

India Ecosystem Insight Report

From Mobile Connectivity to Digital Infrastructure





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 www.gsma.com

Author

GSMA Asia Pacific

Contributors:

Debashish Chakraborty, Senior Director, Advocacy and Industry Engagement, APAC, GSMA
Jeanette Whyte, Head of Public Policy and External Affairs, APAC, GSMA
Sarvashreshth Kalash, Senior Manager, Digital Ecosystem, APAC, GSMA
Bensen Koh, Director of Policy, APAC, GSMA
Samuel Perks, Senior Consultant, APAC, GSMA



A GSMA Report for IMC 2026

This report positions India's mobile ecosystem as a strategic layer of national digital infrastructure: enabling AI diffusion, enterprise productivity, resilient digital public infrastructure, secure digital transactions and sustainable operator investment.



CONTENTS

FOREWORD	03
1. EXECUTIVE SUMMARY	04
2. INTRODUCTION: INDIA'S THIRD TELECOM PHASE	06
3. DEFINING THE SHIFT: FROM CONNECTIVITY TO DIGITAL INFRASTRUCTURE	09
3.1 Connectivity as access	
3.2 Connectivity as infrastructure	
3.3 Connectivity as platform	
3.4 Digital sovereignty	
3.5 What changes for operators and policymakers	
4. PRIORITY AREA I: AI-READY NETWORKS AND FUTURE INFRASTRUCTURE	12
4.1 AI for telecom: making networks more intelligent, efficient and secure	
4.2 Telecom for AI: networks as the distribution layer for India's AI economy	
4.3 India's AI ambitions require an AI-ready networks agenda	
4.4 Managing the trade-offs	
5. PRIORITY AREA II: ENTERPRISE DIGITISATION AND MONETISATION	16
5.1 Fixed wireless access and broadband expansion	
5.2 Enterprise connectivity and private networks	
5.3 Network APIs and Open Gateway	
5.4 Cybersecurity and enterprise trust services	
5.5 Constraints to enterprise and platform growth	
5.6 Policy direction	
6. PRIORITY AREA III: DPI, DIGITAL TRUST AND SECURE DIGITAL GROWTH	21
6.1 Telecom as a key enabler of trust for DPI	
6.2 From OTP dependence to risk-based authentication	
6.3 Scam prevention and cross-sector coordination	
6.4 Privacy, proportionality and user trust	
6.5 Policy direction	
7. POLICY COORDINATION: AVOIDING FRAGMENTED DIGITAL INFRASTRUCTURE GOVERNANCE	24
7.1 Five coordination gaps	
7.2 A national digital infrastructure coordination mechanism	
7.3 Principles for policy coordination	
8. WHAT SUCCESS LOOKS LIKE: OUTCOMES FOR INDIA	26
9. POLICY RECOMMENDATIONS	28
9.1 Recognise telecom as strategic digital infrastructure	
9.2 Build AI-ready and investment-ready networks	
9.3 Scale enterprise and API ecosystems	
9.4 Embed telecom in digital trust and DPI governance	
9.5 Build evidence-based policy capacity	
10. CONCLUSION: THE NEXT DIGITAL INFRASTRUCTURE COMPACT	30

FOREWORD

India has already answered the question of scale. Well over a billion connections, some of the world's most affordable data and a set of public digital rails that other markets now study and try to copy. It is one of the great achievements of modern telecoms, built by operators who invested through some genuinely difficult years. The question this report asks is an exciting one: what does India's mobile ecosystem get to become next, and how quickly can we, as an industry, seize that opportunity?

I have spent enough time in this region to see how much more interesting the story becomes once you look at what runs on top of the network. AI that needs low latency and trusted data flows, enterprises that want connectivity they can build a business around, and a digital public infrastructure that gets stronger every year because the mobile layer underneath it is secure. This report makes the case that these are not side issues for telecom. They are a genuine growth opportunity, and one that plays to India's strengths.

This report sets out a practical and, I believe, hopeful path. Specific, well governed network capabilities, number verification, SIM swap signals, quality on demand, can make India's digital economy safer and more productive, and the early results from initiatives already underway are

encouraging. I asked the team to be candid about where the evidence is still developing rather than to overstate the case, and that honesty only makes me more confident in the direction of travel.

Realising this will take an investment climate that rewards operators for building future ready networks, a regulatory approach that recognises telecom as critical infrastructure, and a genuine partnership between industry, government and the wider digital ecosystem, banks, developers, cloud providers. This report describes that partnership as India's next compact, and I see real appetite from every side of the table to build it.

GSMA will continue to bring global industry evidence, expertise and experience to India's digital transformation. I am confident in the opportunity ahead. This report gives policymakers, operators and partners a clear path to unlock the next phase of India's digital growth, together.



Julian Gorman
Head of Asia Pacific, GSMA

01

Executive Summary



India's telecom sector is entering a new phase. The first phase connected people through mobile access. The second phase made data affordable and enabled mass digital participation. The third phase must now convert telecom scale into strategic digital infrastructure: AI-ready networks, enterprise productivity platforms, secure digital transactions, trusted identity, cybersecurity, digital public infrastructure resilience and programmable network capabilities.

This shift matters because India's digital economy is no longer driven only by consumer internet adoption. The next wave of value will come from productivity, automation, intelligence, trust and resilience. These outcomes require telecom networks to be treated not only as regulated communications services, but as foundational infrastructure for the wider digital economy.

The report focuses on three priority areas. First, AI-ready and future-ready networks: India's AI ambitions will require high-capacity, secure, resilient and increasingly intelligent networks. AI must also be used inside telecom operations to improve planning, energy efficiency, service assurance, cybersecurity and fraud detection. Second, enterprise digitisation and platform-based monetisation: operators need new revenue pathways through fixed wireless access, enterprise connectivity, private networks, cloud connectivity, network APIs and cybersecurity services. Third, digital trust and DPI resilience: as India's digital transaction environment scales, telecom capabilities can support digital trust through secure authentication, fraud prevention and privacy preserving network intelligence

The central policy proposition is that India needs a new digital infrastructure compact between government and industry. Government should provide policy coherence, investment certainty, proportionate regulation, ease of deployment and formal coordination across telecom, AI, DPI, data protection, cybersecurity, competition and financial regulation. Industry should move beyond connectivity by building AI-ready infrastructure, enterprise solutions, API ecosystems, digital trust capabilities and deeper partnerships with government, developers, enterprises and public institutions.

If this transition succeeds, India can move from being one of the world's largest digital consumption markets to becoming a producer of trusted digital infrastructure, standards, platforms and services. The prize is a more productive, inclusive, secure and globally competitive Digital India.

Core recommendations

- **Recognise telecom as strategic digital infrastructure.** Telecom networks should be explicitly recognised as foundational to AI, DPI, cybersecurity, cloud, enterprise digitisation and digital trust.
- **Build AI-ready and investment-ready networks.** India should connect AI policy with telecom readiness through predictable spectrum, fibre, right-of-way, infrastructure sharing, edge/cloud connectivity and proportionate compliance.
- **Scale enterprise and API ecosystems.** Government and industry should support FWA, enterprise 5G, private networks, Open Gateway APIs, developer sandboxes, sector-specific pilots and public procurement models that measure productivity outcomes.
- **Embed telecom in digital trust and DPI governance.** Operators should be integrated into anti-fraud, scam prevention, identity assurance, cybersecurity, and DPI resilience frameworks through formal cross-sector coordination.
- **Develop metrics that capture telecom's broader economic value beyond ARPU.** Policy should measure avoided fraud, AI diffusion, enterprise efficiency, public-service resilience, productivity gains and inclusion outcomes.

