GSMA Intelligence, 2025

Figure 10

Share of total digital transformation expenditure by technology, 2025–2030

Aggregate figures across all countries and vertical sectors surveyed



Source: GSMA Intelligence Enterprise in Focus: Global Digital Transformation Survey 2025

Recent examples of digital transformation initiatives by major enterprises include the following:

- PepsiCo's partnership with Siemens illustrates how manufacturers are moving beyond isolated automation projects towards full-scale operational digitalisation. By creating high-fidelity 3D digital twins of selected US plants and warehouses, the company can simulate end-to-end production and supply-chain flows, establish performance baselines and identify optimisation opportunities before making physical changes.
- Amazon deployed its millionth robot in mid-2025, demonstrating the accelerating industrialisation of robotics on a global scale. The introduction of DeepFleet, a genAI model that orchestrates robotic movement across fulfilment centres, emphasises a shift towards AI-driven logistics systems capable of continuous, autonomous optimisation.
- BMW uses self-driving, cloud-controlled vehicles to move newly assembled cars to loading areas, which reflects the growing integration of autonomous mobility into core industrial workflows. Automating this 0.6 mile transportation step removes the need for human drivers and reduces operational bottlenecks.

Emerging opportunities for operators

The accelerating pace of enterprise digital transformation is expanding the B2B opportunity landscape for all technology suppliers, with telecoms operators particularly well positioned to benefit. Operators already provide the foundational layer of modern digital ecosystems: high-performance 5G and fibre networks, secure connectivity and critical infrastructure. However, the shift towards AI-driven operations, pervasive IoT, real-time data processing and automation is enabling operators to evolve from traditional connectivity providers into fully fledged tech-cos that integrate networks with cloud, edge computing, AI and cybersecurity capabilities.

Although hyperscalers and specialist enterprise software vendors continue to dominate many digital transformation programmes due to their global scale and broad service portfolios, operators have a meaningful opportunity to capture greater value in these digital transformation initiatives. Their strengths in orchestrating complex connectivity environments, managing mission-critical infrastructure and delivering secure, compliant solutions allows them to potentially move higher up the enterprise value chain. This requires a shift from selling bandwidth to delivering integrated, outcome-oriented services.

Operators can pursue this transition through several strategies, including specialising in selected high-value technologies, such as private 5G, edge computing or cybersecurity, and adopting a cross-service model that positions the operator as a technology orchestrator. In most cases, partnerships with equipment vendors, hyperscalers and enterprise technology firms are vital, as they enable operators to offer more comprehensive, vertically relevant solutions that enterprises increasingly require. Recent developments highlight that operators are beginning to reposition themselves as strategic partners in enterprise digital transformation:

- **Telefónica Tech** has launched a managed security service edge solution for customers in the UK and Ireland, built on Netskope technology. The offering targets enterprises with cloud-native or hybrid IT environments, allowing employees to securely access applications and data from any location while reducing risk, cost and architectural complexity.
- **Vodafone Business** has announced a four-year partnership with Centrica to modernise its IT and connectivity estate and introduce new bundled services for UK customers. Working with VOIS and CGI, Vodafone will deliver workplace services and connectivity across 80 sites and approximately 30,000 devices, supporting Centrica's transition to a data-driven enterprise using genAI and machine learning to enhance productivity and personalise employee and customer experiences.

> **The shift towards AI-driven operations, pervasive IoT, real-time data processing and automation is enabling operators to evolve from traditional connectivity providers into fully fledged tech-cos**

03

Mobile industry impact

The mobile industry has become a central force in advancing global digital inclusion, moving far beyond basic connectivity to enable meaningful participation in the digital economy. By expanding access to affordable networks, devices and scalable digital services, mobile operators and ecosystem partners are helping to close long-standing gaps in access to public services, particularly for marginalised populations. As essential services become increasingly digitised, mobile technology acts as both an economic catalyst and a platform for social development, allowing governments and organisations to deliver services more efficiently and inclusively.

At the same time, the mobile industry is emerging as a key enabler of sustainability and resilience across sectors. Connectivity and data-driven solutions support more efficient industrial processes, smarter resource management and reduced environmental impact, allowing other industries to lower their carbon footprints at scale. The sector also plays a critical role in disaster preparedness and response, providing resilient communication networks that support early-warning systems, real-time information flows and coordinated humanitarian operations. Through these capabilities, the mobile industry serves as a foundational pillar for both sustainable development and crisis resilience in an increasingly digital world.