02

Introduction: India's Third Telecom Phase



India's telecom sector has been one of the most important enablers of the country's digital transformation. It has connected people, expanded access to information, enabled digital services at population scale and supported new models of financial, commercial and public-service delivery. The next stage of India's telecom development, however, will be different. The sector is no longer defined only by subscriber growth, voice connectivity or consumer data usage. It is becoming a strategic layer of national digital infrastructure.

This report argues that India is entering a third telecom phase. The first phase was about mobile access: extending basic connectivity to hundreds of millions of people and creating the foundation for mass communication. The second phase was about affordable data and digital adoption: low-cost mobile broadband, smartphones and digital platforms enabled India to become one of the world's largest digital consumption markets. The third phase must now focus on digital infrastructure and economic value creation: AI-ready networks and platforms, enterprise digitisation, secure digital transactions, creating space for innovation, trusted identity, cybersecurity and programmable network capabilities. This report outlines the central argument that India's mobile sector is shifting from connectivity-led growth to a broader digital infrastructure model. As India moves into this next phase of AI-enabled digital infrastructure, competitiveness will depend not only on networks and platforms but also on whether businesses, public institutions and workers have the digital skills needed to adopt and use these technologies effectively.

India enters this phase from a position of significant scale. As of March 2026, India had more than 1.06 billion broadband subscribers, with broadband connections continuing to grow month-on-month. Wireless subscribers, including mobile and fixed wireless access, reached 1.28 billion, while active wireless mobile subscribers stood at 1.18 billion.¹ This scale is important, but the policy question is changing. The priority is no longer only how many people are connected. It is how connectivity can support productivity, innovation, trust and resilience across the wider economy.

Phase 1: Mobile access

India's first telecom phase was defined by the expansion of mobile access. Mobile networks created the base layer for inclusion by allowing citizens, businesses and public institutions to communicate at scale. This was a foundational achievement enabling voice communication, basic messaging, emergency access, information flows and the first generation of digital services.

The policy focus during this phase was therefore rightly centred on coverage, affordability, spectrum availability, competition, licensing reform and network rollout. Success was measured largely through subscriber growth, tele-density and the expansion of service availability.

That phase remains unfinished in some respects. Gaps in coverage quality, rural broadband availability, device affordability and meaningful digital inclusion continue to matter. Urban tele-density stood at 151.47 subscriptions per 100 inhabitants, compared with 60.46 in rural areas, highlighting the continuing connectivity disparity.² However, mobile access alone can no longer define India's telecom ambition. Access is the base layer; it is not the end state.

Phase 2: Affordable data and digital adoption

India's second telecom phase was driven by affordable mobile broadband and mass digital adoption. The combination of low-cost data, smartphones, digital payments, online platforms and app-based services brought millions of Indians into the digital economy. Mobile networks became the distribution layer for digital content, e-commerce, fintech, social media, entertainment, public information and government-to-citizen services.

This phase changed the role of telecom in India's development model. Connectivity moved from being a communications utility to becoming an enabler of digital participation. The impact was visible in the rapid scaling of digital payments, digital identity-linked services, online commerce, education platforms and citizen-facing government services. Mobile became the primary route through which many Indians experienced the internet.

Yet the economics of this second phase also created new tensions. The availability of affordable data supported digital adoption at national scale, but it also increased network demand and capital expenditure requirements. Operators invested heavily in spectrum, fibre, radio networks, transport infrastructure and 4G/5G upgrades, while monetisation remained closely tied to consumer tariffs and data usage. The result is a familiar structural challenge: the mobile sector carries a growing share of the investment burden for the digital economy but does not always capture a proportionate share of the value created on top of its networks.

This is why the transition to the third phase matters. India's next digital leap cannot rely only on more data consumption. It must be supported by stronger digital infrastructure capabilities, deeper enterprise adoption and a more sustainable investment model.

¹ Press Information Bureau (2026) Highlights of Telecom Subscription Data at the end of March 2026, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2254646&lang=1®=3>

² Press Information Bureau (2026) Highlights of Telecom Subscription Data at the end of March 2026, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2254646®=3&lang=1>

Phase 3: Digital infrastructure and economic value creation

The third telecom phase is defined by a shift from connectivity as access to connectivity as infrastructure. In this phase, mobile networks become a foundational layer for AI, cloud, cybersecurity, enterprise productivity, digital public infrastructure, and future digital services.

This transition is closely aligned with India's wider national digital agenda. The IndiaAI Mission, approved with an outlay of over ₹10,300 crore (US\$1.076 billion) over five years, reflects the government's ambition to build domestic AI capacity and expand access to AI compute infrastructure.³ India's Bharat 6G Vision aims for the country to become a frontline contributor to the standards, development and deployment of 6G technology by 2030.⁴

These initiatives point to a broader conclusion: India's AI, DPI, cloud, cybersecurity and future-network ambitions cannot be separated from telecom infrastructure. AI adoption will be strengthened by high-quality connectivity, secure data flows, cloud and edge access, resilient networks and low-latency services. Digital public infrastructure depends upon reliable authentication, trusted communications, fraud prevention and service continuity. Enterprise digitisation will require private networks, fixed wireless access, APIs, managed security and sector-specific connectivity solutions. Public-sector digitalisation will require networks that are secure, interoperable and resilient.

Why this matters now

India's digital economy is moving into a more complex phase. The first wave of digital growth was led by access and adoption. The next wave will be shaped by productivity, trust, automation, intelligence and resilience. This requires a telecom policy lens that goes beyond conventional sectoral boundaries.

For policymakers, the implication is clear: telecom should be treated as strategic digital infrastructure, not only as a regulated communications service. For operators, the implication is equally clear: future growth will depend on moving beyond consumer connectivity into enterprise solutions, network intelligence, API-based services, cybersecurity, edge capabilities and deeper partnerships with government and industry.

The third phase will also require better coordination across policy domains. Telecom policy can no longer be designed in isolation from AI policy, data protection, cybersecurity, cloud infrastructure, competition frameworks, digital public infrastructure and industrial policy. Fragmented governance risks creating overlapping compliance obligations, investment uncertainty and slower innovation. A more coordinated approach can help align national digital ambitions and convert the scale of India's digital society into economic value, institutional trust and global competitiveness.

³ Press Information Bureau (2025) Transforming India with AI, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2178092®=3&lang=2>

⁴ Press Information Bureau (2026) Status of 5G Rollout, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2239109&lang=1®=3>

03

Defining the Shift: From Connectivity to Digital Infrastructure



The transition from mobile connectivity to digital infrastructure is not simply a change in product terminology. It is a change in the economic and institutional role of telecom networks. In the first two phases, connectivity was primarily assessed through access, coverage, affordability, subscriber growth and data usage. In the third phase, these indicators remain important, but they are no longer sufficient. Networks should also be assessed by the value they enable across AI adoption, enterprise productivity, digital public infrastructure, cybersecurity, trusted identity and national resilience.

This report defines the shift through three roles: connectivity as access, connectivity as infrastructure and connectivity as platform. These roles are cumulative rather than sequential. India must continue expanding meaningful access, while also enabling networks to support higher-order digital and economic functions. The policy challenge is therefore not to replace the access agenda, but to expand it.

3.1 Connectivity as access

Connectivity as access remains the foundation of India's digital economy. It includes voice, mobile broadband, fixed broadband, device affordability, network coverage, service quality and meaningful digital inclusion. This role is still essential because gaps in rural broadband, indoor coverage, device affordability, digital skills and service reliability can limit participation in the digital economy. Access is therefore the base condition for every other layer of digital infrastructure.

However, access alone cannot define the next phase. A person may be connected and still be unable to participate meaningfully in AI-enabled services, secure digital transactions, enterprise platforms or public digital systems. The access agenda must therefore evolve from connection availability to meaningful participation in trusted, productive and resilient digital services.