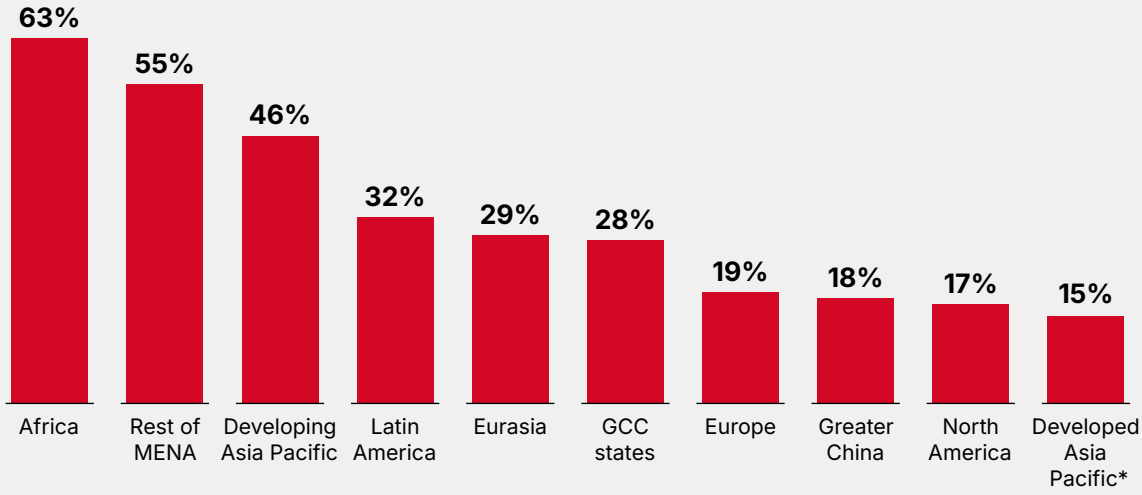
3.1 Enhancing digital inclusion

Mobile internet adoption continues to expand at a record pace, with 58% of the global population, equivalent to 4.7 billion people, now accessing the internet through their own mobile devices. In 2024 alone, around 200 million individuals came online via mobile for the first time, marking the fastest annual growth since 2021. However, more than 3 billion people, representing just under 40% of the world's population, remain unconnected, despite the fact that 96% of the global population now resides within areas served by mobile broadband networks. Furthermore, 9% of the world's population (710 million individuals) used mobile internet in 2024 but not on a device that they own or have primary use of. While the coverage gap[10] has continued to close, progress towards closing the usage gap[11] is stalling, indicating a need to shift the focus, from expanding broadband infrastructure coverage to addressing inequalities in how people access and use mobile internet.

Progress in closing the usage gap remains slow due to persistent demand-side barriers. Many people are still unaware of mobile internet, while others who are aware cannot afford a smartphone or lack the digital skills needed to use online services confidently. Even among current users, concerns about safety, inconsistent service quality and limited relevant content continue to constrain deeper engagement.

Figure 11

The usage gap as a percentage of total population by region



* Includes Australia, Japan, New Zealand, Singapore and South Korea
Source: GSMA Intelligence

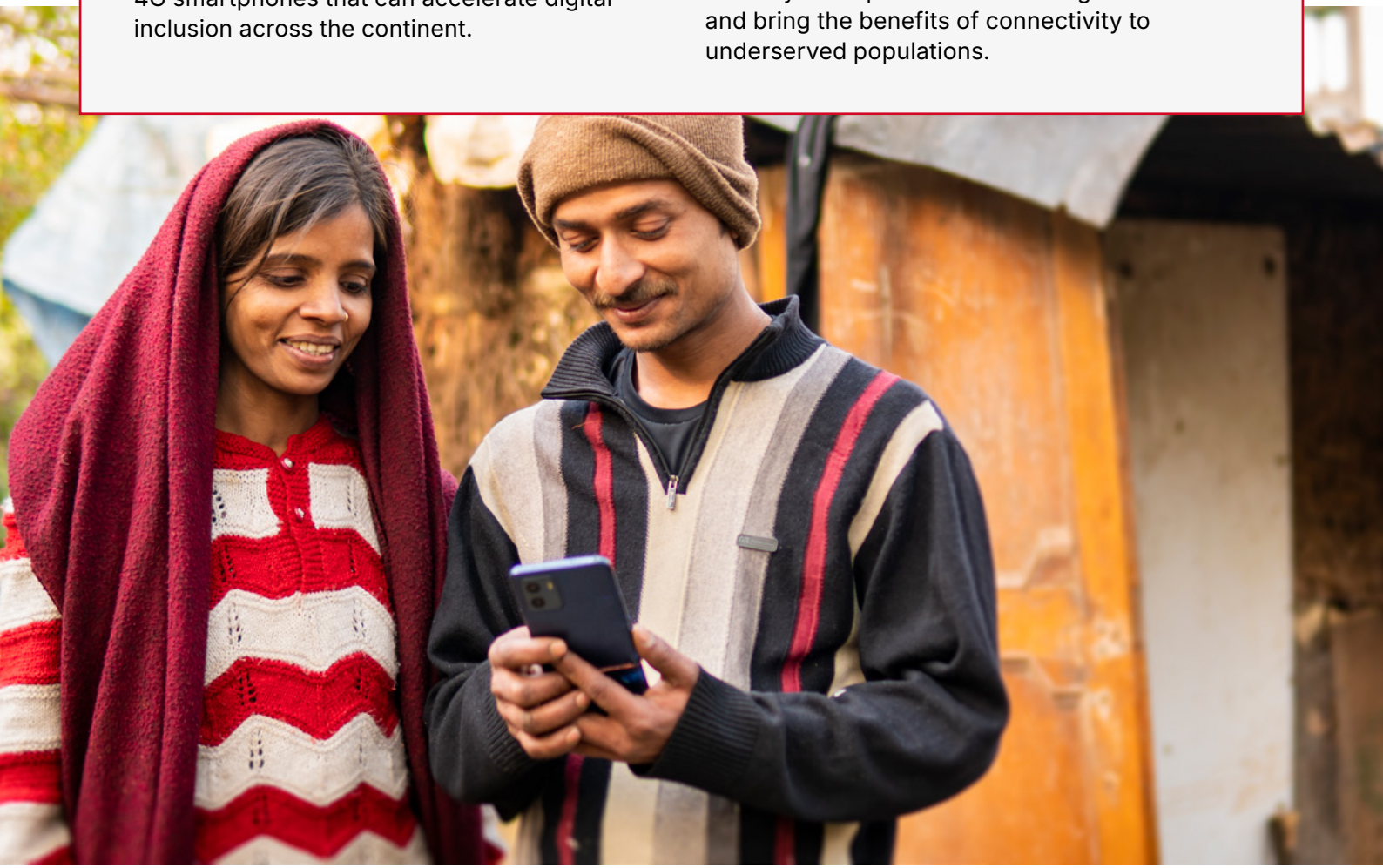
10. People who live in areas without mobile broadband coverage.
11. People who live in areas covered by mobile broadband but do not use it.

The challenge is especially acute in Africa, which accounts for 33% of the world's unconnected population and has the lowest smartphone ownership globally – just 24% of the population in 2024. A GSMA Intelligence study[12] found that affordability is the main reason for the comparatively low level of smartphone adoption; in Sub-Saharan Africa, for example, the cost of a smartphone as a proportion of monthly GDP per capita was 26% in 2024, compared to an average of 16% across LMICs.