3.2 Connectivity as infrastructure

Connectivity as infrastructure describes the role of telecom networks in supporting other critical systems. In this role, networks enable cloud access, data flows, secure transactions, public-service continuity, enterprise operations, digital identity, cybersecurity and emergency resilience. This is where telecom becomes part of India's wider national infrastructure architecture, similar to energy, transport and financial rails.

The infrastructure role is especially important for AI and DPI. AI applications require reliable connectivity between users, devices, edge nodes, cloud platforms and data centres. DPI systems require secure authentication, uptime, resilience and protection against fraud or misuse. Enterprises require predictable connectivity, secure data exchange and service-level assurance. These requirements go beyond bandwidth; they require reliability, trust, latency, security and governance.

3.3 Connectivity as platform

Connectivity as platform refers to programmable network capabilities that can be exposed to developers, enterprises, fintechs, banks, platforms and government through APIs and partnerships. In this model, operators do not only sell connectivity. They expose specific network capabilities such as number verification, SIM swap detection, device status, location verification, fraud-risk signalling and quality on demand, in standardised and privacy-preserving ways.

This platform role can unlock new monetisation pathways while supporting public-interest outcomes. For example, network APIs can make digital onboarding safer, reduce account takeover risk, improve transaction security, and enable better enterprise applications. But platformisation requires standardisation, developer engagement, clear consent models, interoperable commercial frameworks and cross-operator collaboration, even as individual actors retain independent control over pricing, commercial strategy, customer relationships and competitively sensitive information.

3.4 Digital sovereignty

A related issue is the growing policy discussion around digital sovereignty, strategic autonomy and trusted digital infrastructure. For India, these debates are increasingly relevant to sovereign AI capacity, trusted data ecosystems, resilience of critical digital infrastructure, secure cloud and edge infrastructure, cybersecurity, digital public infrastructure and participation in global digital standards. Telecom networks are directly connected to these questions because they provide the foundational layer through which digital services are accessed, secured, scaled, and governed.

At the same time, this report does not treat digital sovereignty as a standalone policy framework. The concept is still evolving globally and can carry different meanings across markets, ranging from domestic capability building and trusted infrastructure to data governance, supply-chain resilience, standards leadership and strategic autonomy. GSMA recognises the growing importance of this agenda and the need to consider how telecom networks contribute to trusted and resilient digital ecosystems. However, the focus of this report is narrower: to examine how India's mobile ecosystem is moving from connectivity-led growth to a broader digital infrastructure model.

Future work could examine digital sovereignty more directly, including how telecom policy can support India's ambitions around sovereign AI, trusted infrastructure, critical infrastructure resilience, secure cross-border digital services and leadership in international standards. For the purposes of this report, digital sovereignty is therefore treated as an important adjacent agenda rather than the central organising framework.

3.5 What changes for operators and policymakers

For operators, the shift means taking on a broader role within the digital ecosystem. MNOs are increasingly positioned to operate as infrastructure partners, enterprise solution providers, API platforms and trust-service enablers. This does not mean abandoning consumer connectivity. It means using the scale and intelligence of telecom networks to support new forms of economic and public value.

For policymakers, the shift requires a broader regulatory lens. Telecom policy can no longer be treated separately from AI policy, cybersecurity, data protection, cloud infrastructure, competition, DPI and financial regulation. A network that supports AI, digital identity, financial transactions and critical public services cannot be governed only as a consumer communications utility. Table 1 summarises the wider policy implications. The digital infrastructure network should be governed as strategic digital infrastructure.

Table 1: Role of Connectivity in India's Digital Infrastructure Transition

Role of connectivity	Primary question	Examples	Policy implication
Access	Who is connected, and at what quality and cost?	Voice, mobile broadband, fixed broadband, rural coverage, device affordability	Maintain coverage, affordability, spectrum, fibre and inclusion policies.
Infrastructure	What economic and public systems depend on networks?	AI, cloud, edge, cybersecurity, DPI, public services, enterprise systems	Treat telecom as foundational infrastructure for national competitiveness and resilience.
Platform	Which network capabilities can be exposed securely to others?	Network APIs - identity signals, device location, fraud-risk signals, geofencing, population density data	Enable interoperable APIs, developer adoption, privacy safeguards and commercial models.

04

Priority Area I: AI-Ready Networks and Future Infrastructure



AI is rapidly becoming a general-purpose technology for the economy, with potential applications across agriculture, healthcare, education, manufacturing, logistics, public administration, financial services and consumer platforms. However, AI adoption at population scale will not depend only on models, applications or compute capacity. It will also depend on the quality, security, reliability and intelligence of the networks that connect users, devices, enterprises, data centres, cloud platforms and digital services.

For India, this creates a strategic policy question: should telecom networks be treated merely as connectivity utilities, or as an essential part of the country's national AI infrastructure? The Government of India's strong focus on expanding the country's data centre capacity, growth of cloud services, enterprise digitisation and increasing use of digital public infrastructure all point in the same direction.⁵ India's AI ambitions will require future-ready networks that can support higher volumes of data, lower latency, secure data flows, edge computing, resilient connectivity and trusted access for users and enterprises.

The relationship between AI and telecom has two dimensions. The first is AI for telecom: the use of AI to make networks more efficient, secure, automated and responsive. The second is telecom for AI: the role of telecom in enabling and accelerating AI adoption across the wider economy. This goes beyond providing the connectivity infrastructure that AI depends on. MNOs can also contribute as responsible data stewards, using network data and intelligence in secure, governed and privacy preserving ways, subject to applicable law and appropriate safeguards. They are also catalysts for the wider AI ecosystem through investment, research partnerships, pilots, skills development and collaboration with governments, academia and technology companies. Both dimensions matter for India's third telecom phase. Together, they show why AI policy and telecom policy can no longer be treated as separate conversations.

4.1

AI for telecom: making networks more intelligent, efficient and secure

Telecom networks are becoming more complex. The expansion of 5G, fibre backhaul, cloud-native architectures, edge infrastructure, private networks, fixed wireless access, network slicing and API-based services requires a more intelligent approach to network planning and management. AI tools can help operators manage this complexity by improving network planning, predictive maintenance, energy efficiency, customer experience, fraud detection and cybersecurity.

In network planning, AI can help operators better anticipate demand, optimise capacity deployment and identify coverage or congestion risks.⁶ This is particularly relevant in India, where traffic patterns vary widely across dense urban centres, rural communities, industrial clusters, transport corridors, pilgrimage routes, public events and seasonal migration patterns. AI-enabled planning tools can potentially support more efficient capital allocation by helping operators identify where investment is most urgently needed and where solutions such as fibre, small cells, fixed wireless access or infrastructure sharing may be most appropriate.

In network operations, AI can support self-optimising networks, anomaly detection, fault prediction and automated service assurance.⁷ This can improve service quality while reducing operating costs. It can also support faster response during outages, traffic surges or cyber incidents. As more economic and public services depend on mobile connectivity, network resilience becomes a national digital infrastructure priority, not only an operator performance issue.

AI can also contribute to energy efficiency. Networks are energy-intensive infrastructure, and operators face growing pressure to expand capacity while managing costs and sustainability commitments. AI-enabled energy optimisation can help reduce power consumption by dynamically managing network resources, improving site-level efficiency and supporting better demand forecasting.⁸ This is especially important as data traffic grows and as operators continue investing in 5G and future network upgrades.

Customer experience is another area where AI can improve telecom operations. AI-enabled tools can support customer service automation, personalised service management, churn prediction and more efficient complaint resolution. However, these applications must be deployed in ways that are transparent, accountable and aligned with consumer protection expectations.

Perhaps most importantly, AI-enabled systems can strengthen network security and fraud prevention. Telecom networks generate signals that can help detect abnormal behaviour, suspicious activity, compromised devices, SIM-related risks and potential fraud patterns. Used responsibly, network intelligence can support anti-scam initiatives, financial transaction security, identity assurance and public-interest digital protection. However, this requires careful governance. AI-enabled security systems must be designed in a way that protects privacy, avoids disproportionate surveillance, minimises false positives and ensures clear accountability.

⁵ Invest India (2026) India's Data Centre Opportunity | Building Digital Infrastructure at Scale, <https://www.investindia.gov.in/team-india-blogs/indias-data-centre-opportunity-building-digital-infrastructure-scale>

⁶ Nouri Omheni, Hend Koubaa and Faouzi Zarai (2025) Artificial Intelligence for 5G and 6G Networks: A Taxonomy-Based Survey of Applications, Trends, and Challenges, <https://www.mdpi.com/2227-7080/13/12/559>

⁷ ETSI (2025) AI in the evolution of Autonomous Networks, [etsi.org/images/files/ETSIWhitePapers/ETSI-WP-69-AI-in_the_evolution_of_Autonomous_Networks.pdf](https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP-69-AI-in_the_evolution_of_Autonomous_Networks.pdf)

⁸ GSMA (2026) Energy Implications of AI for Mobile Operators, https://www.gsma.com/solutions-and-impact/connectivity-for-good/external-affairs/gsma_resources/energy-implications-of-ai-for-mobile-operators/

4.2

Telecom for AI: networks as the distribution layer for India's AI economy

While AI can improve telecom networks, telecom networks are equally essential to the scaling of AI. India's AI opportunity will not be realised only in laboratories, large technology firms or centralised data centres. It will be realised when AI tools become accessible to MSMEs, farmers, healthcare providers, educators, logistics operators, manufacturers, public institutions and citizens across the country.

This requires networks that can support reliable access to AI-enabled applications at scale. AI adoption across the economy depends on several infrastructure conditions. Users need affordable and reliable broadband access. Enterprises need secure and high-quality connectivity. Data needs to move between devices, cloud platforms, edge locations and applications with appropriate latency, security and reliability. Public services need resilient networks to support authentication, delivery and continuity. AI applications in areas such as telemedicine, industrial automation, logistics, mobility, agriculture and education may require different network characteristics, including higher reliability, lower latency or stronger security.

This is where telecom becomes a key enabler for India's AI stack. Connectivity is not simply the last-mile channel through which AI services reach users. It is part of the enabling architecture that determines whether AI can be deployed safely, inclusively and productively. Without

future-ready networks, AI adoption risks becoming concentrated among large firms, urban users and digitally advanced sectors. With the right telecom infrastructure, AI diffusion can be broader, reaching smaller enterprises, public services and underserved regions.

The relevance of telecom will increase as AI moves closer to the edge. Edge computing can support use cases where data processing needs to happen closer to users, devices or machines. This can reduce latency, improve privacy, lower bandwidth costs and support real-time applications. For India, edge-enabled AI could be relevant in manufacturing, logistics, smart cities, healthcare, agriculture, transport safety, energy systems and public service delivery. Telecom operators, with their distributed infrastructure, customer relationships, spectrum assets and network management capabilities, are well placed to support this transition.

Telecom's role in AI extends beyond providing connectivity and infrastructure. MNOs can also contribute as responsible data stewards, using network data and intelligence in secure, governed and privacy preserving ways, subject to applicable law and appropriate safeguards. Beyond data and infrastructure, operators can also act as catalysts for the wider AI ecosystem through investment, research partnerships, pilots and skills development, helping translate AI capabilities into practical applications across sectors.

4.3

India's AI ambitions require an AI-ready networks agenda

India has already recognised AI as a strategic national priority. However, AI policy is often discussed through the lens of compute, datasets, digital skills, start-ups, model development and responsible AI governance. These are all essential. But they are incomplete without a network readiness agenda. An AI-ready networks agenda should address five priorities.

First, India needs high-capacity and resilient connectivity to support rising data demand. AI applications, cloud services, video, immersive technologies, enterprise applications and machine-to-machine communication will all increase pressure on networks. Operators will need to continue investing in spectrum, fibre, transport networks, radio access networks, cloud-native systems and future network upgrades.

Second, India needs to strengthen cloud and edge connectivity. AI adoption requires efficient connectivity between users, enterprises, data centres, cloud platforms and edge nodes. Telecom networks can support this by enabling secure, low-latency and high-quality access to cloud and edge services.

Third, India needs enterprise-grade network capabilities. AI-enabled productivity gains will depend on whether enterprises can adopt reliable connectivity, private networks, secure IoT, managed services and sector-specific solutions. This is particularly important for manufacturing, logistics, ports, healthcare, education, agriculture, and public sector institutions.

Fourth, India needs trusted network intelligence. AI-enabled fraud detection, cybersecurity, identity assurance and service protection can strengthen digital trust. But this must be supported by clear governance frameworks that define permissible use, privacy safeguards, accountability mechanisms and coordination models across sectors.

Fifth, India needs investment certainty. AI-ready networks require long-term capital investment. Operators cannot be expected to continuously expand and modernise infrastructure if monetisation remains uncertain, regulatory obligations grow, and returns on network investment remain constrained. An AI-ready networks agenda must therefore be linked to an investment-ready policy environment.

4.4

Managing the trade-offs

The AI-telecom convergence creates important trade-offs that policymakers and industry will need to manage.

The first trade-off is between demand growth and value capture. AI adoption will increase demand for data, network quality and advanced connectivity. At the same time, the strategic opportunity for India is to ensure that this growing demand translates into broader domestic value creation. The question is not simply how quickly telecom networks can scale to accommodate AI-driven demand, but how infrastructure investment can be aligned with the growth of India's domestic AI ecosystem and the development of new business models and services. Without this alignment, India risks primarily absorbing the infrastructure demands of AI without capturing the wider economic value that the AI-telecom convergence could generate.

The second trade-off is between affordability and investment. India's low-cost data model has delivered enormous benefits for digital inclusion. However, future-ready infrastructure requires sustained investment. The policy challenge is to preserve affordability and inclusion while enabling operators to earn sufficient returns to invest in network quality, capacity, security and innovation.

The third trade-off is between data use and trust. AI systems require data, and networks generate valuable signals that can improve security, quality and service delivery. However, data use must align with privacy, consent, proportionality and consumer trust. India's data protection framework (DPDP Act) and wider digital governance architecture will need to support responsible innovation while protecting citizens.

The fourth trade-off is between security and operational burden. Telecom operators can play a significant role in

fraud prevention, cybersecurity and digital trust. However, regulatory frameworks should avoid imposing disproportionate obligations or fragmented compliance requirements that undermine innovation or create operational uncertainty. Security frameworks should be risk-based, evidence-led and coordinated across agencies.

The fifth trade-off is between sector-specific regulation and ecosystem-wide integration. AI, telecom, cloud, cybersecurity, data protection and digital public infrastructure are increasingly interdependent, but each sector domain also has distinct risks. Highly sector-specific approaches can provide clarity and address sector-specific concerns, but risks creating overlapping rules and missed opportunities. A coordinated national digital infrastructure approach would help align these domains.

India should thus treat AI-ready telecom infrastructure as a national competitiveness priority. This does not mean creating a separate policy framework for every technology trend. Rather, it means recognising that telecom networks are foundational to AI diffusion, enterprise productivity, public service delivery and digital trust. The policy direction should include predictable spectrum and infrastructure policies, easier right-of-way and deployment processes, support for fibre and backhaul expansion, incentives for cloud and edge connectivity, proportionate compliance obligations, and frameworks that encourage network innovation. It should also support collaboration between telecom operators, AI developers, cloud providers, public institutions, start-ups and enterprise users.