Mobile industry efforts to improve smartphone affordability

In October 2025, the GSMA, working with six major African operators – Airtel, Axian Telecom, Ethio Telecom, MTN, Orange and Vodacom – introduced a set of minimum specifications for affordable entry-level 4G smartphones. By defining requirements for memory, RAM, camera quality, display size, battery performance and other essential features, the initiative aims to standardise expectations for low-cost devices while ensuring reliability and durability. The GSMA is now engaging with OEMs and technology partners to build consensus around these specifications, with the goal of enabling large-scale production of affordable 4G smartphones that can accelerate digital inclusion across the continent.

This effort builds on the GSMA Handset Affordability Coalition, a broader global coalition launched in 2024 to expand access to affordable smartphones in LMICs. By September 2025, the coalition had grown to 25 members, spanning mobile operators, device manufacturers, ecosystem players, financing institutions, international organisations and philanthropic foundations. The partnership focuses on addressing three structural barriers to affordability: reducing taxation on entry-level devices; reshaping cost structures to enable ultra-low-cost smartphone production at scale; and advancing innovative de-risking and financing models that make devices more accessible to underserved populations. Together, this reflects a coordinated industry-wide push to enhance digital inclusion and bring the benefits of connectivity to underserved populations.



12. Accelerating Smartphone Adoption in Africa, GSMA, 2026

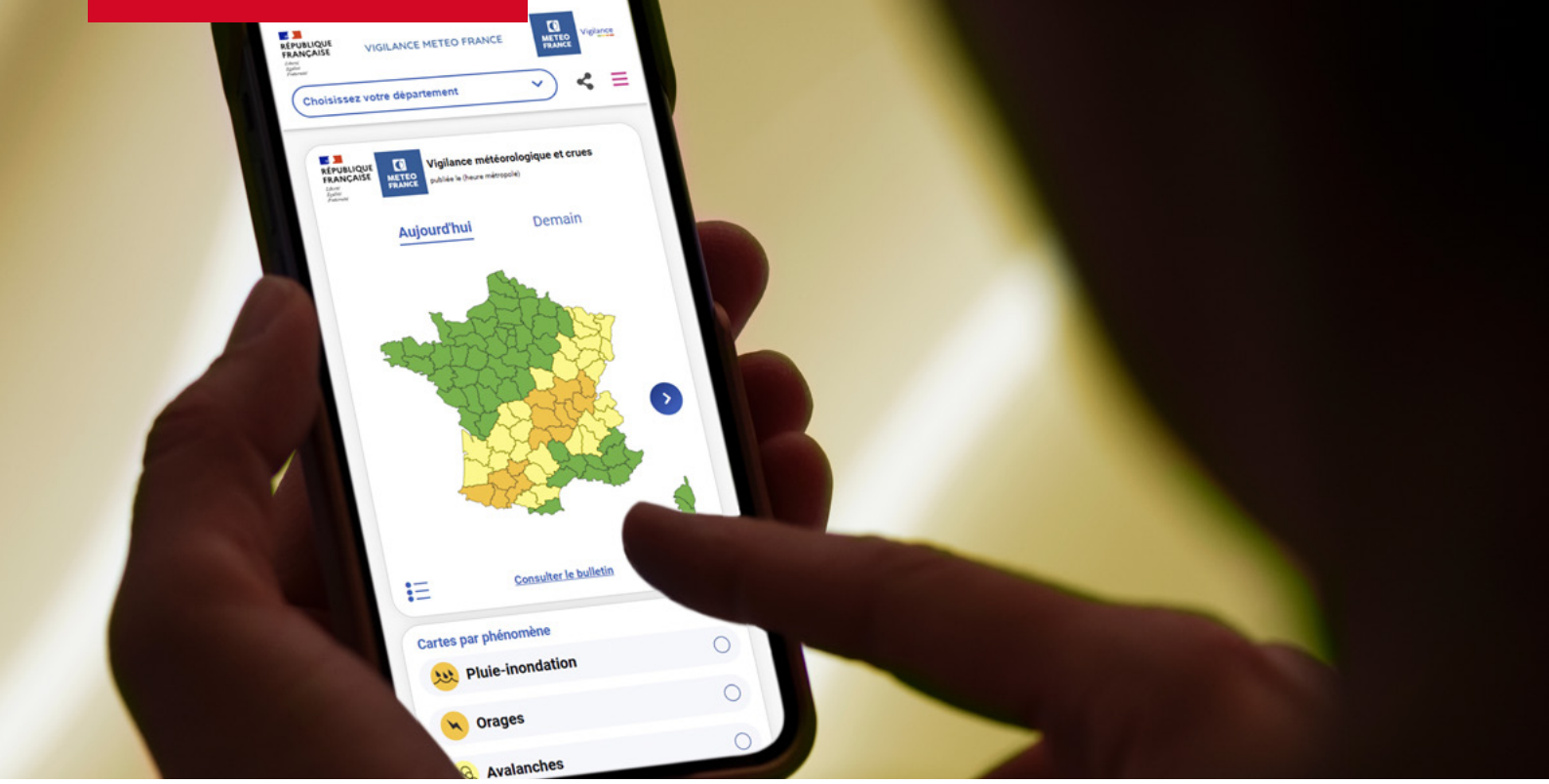
3.2
Enabling the shift to sustainability in vertical sectors

Mobile operators are becoming central to helping other industries transition to more sustainable operations and meet net-zero goals. As AI adoption and compute demand rise across cloud and edge environments, operators face increasing energy pressures while also shaping the carbon footprint of the broader digital economy through their networks, data centres and edge platforms.