The outcome should be a clear national agenda: India's AI future will depend not only on algorithms and compute, but also on the networks that make AI usable, trusted and available across the economy.

05

Priority Area II: Enterprise Digitisation and Monetisation



India's telecom sector has reached a point where future growth cannot depend only on consumer connectivity. The first two telecom phases were built around subscriber growth, mobile access, affordable data and mass digital adoption. That model created enormous public value and positioned mobile networks as the main route through which citizens accessed the internet. However, the next phase of sector growth will require a broader monetisation model: one that links telecom infrastructure to enterprise productivity, secure digital transactions, industry modernisation and platform-based services.

If AI-ready and future-ready networks are the infrastructure foundation, enterprise digitisation and platform monetisation are among the clearest pathways through which operators can convert that infrastructure into new sources of growth. India's operators must be enabled to move from connectivity providers to enterprise infrastructure partners, API platform providers and trust-service enablers. This is not a speculative opportunity. India's economy is digitising across sectors, but enterprise adoption remains uneven. Large firms are investing in cloud, automation, cybersecurity, IoT, AI and data-driven operations. MSMEs are using digital payments, online marketplaces and basic software tools, but many still lack reliable broadband, secure digital systems, and affordable productivity solutions. Public-sector institutions are also digitising service delivery, monitoring, administration, and citizen engagement. Across these different segments, the common requirement is trusted, high-quality digital infrastructure.

Telecom operators are well positioned to serve this demand because they bring assets that few other actors possess at national scale: licensed spectrum, nationwide networks, customer reach, billing relationships, distributed infrastructure, security capabilities, enterprise relationships, operational experience, rich localised, contextual metadata and real-time network intelligence. The policy and commercial challenge is to convert these assets into scalable enterprise and platform services.

This chapter focuses on four targeted opportunities: fixed wireless access and broadband expansion; enterprise connectivity and private networks; network APIs and Open Gateway; and cybersecurity and enterprise trust services. These areas are intentionally specific as they identify near-term opportunities that are relevant to India's digital infrastructure transition and can create value for both operators and the wider economy.

5.1 Fixed wireless access and broadband expansion

Fibre will remain essential for long-term digital infrastructure, high-capacity backhaul, enterprise connectivity and data centre interconnection. However, fibre deployment can be difficult, slow or commercially challenging in areas affected by right-of-way constraints, low population density, local permissions, civil works costs or uncertain demand. FWA can complement fibre by offering a faster route to broadband connectivity for homes, MSMEs, semi-urban areas, rural communities and public institutions.

India's early FWA data already suggests strong relevance beyond dense urban markets. According to TRAI, total wireless FWA subscribers using 5G radio access technology increased from 12.32 million at the end of March 2026 to 12.55 million at the end of April 2026. Of these, 6.26 million were urban users and 6.29 million were rural users, meaning the rural share was slightly higher than the urban share at the end of April 2026. This is significant because it shows that FWA is not only an urban premium broadband product; it can also become a practical broadband solution for underserved regions where fixed-line expansion may be slower.

For households, FWA can improve broadband availability and quality where fixed broadband penetration remains limited. For MSMEs, it can support digital payments, online sales, inventory management, cloud software, customer communication, compliance tools and platform participation. For public institutions, it can connect

schools, clinics, local government offices, community centres and service delivery points. In these contexts, FWA is not simply another access product. It is an enabling layer for digital participation and local productivity.

FWA also strengthens the business case for 5G. In many markets, 5G monetisation has been challenging because consumers may not always pay significantly more for faster mobile data alone. FWA creates an additional use case by allowing operators to use 5G capacity to serve home and business broadband demand. In India, this is particularly relevant because data traffic is rising rapidly and 5G networks are already carrying a growing share of total usage.

The policy implication is that FWA should be integrated into India's broadband strategy. It should not be treated as a substitute for fibre, but as a complementary deployment model. Fibre will remain indispensable, especially for backhaul, enterprise-grade capacity and long-term network resilience. But FWA can expand broadband faster in areas where fibre deployment is constrained. This is especially important if India wants to support digital inclusion, MSME growth and public-service digitisation beyond major metropolitan centres. The objective should be to use all available technologies to expand meaningful broadband access, rather than treating fibre and wireless as competing policy choices.

5.2 Enterprise connectivity and private networks

The second opportunity is enterprise connectivity and private networks. India's next productivity gains will increasingly depend on the digitisation of key economic sectors. These sectors need connectivity that is more reliable, secure, and tailored than standard consumer-grade services. Enterprise connectivity is therefore not only a telecom revenue opportunity. It is a national productivity opportunity.

Industrial clusters, ports, airports, logistics hubs, warehouses, manufacturing units, healthcare campuses, universities, mines, public-sector campuses and smart infrastructure projects would benefit greatly from high-quality connectivity with predictable performance. In some cases, this may be delivered through enhanced public network services. In others, it may require dedicated private networks, managed campus connectivity, edge computing, IoT platforms or service-level guarantees.

Private networks can support use cases such as industrial automation, machine connectivity, robotics, worker safety, asset tracking, predictive maintenance, remote inspection, connected vehicles, video analytics, smart warehousing and secure campus operations. These are operational use cases, not merely communications use cases. Their value lies in reducing downtime, improving efficiency, enhancing safety, increasing visibility and enabling real-time decision-making.

India's opportunity is substantial but still early. India's deployment ecosystem remains at an early stage compared with more mature industrial 5G markets. This gap should not be viewed only as a weakness. It is also an opportunity to design an India-specific enterprise connectivity model that reflects the country's manufacturing ambitions, logistics needs, public-sector digitisation priorities and MSME structure.

The key policy question is how to support enterprise adoption while preserving incentives for operators to invest. Private network frameworks should encourage innovation, but they

should also avoid fragmenting spectrum use or undermining the economics of public network investment. India needs a balanced model that enables enterprises to access reliable and customised connectivity while ensuring that licensed operators remain central partners in deployment, management, security and service assurance.

Demand creation will be as important as supply. Many enterprises, especially outside large corporates, do not yet fully understand the productivity value of advanced connectivity. For them, connectivity is often seen as a cost line rather than a strategic input. This limits willingness to pay for higher-quality services. Operators and government therefore need to demonstrate use cases in sector-specific contexts. A manufacturing unit needs to see how private connectivity reduces downtime or improves quality control. A hospital needs to see how secure connectivity supports patient systems, telemedicine and device integration. A logistics hub needs to see how connected operations reduce delays and improve asset visibility.

India should therefore support enterprise connectivity pilots in priority sectors. These pilots should not be technology showcases alone. They should measure business outcomes such as productivity gains, operational efficiency, downtime reduction, safety improvements, fraud reduction, energy efficiency, service reliability and export competitiveness. This evidence will be critical for scaling demand.

Public-sector procurement can also play a catalytic role. Government is a major buyer of digital infrastructure, but procurement often treats connectivity as a commodity. In the third telecom phase, public procurement should recognise advanced connectivity as productivity and resilience infrastructure. Smart cities, public hospitals, transport systems, education campuses, industrial parks, logistics corridors and government service centres can all become anchor demand sites for enterprise-grade connectivity.

5.3 Network APIs and Open Gateway

For decades, telecom networks have contained valuable capabilities: identity signals, device status, location information, quality-of-service controls, SIM lifecycle data and fraud indicators. Historically, these capabilities were difficult for developers and enterprises to access in a standardised, scalable and privacy-preserving way. Network APIs change this by allowing operators to expose specific network functions through common interfaces that can be used by developers, fintechs, banks, platforms, enterprises and public institutions.

GSMA Open Gateway provides a global framework for this transition. It is designed to enable common, interoperable network APIs based on CAMARA standards, allowing developers and enterprises to access network capabilities consistently across operators and markets. Relevant API categories include number verification, SIM swap detection, device status, location verification, quality on demand and fraud risk signalling.

For India, the opportunity is particularly strong because of the scale and intensity of digital transactions. In such an environment, even incremental improvements in authentication, fraud detection, onboarding and transaction

security can create significant economic and consumer protection benefits.

The initial Indian Open Gateway use case is already aligned with this trust agenda. In October 2025, Indian mobile operators, supported by GSMA Open Gateway, announced federated network services to help online businesses combat scams and identity theft, including SIM Swap API. This API is designed to help businesses detect SIM-related fraud risks using standardised network capabilities.

This matters because India's current authentication model relies heavily on mobile numbers and OTPs. OTPs have enabled digital adoption at scale, but they also have vulnerabilities, including SIM swap fraud, phishing, social engineering and account takeover. Number verification and SIM swap APIs can help create a more secure, seamless and risk-based authentication model. For example, a bank or fintech could assess whether a SIM has recently been swapped before allowing a high-risk transaction. A digital platform could verify whether the phone number being used by a customer matches real-time network information. A public service platform could reduce account takeover risk during onboarding or recovery.

Beyond fraud prevention, APIs can support broader enterprise and developer innovation. Quality-on-demand APIs can support applications that require assured network performance, such as remote operations, gaming, industrial monitoring or live video services. Device status APIs can help enterprises assess whether a device is reachable or active. Location verification can support logistics, mobility, financial risk checks or emergency services, subject to appropriate consent and legal safeguards.

However, API monetisation will not happen automatically. It requires five conditions.

First, APIs must be standardised across operators. Developers will not build at scale if every operator exposes different interfaces, commercial terms or technical requirements.

Second, APIs must be easy to access and integrate. Documentation, sandboxes, developer tools and testing environments will be essential.

Third, pricing models must be commercially viable. APIs must generate value for enterprises while providing operators with a return on the network capabilities being exposed.

Fourth, privacy and consent models must be clear. Network APIs should expose specific, purpose-limited signals rather than broad personal data. This will be essential for user trust and regulatory acceptance.

Fifth, ecosystem adoption must be actively developed. Banks, fintechs, e-commerce platforms, digital identity providers, insurers, logistics firms, public agencies and start-ups need to understand the use cases and business value.

India's digital economy is well suited for this model. The country has the scale, developer base, digital payments ecosystem and public digital infrastructure to become a leading market for network API adoption. But this will require deliberate coordination between operators, GSMA, developers, regulators, financial institutions and major digital platforms.

5.4 Cybersecurity and enterprise trust services

The fourth opportunity is cybersecurity and enterprise trust services. As India's economy digitises, cybersecurity is becoming a core business requirement rather than a specialised IT function. Enterprises face growing exposure to phishing, ransomware, malware, identity theft, account takeover, data breaches, supply-chain attacks, payment fraud and operational disruption. MSMEs are particularly vulnerable because many lack dedicated cybersecurity teams, tools or budgets.

The scale of the challenge is clear. PIB data shows that from 2022 to 2024, more than 9.42 lakh SIM cards and 2,63,348 IMEIs linked to cyber frauds were blocked, underlining the connection between telecom networks, digital identity and fraud prevention.⁹

Separately, India's National Cyber Crime Reporting Portal data shows that India recorded more than 24 million financial cyber-fraud complaints in 2025, involving reported losses of approximately ₹22,495 crore.¹⁰ This highlights the scale of cyber-enabled financial crime.

These trends create a significant role for telecom operators. Operators can provide secure connectivity, managed security services, DDoS protection, threat intelligence, mobile identity assurance, fraud risk signalling, IoT security, endpoint protection partnerships and incident response support. They can also help enterprises secure the network layer of their operations, which becomes increasingly important as businesses adopt cloud services, connected

devices, remote work tools, digital payments and AI-enabled applications.

For MSMEs, operators can package cybersecurity into simple and affordable managed services. This could include secure broadband, device protection, phishing protection, managed firewalls, identity checks, fraud alerts and basic cyber hygiene tools. For larger enterprises, operators can provide more advanced services, including secure private connectivity, managed SOC partnerships, threat detection, cloud security connectivity, zero-trust network access and IoT security.

Telecom operators also have a role in public-interest digital trust. Network-level intelligence can support scam prevention, suspicious traffic detection, messaging security, SIM-related fraud detection and secure authentication. However, this must be governed through clear frameworks that protect privacy, ensure proportionality and define lawful data use. Trust services should not become a route to excessive data collection. They should be designed around specific risk signals, clear purposes and accountable governance.

Cybersecurity also has a direct link to enterprise monetisation. As businesses become more dependent on digital operations, they will increasingly value secure connectivity and managed trust services. Operators can therefore build cybersecurity into enterprise offerings rather than treating it as an add-on. In the third telecom phase, trust can become a revenue model as well as a public good.

⁹ Press Information Bureau (2025) Curbing Cyber Frauds in Digital India, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146®=48&lang=2>

¹⁰ Press Information Bureau (2026) Cybercrime Reporting and Investigation, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2226441&lang=1®=1&utm>

5.5 Constraints to enterprise and platform growth

The four opportunities outlined above are significant, but they face real constraints.

The first constraint is uneven enterprise demand. India's enterprise base is highly diverse. Large firms may be ready for private networks, cloud connectivity, and advanced cybersecurity, while many MSMEs still need basic broadband, digital tools, and simple security products. Operators will need differentiated offerings for different levels of digital maturity. A one-size-fits-all enterprise strategy will not work.

The second constraint is limited understanding of productivity value. Many businesses still assess connectivity mainly through price rather than operational impact. This makes it difficult to monetise quality, reliability, security or service-level assurance. Operators and policymakers need to shift the conversation from connectivity cost to productivity value.

The third constraint is ecosystem readiness. APIs, private networks, and cybersecurity services require partnerships. Operators cannot scale these models alone. They need

developers, cloud providers, system integrators, device manufacturers, fintechs, banks, platforms, public institutions and sector-specific technology providers. Ecosystem development will be as important as network capability.

The fourth constraint is public procurement and regulatory design. Government procurement often treats connectivity as a commodity service. This can discourage advanced connectivity solutions that may cost more upfront but deliver greater productivity, security or resilience benefits. Regulatory frameworks may also lag behind the changing role of telecom, especially in areas such as APIs, identity assurance, private networks, data sharing, cybersecurity coordination and digital trust services.

The fifth constraint is investment incentive. FWA, enterprise connectivity, APIs and cybersecurity all require investment in platforms, systems, talent, partnerships, security architecture, developer engagement and network upgrades. Operators need confidence that these investments can generate returns. Policy frameworks should therefore support commercial experimentation, proportionate regulation and long-term infrastructure investment.

5.6 Policy direction

India should build a stronger enterprise connectivity and platform ecosystem as part of its third telecom phase. The objective should be to move from connectivity consumption to connectivity-enabled productivity. This requires coordinated action by government, regulators, operators, enterprises, developers, cloud providers, financial institutions and public agencies.

The policy direction should include six priorities.

First, FWA should be recognised as a core part of India's broadband expansion toolkit. It should complement fibre deployment and support home broadband, MSME connectivity, public institutions and underserved areas.

Second, India should accelerate enterprise 5G and private network adoption through sector-specific pilots, industrial testbeds, public-private partnerships and procurement models that measure productivity outcomes.

Third, Open Gateway and network APIs should be supported as a platform opportunity for India's digital economy. This should include developer sandboxes, cross-operator standardisation, privacy-preserving design and priority use cases in fraud prevention, identity assurance, fintech, e-commerce, logistics and public services.

Fourth, telecom-enabled cybersecurity and trust services should be integrated into enterprise digitisation strategies. Operators should be enabled to support MSMEs and larger enterprises with secure connectivity, managed security and fraud-risk services.