In response, operators are making their own infrastructure more sustainable, with renewable energy and AI-driven efficiency, while also enabling enterprises to use compute more sustainably. By lowering the carbon intensity of connectivity and supporting smarter digital operations, operators are helping industries decarbonise at scale, such as in the following examples:

- **e&**, working with Ericsson, has developed smart sites that combine AI-powered energy-saving software with zero-footprint site designs to cut the energy intensity of network infrastructure. Originally deployed across e&'s own footprint, these high-efficiency site architectures are now being offered as templates for enterprise private networks. By applying AI-driven optimisation and low-impact site engineering, the solutions enable enterprises to reduce local network energy consumption by up to 52%, providing a scalable pathway to lower-carbon digital infrastructure.[13]
- **Deutsche Telekom** is pursuing a similarly ambitious approach, anchored in its 2025 net-zero Scope 1 and 2 commitments. The company has operated all data centres on 100% renewable electricity since 2021 and has developed AI-optimised, industrial-grade facilities that achieve a 1.3 power usage effectiveness (PUE) while consuming 30% less energy than comparable sites.[14] This supply-side efficiency strategy significantly reduces the carbon intensity of compute operations and positions Deutsche Telekom as a leader in sustainable digital infrastructure.
- **KDDI's** Green Mobile initiative provides corporate customers with mobile services powered entirely by renewable energy. By embedding clean energy sourcing directly into mobile subscriptions, the offering enables enterprises to reduce Scope 3 emissions associated with their communications footprint, an area that is typically difficult to influence. This positions KDDI not only as a low carbon operator but also as an active enabler of value chain decarbonisation for its business customers.
- **Singtel's** Paragon uses AI-driven orchestration to enable carbon-aware cloud routing and emissions-optimised workload placement, shifting workloads to regions with lower grid carbon intensity and scheduling non-urgent tasks during periods of higher renewable energy supply. By optimising both the location and timing of compute while maintaining performance and service-level-agreement requirements, Paragon lowers the carbon intensity of AI and cloud workloads and helps enterprises improve sustainability without compromising operational quality.
- **SK Telecom** is rapidly scaling up its green AI data-centre footprint across South Korea and Southeast Asia, partnering with AWS, Nvidia and SK Innovation to build high-efficiency compute infrastructure. The expansion of the Ulsan AI data centre to 1 GW, combined with energy-specialised measures such as liquefied natural gas–based power systems and advanced cooling technologies, reflects a strategic push to create resilient, low-carbon AI hubs capable of supporting increasingly intensive AI workloads.[15]

13. e& and Ericsson: Collaborative journey towards Net Zero, Ericsson, 2025
14. We Walk the Talk, T-Systems, 2025
15. "SK Telecom Accelerates Expansion of Its AI Data Center Initiative", SK Telecom, November 2025



3.3 Supporting disaster response and rescue efforts

Globally, extreme weather events are becoming more frequent, intense and destructive, with the World Meteorological Organization documenting clear increases in heat extremes, heavy rainfall and the associated socioeconomic impacts. The consequences were stark in 2025. Aon estimated that global insured losses from natural catastrophes in 2025 reached approximately $120–127 billion, marking the sixth consecutive year of losses exceeding the $100 billion threshold.[16] Against this backdrop, the effectiveness of disaster response increasingly hinges on timely warnings, real-time coordination and rapid restoration of essential services.

Communications networks form the backbone of these capabilities, enabling alert dissemination, situational awareness, responder coordination and public access to critical information. In 2025, operators expanded their resilience strategies through deployable infrastructure, satellite-enabled back-up connectivity, priority-access mechanisms and integrated coordination platforms. Satellite communications has also become a central pillar of emergency preparedness and response, providing continuity when terrestrial networks are damaged or overloaded.

For example, Vodafone, in partnership with AST SpaceMobile, is developing satellite-enabled operational capabilities to maintain emergency connectivity when terrestrial networks fail, strengthening continuity during large-scale disruptions. Similarly, Orange is integrating Eutelsat OneWeb's satellite links into its SafetyCase units, providing resilient back-up channels for alerts and coordination in disaster situations. In Japan, the major operators – NTT Group, KDDI, SoftBank and Rakuten Mobile – jointly launched a nationwide disaster-information-sharing platform in July 2025, creating a unified mechanism for real-time coordination, accelerated network restoration and prioritised communications during large-scale emergencies. These developments strengthen disaster resilience by ensuring faster situational awareness, more efficient resource deployment and more reliable connectivity when it matters most.

16. "'Quiet' catastrophe year still delivers sixth straight $100bn-plus loss total: Aon", Insurance Business, January 2026

Operators support disaster response and recovery during the 2025 Los Angeles wildfires

In January 2025, fast-moving wildfires swept through parts of the Los Angeles metropolitan area, triggering mass evacuations and causing extensive damage to homes, transport corridors and power infrastructure. Prolonged outages and hazardous conditions disrupted essential services, placing a heavy strain on emergency coordination and public communications at the height of the crisis. AT&T, T-Mobile US and Verizon bolstered disaster response by reinforcing network resilience, deploying emergency assets and providing customer relief during the crisis.

Critical infrastructure and satellite deployment

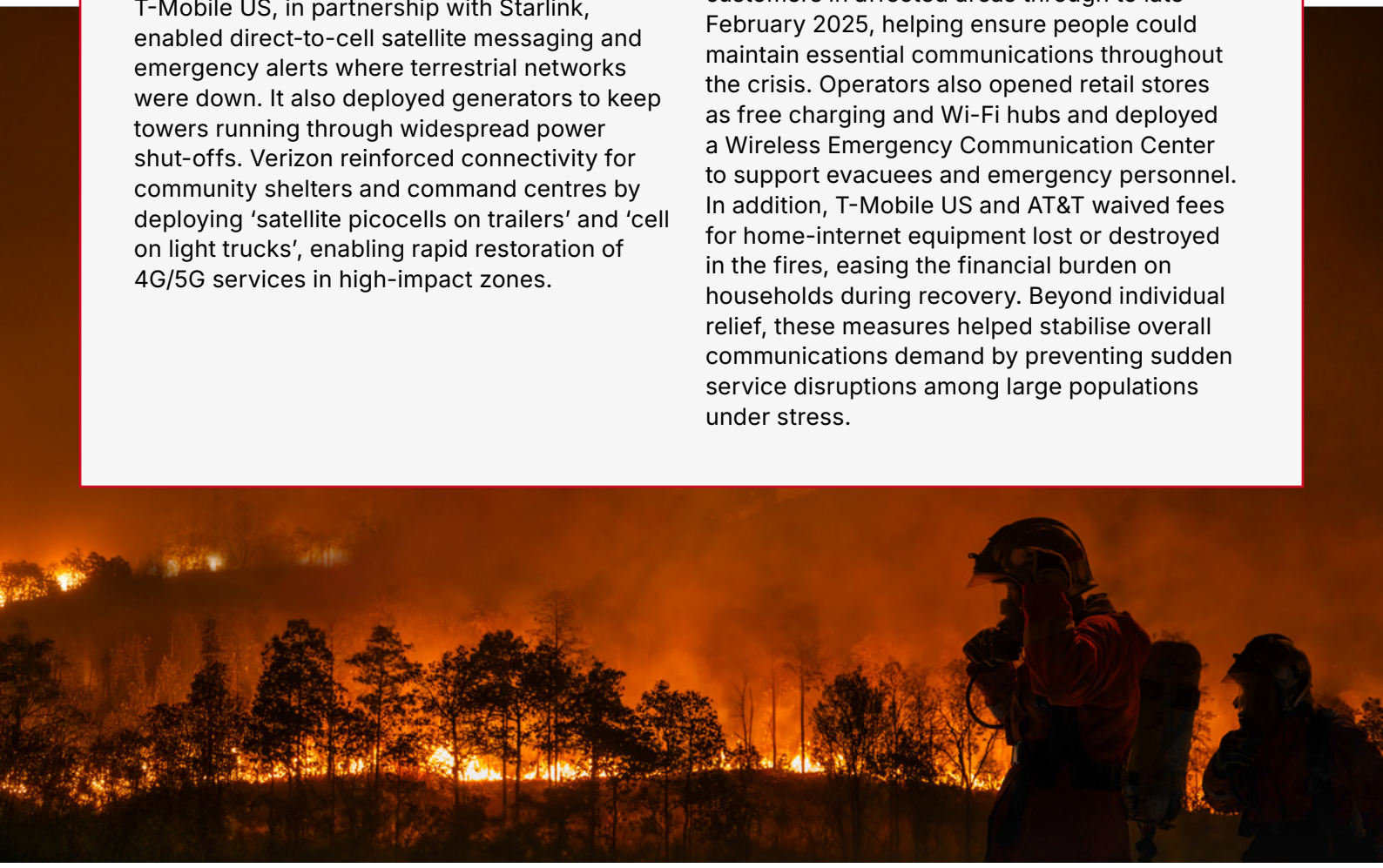
AT&T deployed its drone-based Flying Cell on Wings to provide aerial coverage for multiple users at a time and used LEO-enabled connectivity trailers to re-establish service in remote or inaccessible areas, strengthening operational reach during the emergency. T-Mobile US, in partnership with Starlink, enabled direct-to-cell satellite messaging and emergency alerts where terrestrial networks were down. It also deployed generators to keep towers running through widespread power shut-offs. Verizon reinforced connectivity for community shelters and command centres by deploying 'satellite picocells on trailers' and 'cell on light trucks', enabling rapid restoration of 4G/5G services in high-impact zones.

Support for first responders

AT&T activated its FirstNet public-safety network to prioritise emergency traffic for agencies such as CalFire, deploying its Compact Rapid Deployable – single-operator units that can be set up within minutes – to establish dedicated coverage in critical areas. T-Mobile US supported first responders through its T-Priority platform, enabling a dedicated 5G network slice for Los Angeles Fire Department personnel to maintain high-performance connectivity despite extreme network congestion. Verizon Frontline responded to a wide range of mission-critical requests, delivering routers, hotspots and network extenders directly to incident zones to reinforce communications for frontline teams.

Community relief efforts

AT&T, Verizon and T-Mobile US waived domestic call, text and data charges for customers in affected areas through to late February 2025, helping ensure people could maintain essential communications throughout the crisis. Operators also opened retail stores as free charging and Wi-Fi hubs and deployed a Wireless Emergency Communication Center to support evacuees and emergency personnel. In addition, T-Mobile US and AT&T waived fees for home-internet equipment lost or destroyed in the fires, easing the financial burden on households during recovery. Beyond individual relief, these measures helped stabilise overall communications demand by preventing sudden service disruptions among large populations under stress.



04

Policies for innovation and growth

The mobile industry sits at the centre of the digital economy. Its continued growth relies on forward-looking, enabling policies. As AI, cloud technologies and advanced connectivity reshape how societies operate, mobile networks are carrying more data, supporting more critical services and driving greater innovation than ever before. At the same time, spectrum demand is rising, cyberthreats are becoming more sophisticated and expectations for secure, high-performance digital services continue to increase. In this context, supportive policy frameworks are essential to ensure that mobile networks can expand, evolve and remain resilient. They form the foundation for the wider digital ecosystem, fuelling economic growth, enabling new industries and ensuring that the benefits of digital transformation reach people and businesses everywhere.

4.1
Securing future spectrum requirements

Mobile's ability to deliver economic growth relies on spectrum. While 5G launches continue, the mobile ecosystem is also starting work with governments to plan spectrum for 6G, which will come into use during the 2030s. Channel sizes will increase from 100 MHz in the 5G era to 200–400 MHz in the next phase of mobile's evolution. 6G implementations are not likely to be widespread before 2030, but planning spectrum harmonisation, such as for the 4.5 and 7 GHz bands, is already advanced.

Spectrum must be effectively licensed at the correct time. Spectrum roadmaps that consider market dynamics and growth in demand for mobile data can help deliver this. Roadmaps are an important means of ensuring there is sufficient spectrum to meet future demand from businesses and consumers. Information on spectrum releases is critical for mobile operators to prepare investment plans, secure financing and develop arrangements for deploying different technologies.

Spectrum plans that enable enterprise digitalisation are also part of roadmap planning. This means that operators will require spectrum not just for consumers but also for industrial connectivity. Now that enterprise connectivity is a maturing sector, the practice of setting aside spectrum for specific uses is being limited. Setting aside spectrum for specific uses, such as local or bespoke private networks, does not encourage private networks (as had been initially thought), but rather harms the amount of spectrum available to provide industrial connectivity through mobile operators. Small set-asides to encourage experimentation and creativity (e.g. in 4.1–4.2 GHz or in non-core bands) are continuing, which are less disruptive.