Fifth, public procurement should recognise advanced connectivity as productivity and resilience infrastructure. Government can act as an anchor customer for enterprise-grade connectivity in health, education, transport, smart cities, industrial parks and public administration.

Sixth, regulatory frameworks should preserve investment incentives while enabling innovation. Operators should have the confidence to invest in enterprise platforms, APIs, cybersecurity and advanced connectivity without facing fragmented obligations or uncertain commercial returns.

The central message is that enterprise digitisation is not only a new revenue opportunity for operators. It is a pathway for India to convert telecom scale into economic productivity. If Chapter 4 showed why networks must become AI-ready and future-ready, Chapter 5 shows how those networks can become commercially sustainable and economically productive. Fixed wireless access, enterprise connectivity, network APIs and cybersecurity services provide the bridge between infrastructure investment and value creation.

06

Priority Area III: DPI, Digital Trust and Secure Digital Growth



India's digital public infrastructure has created one of the world's most extensive digital transaction environments. Aadhaar, UPI, DigiLocker, ONDC and other public digital rails have enabled population-scale participation in payments, identity-linked services, document access, commerce and government delivery. The success of this model has made digital systems central to daily life, public administration and economic activity.¹¹

Scale, however, also changes the risk profile. As more citizens, enterprises and public services depend on digital systems, the consequences of fraud, identity misuse, phishing, scams, spam, account takeover, data misuse and platform vulnerabilities become more serious. Trust is therefore no longer a soft outcome. It is a core infrastructure condition for India's digital economy.

Telecom is central to digital trust because mobile numbers, SIM identity, device signals, connectivity patterns and network intelligence are deeply embedded in India's digital services ecosystem. Many digital services use mobile numbers for onboarding, authentication, account recovery, alerts and transaction confirmation. This makes telecom both a dependency and an opportunity: a dependency because weaknesses in mobile-linked authentication can create systemic risk, and an opportunity because network capabilities can help strengthen digital trust at scale.

6.1

Telecom as a key enabler of trust for DPI

India's next DPI phase should integrate telecom as an important enabler of digital trust and security layer, not merely as access infrastructure. Telecom has a key role to play alongside government, financial institutions, digital platforms and others. This does not mean turning operators into identity authorities or surveillance actors. It means recognising that specific network signals can support safer digital interactions when they are used in a purpose-limited, privacy-preserving, and accountable manner.

Potential use cases include anti-fraud coordination, identity assurance, scam prevention, SIM-swap risk checks, financial transaction security, public-service authentication, secure citizen access, emergency communications and privacy-preserving network intelligence. These use cases are most valuable when they are embedded into risk-based workflows rather than used as broad or intrusive data-sharing mechanisms.

6.2

From OTP dependence to risk-based authentication

India's digital adoption has relied heavily on mobile numbers and OTPs. This model has been successful because it is simple, scalable and familiar to users. But OTP dependence also creates vulnerabilities, including social engineering, phishing, SIM swap fraud, compromised devices and account takeover. As digital services become more valuable and more widely used, authentication must become more risk based.

Network-enabled risk signals can complement existing authentication methods. A bank, fintech or public service platform could assess whether a SIM was recently swapped before allowing a high-risk transaction. A platform could check whether a user's phone number matches verified network information. A government service could reduce account recovery risk by combining user consent, device status and network signals. These mechanisms should not replace legal identity frameworks, but they can make digital interactions safer and more resilient.

¹¹ Press Information Bureau (2026) India's Digital Public Infrastructure, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2235812&lang=1®=3>

6.3

Scam prevention and cross-sector coordination

Digital scams often move across sectors: telecom networks, messaging channels, financial accounts, payment systems, social platforms, and e-commerce interfaces. No single institution can solve this by itself. Operators may detect SIM-related or traffic-related anomalies; banks may detect suspicious transaction patterns; platforms may detect malicious accounts; law enforcement may see fraud complaints; CERT-In and sectoral regulators may identify broader threat patterns. The challenge is to connect these signals lawfully and quickly enough to reduce harm.

India should therefore strengthen coordination with structured anti-fraud collaboration between telecom operators, financial institutions, digital platforms, regulators and law enforcement. This should include clear escalation channels, shared taxonomies of fraud typologies, privacy-preserving risk signals, rapid blocking or mitigation processes, and transparent accountability. The objective should be to reduce fraud while preserving user rights and avoiding disproportionate burdens on any single sector.

6.4

Privacy, proportionality and user trust

The digital trust agenda must be designed carefully. Network intelligence can strengthen security, but it can also raise concerns about privacy, consent, proportionality and misuse. Trust services should therefore be governed around specific use cases, defined purposes, minimal data exposure, user protection, auditability and clear accountability.

A practical approach would distinguish between data sharing and signal sharing. In many cases, enterprises or public agencies do not need broad personal data. They need a narrow risk signal: whether a SIM has recently changed, whether a number can be verified, whether a device is reachable, or whether a transaction should be treated as higher risk. This purpose-limited model can support both security and privacy.

6.5

Policy direction

- **Integrate telecom into DPI resilience planning.** Telecom should be included in digital public infrastructure resilience discussions, particularly where mobile numbers, authentication and secure access are involved.
- **Build risk-based authentication pilots.** Banks, fintechs, public services and operators should test network-enabled risk signals for high-risk transactions and account recovery.
- **Create formal anti-fraud coordination mechanisms.** DoT, MeitY, TRAI, RBI, CERT-In, law enforcement, operators, banks and platforms should coordinate on fraud typologies, escalation protocols and lawful mitigation.
- **Use privacy-preserving network intelligence.** Digital trust services should rely on narrow, purpose-limited signals rather than broad data sharing.
- **Avoid fragmented compliance burdens.** Security obligations should be risk-based, evidence-led and coordinated across regulators to avoid duplication and operational uncertainty.

The core point is that India's next phase of digital growth will depend on trust as much as access. Telecom can help strengthen that trust if it is integrated into DPI governance as a secure, accountable and privacy-preserving infrastructure layer.

07

Policy Coordination: Avoiding Fragmented Digital Infrastructure Governance



India's digital infrastructure policy landscape is becoming increasingly interdependent. Telecom, AI, data centres, cloud, cybersecurity, data protection, competition, financial regulation, semiconductor policy, industrial policy and DPI are no longer separate domains. Decisions in one area now have direct consequences for the others.

This creates a coordination challenge. If these domains are governed in silos, India risks overlapping compliance obligations, inconsistent policy signals, slower deployment, investment uncertainty and missed opportunities for cross-sector innovation. A stronger coordination model is therefore essential to make the third telecom phase work.

7.1

Five coordination gaps

Telecom and AI policy alignment. AI adoption requires network readiness. AI policy should therefore include telecom infrastructure, edge connectivity, secure data flows and network resilience as part of the national AI stack.

Telecom and DPI alignment. DPI depends on reliable, secure and inclusive connectivity. Telecom should be included in DPI resilience, authentication and secure-access planning.

Telecom and cybersecurity alignment. Operators are central to critical infrastructure resilience, fraud prevention and secure communications. Cybersecurity frameworks should recognise telecom's role without creating fragmented obligations.

Telecom and data/competition governance alignment. Digital markets are shaped by data, platforms, cloud and network access. Data protection, competition and telecom policy must be aligned where network capabilities are used for identity, trust, APIs or enterprise services.

Telecom and investment policy alignment. Future networks require long-term capital expenditure. Policy should align spectrum, right-of-way, infrastructure sharing, taxation, public procurement and regulatory obligations with investment needs.

7.2

A national digital infrastructure coordination mechanism

India could consider designating a national digital infrastructure coordination mechanism, bringing together DoT, MeitY, TRAI, CERT-In, RBI, CCI, data protection authorities, relevant ministries, state-level implementation bodies and industry. The objective should be to establish a structured mechanism or framework for aligning policy design, implementation and investment priorities.