The cost of spectrum also has a major impact. Governments and regulators should assign spectrum for mobile to support their digital connectivity goals, rather than as a means of maximising state revenues. Effective spectrum pricing policies are vital to support better-quality and more affordable mobile services.

> **Setting aside spectrum for specific uses does not encourage private networks, but rather harms the amount of spectrum available to provide industrial connectivity through mobile operators**

Meeting connectivity needs through effective spectrum policies

Continued growth and innovation depend on clarity of spectrum availability in the short and long terms. Roadmaps can be developed going into the 2030s that include low-, mid- and high-band spectrum, which will benefit network investment. More spectrum is needed for increased capacity and faster networks. An average of 2–3 GHz of mid-band spectrum (frequency bands between 1 GHz and 10 GHz) will be required in the 2035–2040 period to meet demand in locations around the world with high-population densities.

Mid-bands provide city-wide coverage and cater for around 80% of indoor capacity in urban areas, where mobile is predominantly used indoors. They will also deliver much of the capacity required for enterprise digitalisation and industrial connectivity. Consequently, any country that wants to maximise the socioeconomic benefits derived from 5G needs to assign more mid-band spectrum.

3.5 GHz has been the launch band for 5G, while the accelerating momentum behind 6 GHz has confirmed it as the harmonised home for the future of mid-band capacity. The footprint for the 6 GHz band continues to develop in major markets throughout Europe, the Middle East and Africa (EMEA), Asia Pacific and the Americas, such as in India, China, Brazil and Mexico. Over 80% of the global population now lives in a country that supports 6 GHz mobile. However, reaching the 2–3 GHz goal by 2035–2040 (which rises to 2.5–4 GHz in the busiest markets) is difficult to achieve without adding new bands. For this reason, the World Radiocommunication Conference 2027 (WRC-27) will consider the 4.5 and 7 GHz bands.

Increasing low-band capacity should also be a priority as countries plan their roadmaps. Low bands are ideal for covering wide areas with a lower population density. This makes them an important resource as countries look to address coverage and usage gaps with broad and affordable connectivity.

High-band spectrum, or mmWave, is essential for the deployment of networks with ultra-high speeds and the lowest possible latencies. Governments and regulators should plan to make core high-band spectrum available in high-use hotspots as demand increases. High bands can complement low- and mid-band spectrum in dense urban areas, provide fibre-like connectivity through fixed wireless access (FWA) technologies and help innovate enterprise connectivity.

Spectrum licensing, pricing and conditions

Roadmaps are an important means of ensuring there is sufficient spectrum for future demand from consumers and new technologies. Information on spectrum releases is critical for mobile operators to prepare investment plans, secure financing and develop arrangements for deploying different technologies.

The timely release of technology- and service-neutral spectrum bands can deliver a positive impact on consumers. Long-term value, innovation and cost reductions need to be provided through relatively short technology cycles. If spectrum is released sooner, operators have more time to invest in new technologies that are more efficient and sustainable to make them available nationwide. More spectrum also eases capacity constraints in urban areas so that operators are better able to invest in rural areas.

Conversely, unnecessary delays to spectrum awards risk harming mobile broadband service rollouts, leaving more people unconnected and weakening the positive enablement effect that mobile can have on the reduction of carbon emissions.

Spectrum roadmaps can help define when spectrum should be made available, but barriers remain. Setting aside spectrum for specific uses such as local or bespoke private networks is an unnecessary barrier to meeting demand and should be avoided in priority 5G bands (particularly 3.5 and 6 GHz). Approaches such as leasing or sharing are typically better options in these situations, while private mobile networks are commonly provided by mobile operators within licensed public mobile spectrum.

The cost of spectrum also has a major impact, from when it is assigned to ongoing fees and the cost of renewals. Governments and regulators should assign spectrum to support their digital connectivity goals rather than as a means of maximising state revenues. Effective spectrum pricing policies are vital to support better-quality and more affordable mobile services. In turn, this will help address issues such as the usage gap and help get more people online. High reserve prices, artificially limited spectrum supply (including the set-asides mentioned above) and poor auction design can all have a negative impact due to suppressed investment capabilities (i.e. slower mobile broadband, limited coverage and higher prices for consumers).

Whatever the means of delivering spectrum to operators – an auction, an administrative process or another mechanism – governments that adhere to the policy objectives of maximising broadband rollout will achieve the best networks for their citizens.

Fortunately, governments and regulators are adopting new pricing and licensing approaches to ease the financial pressure on operators while encouraging investments in connectivity and coverage. One of these approaches is licensing spectrum on a technology-neutral basis (allowing the refarming of spectrum for 4G and 5G at a pace driven by market demand). Licensing terms are extended or made indefinite without additional payments, helping create an investment-friendly environment for the future. Regulators are also attaching coverage commitments in exchange for lower prices when auctioning or renewing spectrum.

Conditions should always be used with caution after careful consideration of any potential risks. Consulting with the industry will help maximise the chance of a successful outcome.

Maximising the benefits of mobile

Governments and regulators should:

- make available sufficient spectrum and avoid limiting the supply via set-asides
- set modest reserve prices and annual fees to let the market determine spectrum prices
- carefully consider auction design to avoid unnecessary risks for bidders (e.g. avoiding mismatched lot sizes, which create artificial scarcity)
- develop and publish a spectrum roadmap with the input of stakeholders to help operators plan effectively around future availability
- consult stakeholders on the award rules and licence terms and conditions, taking them into account when setting prices (onerous obligations reduce the value of spectrum).

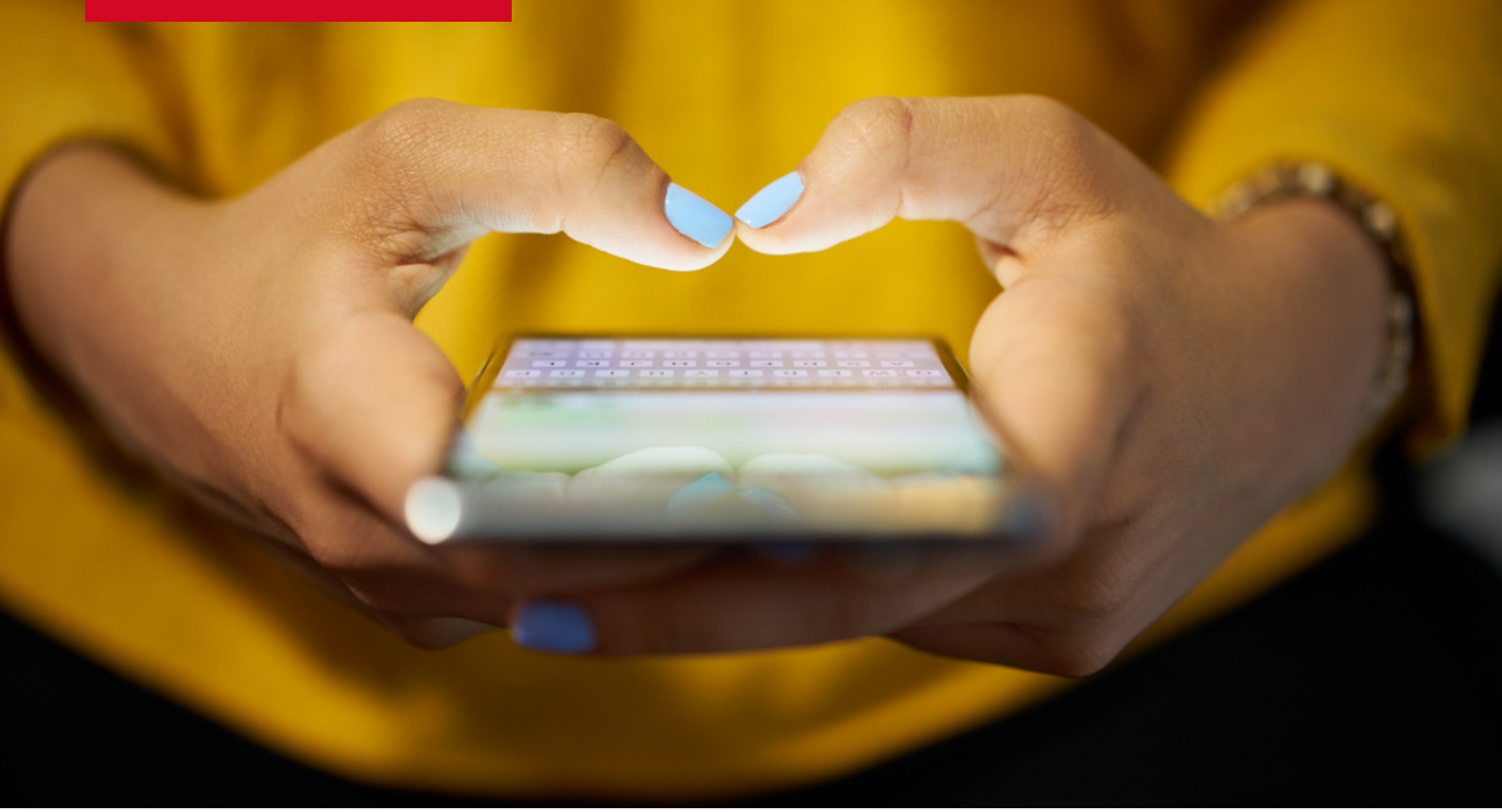
6G spectrum and WRC-27

6G is expected to be deployed from around 2030, with large initial rollouts likely to occur in China, Japan, South Korea, the US, the GCC states, Europe, Vietnam and India. The number of 6G connections could reach more than 5 billion by 2040, representing approximately half of all mobile connections globally. The technology is expected to enable new and emerging use cases that could increase demand further in the 2030–2040 period, with much heavier uplink requirements. These include extended reality (XR), image- and video-driven genAI and potentially holographic communication.

2 GHz of mid-band spectrum is required to be available by 2030 onwards and 2–3 GHz (in all countries) or 2.5–4 GHz (in higher-demand countries) may be required in the 2035–2040 period to cope with the additional traffic demand. Due to the long timescale needed to deliver widespread harmonisation of spectrum, government and regulatory planning is already happening for mobile in the 2030s. The upper 6 GHz band, which has already been widely harmonised and provides capacity for multiple channels over 200 MHz, is being considered as the next expansion band for mobile evolution in the widest number of countries.

WRC-27 will consider bands for the next phase of evolution, including the 4.5 and 7–8 GHz bands. However, as each of these bands has incumbent use, regulators and policymakers need to plan for increased mobile spectrum requirements now, considering the lead times required for international harmonisation, equipment development and network deployment.

Economic growth from mobile broadband will depend on sufficient spectrum availability. As wireless connectivity expands beyond smartphones to industrial machines and connected vehicles, meeting this demand will require timely allocation of additional spectrum to support future network capacity.



4.2
Staying safe in the digital world

The global financial cost of cybercrime, including fraud, is projected to escalate from $9.22 trillion in 2024 to $15.63 trillion by 2029.[17] The potential outcomes of this threat for consumers include significant financial loss, considerable emotional distress and the erosion of trust in digital services, creating a barrier to the adoption of beneficial technologies. Furthermore, the adaptability and global reach of technology such as AI is allowing organised criminals to perpetrate social engineering at scale and refine their deceptive tactics to target diverse populations across multiple regions. Vulnerable groups such as older people are often targeted in many developed markets, such as the UK, Australia and the US. Meanwhile, mobile money users are a key target for criminals in Africa, Asia Pacific and Latin America.