Such a framework could focus on four functions. First, strategic alignment: ensuring that telecom readiness is reflected in AI, DPI, cybersecurity and cloud policy. Second, implementation coordination: identifying deployment bottlenecks such as right-of-way, fibre permissions, infrastructure sharing and public procurement constraints. Third, risk governance: coordinating on fraud, cyber incidents, data use, authentication and critical infrastructure resilience. Fourth, evidence generation: measuring the economic value of telecom beyond ARPU and data usage.

7.3

Principles for policy coordination

- **Technology-neutral but infrastructure-aware.** Policy should support multiple deployment models - fibre, FWA, mobile, satellite, edge and private networks - while recognising their different use cases.
- **Proportionate and risk-based.** Compliance obligations should be aligned with actual risk, institutional capacity and operational feasibility.
- **Outcome-oriented.** Policy should measure productivity, resilience, inclusion, fraud reduction and investment outcomes, not only rollout metrics.
- **Interoperable by design.** APIs, identity signals, digital trust systems and public-sector platforms should avoid fragmented technical approaches.
- **Investment-compatible.** Policy ambitions must be matched with incentives for long-term network investment and sustainable operator economics.

The central coordination challenge is to ensure that India's digital policies reinforce one another. Telecom policy should enable AI, DPI and enterprise productivity. AI and DPI policy should recognise telecom as an infrastructure dependency. Cybersecurity and data governance should enable trust without undermining innovation. Investment policy should support the networks that all these ambitions require.

08

What Success Looks Like: Outcomes for India



The third telecom phase should be judged by outcomes, rather than only by technology deployment. Success does not simply involve more 5G sites, more data traffic or more digital services. Success would involve converting telecom scale into competitiveness, productivity, trust, inclusion and sustainable investment for India, as is illustrated in Table 2.

Table 2: The role of telecom in India's digital ecosystem

Outcome	What it means	Why telecom matters
Stronger digital competitiveness	India moves from digital consumption at scale to production of trusted infrastructure, platforms, standards and services.	Networks provide the foundational layer for AI, cloud, APIs, edge and secure digital services.
Wider AI diffusion	AI adoption expands beyond large firms and technology companies into MSMEs, agriculture, healthcare, logistics, manufacturing, education and public services.	Reliable, secure and high-quality connectivity determines whether AI can reach users and enterprises at scale.
More resilient DPI	Public digital systems become more trustworthy, secure and resilient against fraud, identity misuse and service disruption.	Telecom-enabled authentication, fraud signals and network resilience support DPI trust.
Enterprise productivity gains	5G, FWA, private networks, APIs, cloud connectivity and cybersecurity support enterprise modernisation.	Operators can provide the connectivity and trust services required for sector-specific digitisation.
Sustainable operator economics	New monetisation pathways improve the business case for continued network investment.	Enterprise services, APIs, FWA and cybersecurity can reduce reliance on consumer tariffs alone.
Deeper inclusion	Inclusion moves from basic access to meaningful participation in trusted, productive and AI-enabled services.	Networks enable access to broadband, public services, digital payments, AI tools and enterprise platforms.

These outcomes are mutually reinforcing. Wider AI diffusion increases demand for reliable networks. Enterprise productivity creates stronger monetisation pathways. Digital trust increases confidence in DPI and online commerce. Sustainable operator economics support continued investment. Deeper inclusion expands the social and economic benefits of digital infrastructure.

09

Policy Recommendations



The recommendations below translate the report's analysis into a practical policy agenda. They are framed as system-level recommendations rather than narrow sectoral asks because the third telecom phase requires coordinated action across government, regulators and industry.

9.1 Recognise telecom as strategic digital infrastructure

Government can formally recognise telecom networks as foundational infrastructure for AI, DPI, cybersecurity, cloud, enterprise digitisation and digital trust. This recognition should be reflected in national digital policy, AI policy, DPI strategy, cybersecurity planning and public procurement.

The policy language should move beyond telecom as a consumer communications service. It should recognise networks as enabling infrastructure for productivity, public-service delivery, secure transactions and national competitiveness. This would support better coordination across DoT, MeitY, TRAI, CERT-In, RBI, CCI and other relevant bodies.

9.3 Scale enterprise and API ecosystems

Government and industry should support enterprise digitisation through FWA, enterprise 5G, private networks, cloud connectivity, Open Gateway APIs, cybersecurity and sector-specific use cases. The focus should be on measurable productivity outcomes rather than technology showcases alone.

India should create developer sandboxes, cross-operator API standardisation, privacy-preserving API design, sector-specific pilots and commercial models that make network capabilities useful to banks, fintechs, e-commerce platforms, logistics firms, public agencies, start-ups and enterprises.

9.5 Build evidence-based policy capacity

India should measure the value of telecom beyond ARPU, subscriber numbers and data traffic. Relevant indicators should include productivity gains, avoided fraud, AI diffusion, enterprise efficiency, public-service resilience, cybersecurity outcomes, quality of service and inclusion outcomes.

Evidence-based policy capacity will be particularly important for procurement, enterprise pilots, network API adoption, cybersecurity coordination and digital trust. It will help government and industry identify which interventions create measurable economic and public value.

9.2 Build AI-ready and investment-ready networks

India should develop an AI-ready networks agenda that connects AI policy with telecom readiness. This should include spectrum clarity, fibre and backhaul expansion, right-of-way reform, infrastructure sharing, cloud and edge connectivity, network resilience, cybersecurity readiness and proportionate compliance obligations.

Investment certainty is essential. Operators cannot be expected to continuously modernise networks if returns remain uncertain and obligations become fragmented. Policy should therefore support long-term capital formation through predictable regulation, ease of deployment and incentives for future-ready infrastructure.

9.4 Embed telecom in digital trust and DPI governance

Operators should be integrated into anti-fraud, scam prevention, identity assurance, cybersecurity and DPI resilience frameworks. This should include structured coordination between telecom operators, financial institutions, digital platforms, regulators and law enforcement.

Digital trust mechanisms should rely on narrow, purpose-limited and privacy-preserving network signals wherever possible. The aim should be to reduce fraud and strengthen authentication without creating disproportionate surveillance, broad data sharing or unclear accountability.

10

Conclusion: The Next Digital Infrastructure Compact



India's first telecom phase connected people. The second made data affordable and enabled mass digital participation. The third must turn the mobile ecosystem into a strategic layer of national digital infrastructure.

This transition is necessary because the next stage of India's digital economy will be shaped by AI, enterprise productivity, cybersecurity, trusted identity, secure transactions, public-sector digitalisation and resilient digital public infrastructure. None of these ambitions can be separated from telecom networks. The quality, security, reliability and intelligence of networks will determine whether India's digital transformation becomes more productive, inclusive and trusted.

The required response is a new compact between government and industry. Government must provide policy coherence, investment certainty, institutional coordination, proportionate regulation and recognition of telecom as digital infrastructure. Industry must move beyond connectivity by building AI-ready infrastructure, enterprise solutions, API ecosystems, digital trust capabilities and deeper partnerships with government and the wider digital economy.

The compact should be practical. It should help operators invest in future-ready networks. It should help enterprises adopt secure and productivity-enhancing connectivity. It should help public institutions build more resilient digital services. It should help citizens participate safely in digital systems. It should also help India develop the standards, platforms and trust architectures required for long-term digital competitiveness.

The prize is significant: a more productive, inclusive, secure and competitive Digital India. The third telecom phase is therefore not only a sectoral transition. It is a national digital infrastructure agenda.

GSMA Head Office

1 Angel Lane
London
EC4R 3AB
United Kingdom