Human behaviour is often the weakest link in the security chain, and criminals are increasingly exploiting this through social-engineering techniques to obtain the information they need for online crimes. Social engineering targets human psychology, manipulating individuals into disclosing personal data or authorising transactions they believe to be legitimate. Fraudsters favour these tactics because they allow access to online services, digital devices and sensitive information without having to bypass technical security measures such as firewalls or antivirus software. Often described as 'human hacking', social engineering exploits emotional triggers – such as fear, curiosity or sympathy – to pressure individuals into revealing confidential information or completing fraudulent financial actions.

The effects ripple outwards, affecting global markets, increasing security costs and hampering digital transformation efforts in vulnerable regions. In 2023, Australians lost AUD2.74 billion ($1.9 billion) to scams, with the oldest age groups most targeted, resulting in losses for people over the age of 65 of AUD120 million ($83 million).[18] The US reported losses of $10 billion to scams in 2023 with imposter (impersonation) fraud the top fraud category, with reported losses of $2.7 billion.[19]

17. Estimated cost of cybercrime worldwide 2018–2029, Statista, January 2026
18. "Scam losses decline, but more work to do as Australians lose $2.7 billion", The Australian Competition and Consumer Commission, April 2024
19. "Think you know what the top scam of 2023 was?", Federal Trade Commission, February 2024

Response measures to social engineering and fraud

To combat social engineering fraud, governments, regulators and the mobile industry are employing various measures:

- **Education and awareness campaigns:** As criminals continue to adapt their methods, public awareness efforts remain key to equipping individuals with the knowledge they need to safeguard their personal and financial information. By urging consumers to stop and consider whether a situation is genuine before acting, such campaigns can help build a more fraud-resilient population.
- **Technical measures:** To protect their customers, mobile operators are investing significant resources in solutions, including firewalls, authentication mechanisms, robust information security policies and continuous system monitoring and reporting mechanisms.
- **Reporting services:** Mobile operators provide spam reporting services that allow mobile customers to report unwanted SMS messages or phone calls to their provider, which in turn will update its network protections accordingly.
- **Collaboration:** The global nature of fraud means that no single entity or industry can combat impersonation fraud alone. Collaborative data-sharing platforms are now being developed to facilitate the exchange of information between key stakeholders, enabling faster detection and response to emerging fraud schemes.
- **Legislative measures:** Fraudulent activity is addressed by a variety of laws and regulations worldwide, with specific legal frameworks varying by country. Financial regulators worldwide have enforced stricter know-your-customer (KYC) requirements to ensure businesses verify the identity of their clients, reducing the likelihood of impersonation fraud.
- **International frameworks:** As social engineering and impersonation fraud often transcend national borders, international cooperation is critical in combatting these global threats. Countries and organisations around the world are increasingly collaborating to harmonise legal frameworks, share intelligence and coordinate cross-border enforcement efforts.

4.3
Supporting the mobile industry to tackle evolving cyberthreats

As digital dependency grows, exposure to cyberthreats rises in parallel, creating serious risks for individuals, businesses, governments and society as a whole. Secure mobile networks are therefore not just a technical necessity, but a foundation for trust and safety in a connected world. The rapidly evolving threat landscape is increasing the cost and complexity of effective cybersecurity for mobile operators, making the role of regulation more critical than ever.

A GSMA report[20] estimates that mobile operators globally spend between $15 billion and $19 billion annually on their 'core' cybersecurity activities, including technical security functions and threat-monitoring teams. This figure likely underestimates total spending in cybersecurity, as it excludes broader activities that contribute to cybersecurity, such as governance, training and ensuring network resilience.

Mobile operators worldwide face similar challenges in meeting cybersecurity regulatory requirements. Well-designed frameworks help them manage risks proportionately and strengthen network security and resilience, while poorly aligned or overly burdensome rules can increase costs, complicate operations and even create new vulnerabilities.

To support effective policymaking, the GSMA has outlined six core principles that legislators and regulators should consider when shaping cybersecurity policy. Applied consistently, these principles help minimise unnecessary costs and allow operators to focus on genuine risks and mitigation. They are relevant to all countries: in less mature digital markets, they guide the development of robust policy foundations; in more advanced markets, they help refine and consolidate existing rules so operators can concentrate on tackling threats and protecting end users.

The six principles for best practice cybersecurity policy

Harmonisation: Align cybersecurity policy with international standards wherever possible, to reduce regulatory fragmentation and inconsistency.

Consistency: Ensure new policies and frameworks are consistent with existing policy to avoid duplication or conflict.

Risk- and outcome-based: Adopt risk-based and outcome-based approaches in the design and implementation of cybersecurity regulation, giving operators flexibility to innovate and deploy effective solutions.

Collaboration: Promote a collaborative regulatory culture with the industry (supported by secure threat-intelligence sharing to strengthen resilience), increase awareness of cyberthreats, enable constructive enforcement and foster a joint approach to combating cybercrime.

Security by design: Encourage a proactive, security-by-design approach to mitigating cyber risks.

Capacity building: Strengthen the institutional capacity of cybersecurity authorities to ensure a whole-of-government approach and effective application of policy and regulation.

20. The Impact Of Cybersecurity Regulation On Mobile Network Operators, GSMA, 2025

Further reading

Consumer devices: what matters to consumers in 2026, and the trends set to shape purchases and usage, GSMA Intelligence, 2026

Digital transformation of vertical sectors: the new wave of B2B opportunities revealed by the 2025 global enterprise survey, GSMA Intelligence, 2025

CES 2026: how advanced AI is shaping devices, smart home, digital entertainment and automotive, GSMA Intelligence, 2026

Accelerating Smartphone Adoption in Africa, GSMA, 2026

Fraud and Scams: Staying Safe in the Mobile World, GSMA, 2025

The Impact Of Cybersecurity Regulation On Mobile Network Operators, GSMA, 2025

The State of Mobile Internet Connectivity 2025: Overview Report, GSMA Intelligence, 2025

eSIM will unlock LPWAN-based IoT opportunities, GSMA Intelligence, 2025

Staying one step ahead: telco security in 2025, GSMA Intelligence, 2025

Telco AI: State of the Market, Q4 2025, GSMA Intelligence, 2026

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom