

VOICE & DATA

Connecting the Digital World

 CyberMedia

METEOROID, METEOR— OR METEORITE?

Release 20 studies are underway, but experts warn 6G may fracture into variants unless interoperability, AI standards, and coexistence are nailed early.



+ FOCUS: CAN THE TECHCO PIVOT DRIVE RELIANCE JIO'S USD 170 B BID?





APEEJAY SCHOOL

Pitampura, New Delhi | Estd. in 1990



**FOUNDATION
FOR LIFELONG
LEARNING
STARTS HERE**

KEY FEATURES



Regular student updates on the School Parent App



NEP 2020 aligned curriculum



Emphasis on value-based holistic education and life skills



Safe and secure campus with state-of-the-art infrastructure



Thematic learning with integration of Music, Arts, Sports and ICT



Air-conditioned transport facility available as per CBSE guidelines including GPS, CCTVs etc



AWARDS AND RECOGNITIONS

Ranked No. 1

in North Delhi Leader's
Category by
**Times Now School
Ranking 2025**

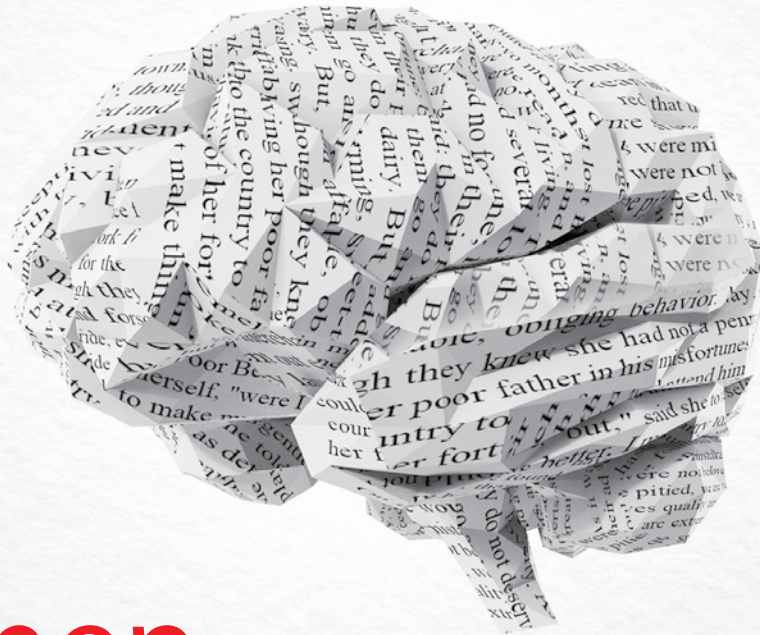
For more details, please contact us:

📍 Plot No. 10, Road No. 42, Sainik Vihar, Pitampura, Delhi – 110034

☎ +91- 7303-096-827, 011- 2702-2140, 011- 2701-2615

🌐 apeejay.edu/pitampura/

✉ skool.pp.del@api.edu



When print talks, the brain remembers

That's the power of print. In addition to **70% higher recall**, according to neuroscience research it's proven that print content is **21% easier to understand** and more memorable than digital media. That is why, print content connects with our brain more efficiently and effectively. So, choose to read newspapers.



INS

THE INDIAN NEWSPAPER SOCIETY

EDITORIAL

MANAGING EDITOR: Thomas George
CONSULTING GROUP EDITOR: Ibrahim Ahmad
EDITOR: Shubendu Parth
CONSULTING EDITOR: Pradeep Chakraborty
CONTRIBUTING EDITOR: Pratima Harigunani
ASSISTANT EDITOR: Ayushi Singh
CONTENT EXECUTIVE (Online): Punam Singh
SUB EDITOR: Manisha Sharma
SR. MANAGER DESIGN & COVER DESIGN: Vijay Chand
VICE PRESIDENT RESEARCH: Anil Chopra
MANAGER CYBERMEDIA LABS: Ashok K Pandey

LARGE BUSINESS CONVENTIONS & PROJECTS
CONFERENCE PRODUCER: Ajay Dhoundiyal

BUSINESS SOLUTIONS & SALES

VICE PRESIDENT - SALES & MARKETING: Aninda Sen
SR MANAGER: Ajay Dhoundiyal (North)
SR MANAGER: Sudhir Arora (North, East)
SR. MANAGER: Anita Swamy (South)

MARKETING & ALLIANCES

SR MANAGER: Ajay Dhoundiyal
ASSISTANT MANAGER: Mohd Atif Uddin

EVENTS, OPERATIONS & COMMERCIALS

SR. MANAGER, OPERATIONS: Ankit Parashar
CREATIVE DESIGN: Sunali
SR. MANAGER - ONLINE AD OPERATIONS: Suneetha B S
SR. MANAGER - COMMERCIAL & MIS: Ravi Kant Kumar
MANAGER - COMMERCIAL & ADMIN: Ashok Kumar

DISTRIBUTION & GROWTH:

GM - DISTRIBUTION & GROWTH: Prateek Malik
SR. MANAGER - INSTITUTIONAL SUBSCRIPTION: Sudhir Arora
SR. MANAGER - INSTITUTIONAL SUBSCRIPTION: C. Ramachandran (South)
SR. MANAGER - AUDIENCE GROWTH: Alok Saxena
EXECUTIVE - AUDIENCE SERVICE: Kusum Sharma
MANAGER - CREATIVE OPERATIONS: Suraj Singh
SOCIAL MEDIA EXECUTIVE: Amit Bhardwaj, Priyanshi Goyal
SEO TEAM: Neha Joshi, Chandan Kumar Pandey
PRESS CO-ORDINATOR: Rakesh Kumar Gupta

OUR OFFICES

GURGAON (CORPORATE OFFICE)

Cyber House
B-35 Sector-32, Gurgaon, Haryana - 122 003
Tel: 0124 - 4237517, Fax: 0124 - 2380694

BENGALURU

205-207, Shree Complex (Opposite RBNMS Ground)
#73, St John's Road, Bengaluru - 560 042
Tel: +91 (80) 4302 8412, Fax: +91 (80) 2530 7971

MUMBAI

INS tower, Office No. 326, Bandra Kurla Complex Road,
G Block BKC, Bandra East, Mumbai - 400051
Mobile: +91 99694 24024

INTERNATIONAL

Huson International Media
President, 1999, South Bascom Avenue, Suite 1000,
Campbell, CA95008, USA
Tel: +1-408-879 6666, Fax: +1-408-879 6669

Voice&Data is printed and published by Pradeep Gupta on behalf of Cyber Media (India) Ltd, D-74, Panchsheel Enclave, New Delhi - 110 017, and printed by him at M/s Archana Printers, D-127, Okhla Industrial Area, Phase-1, New Delhi 110020. Editor: Shubendu Parth

For subscription queries, please email: subscriptions@cybermedia.co.in or send a WhatsApp message to 9289870545.

All Payments Favoring: CYBER MEDIA (INDIA) LTD
Distributors in India: IBH Books & Magazines Dist. Pvt. Ltd, Mumbai.
All rights reserved. No part of this publication be reproduced by any means without prior written permission from the publisher
Corporate Website: www.cybermedia.co.in
www.ciol.com (India's #1 IT Portal)

January 2026

[CONTENTS]

COVER STORY 24

METEOROID, METEOR— OR METEORITE?

Release 20 studies are underway, but experts warn 6G may fracture into variants unless interoperability, AI standards, and coexistence are nailed early.



INDUSTRY SPEAK

08 Data–AI–telecom troika: India's next growth engine

10 India's OT blind spot: The risk beneath digital growth

13 Semicon PLI could de-risk India's digital infrastructure build

16 Premium phones: India's aspiration meets affordability

TECHNOLOGY

41 Laser nanowire films promise EMI shielding for 6G devices

44 From dumb pipes to intelligent telecom platforms

50 Cloud-native workflows are shrinking enterprise latency

TRENDS 2026

54 The thinking network: Making every node count

56 Security goes autonomous: AI agents, twins, AR wearables

60 Digital infrastructure shifts from scale to trust

63 The new enterprise core: cloud, cyber, and connectivity

BROADBAND BYTES



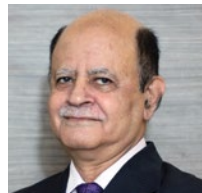
18 India's 2030 spectrum plan backs 6G, stumbles on Wi-Fi

TV Ramachandran

INSIGHT

21 Trusted photonics: Securing India's optical backbone

TELECOM TALK



29 Beyond uptime: Redesigning telecom for disasters

Lt Gen Dr SP Kochhar

FOCUS

32 Can the techco pivot drive Reliance Jio's USD 170 B bid?

PERSPECTIVE



38 AWS custom silicon: turning AI into infrastructure

SATINDER PAL SINGH

COMMENTARY

68 Creating sustainable, scalable, secure data centre stacks

70 From threats to trust: How AI secures digital growth

REPORT

72 5G FWA growth drives a modest wireless subscriber uptick

REGULARS

06 Voicemail

07 Opening Note

74 Postscript

[NEXT ISSUE]



DECEMBER 2025

Scan QR Code
& Subscribe now...



SEND YOUR FEEDBACK FOR US
TO SERVE YOU BETTER...

For **subscription queries**, please email:
subscriptions@cybermedia.co.in or
send a WhatsApp message to **9289870545**.

You can also write to
Reader Service Executive, **VOICE&DATA**,
Cyber House, B-35 Sector 32,
Gurgaon-122 003, Haryana
Tel: 9953150474, 7993574118



Share your views at vndedit@cybermedia.co.in

NEXT
ISSUE

DIGITAL TRANSFORMATION ON A BUDGET



For any query: ajaydh@cybermedia.co.in



SHUBHENDU
PARTH

[OPENING NOTE]

From a billion broadband users, the real network test begins now

India has crossed a psychological and structural milestone: one billion broadband subscriptions. In November 2025, broadband users touched 100.37 crore—up from 13.15 crore in November 2015, a six-fold expansion in a decade. The number itself is staggering, but the story it tells is even more consequential: connectivity in India is no longer an enabling layer—it is a core economic infrastructure, as fundamental as roads, power, and banking.

And yet, if the last decade was about scale, the next one will be about execution.

TRAI's latest Annual Report (FY25) captures this transition in the subtext of the numbers. India remains the world's second-largest telecom market, with 120.08 crore subscribers recorded in FY25, but the underlying pattern is shifting. Wireless subscriptions dipped by 85 lakh during FY25, while wireline grew 9.6%, adding 32.5 lakh users. That is not a statistical quirk. It is an indicator that India is maturing from mobile-first expansion to deeper, fixed broadband capacity—fibre, home networks, enterprise access, and the quality layer needed for the next decade of digital services.

Now ask a simpler question: where does the real digital economy live? Not on highways and metro corridors alone. It lives indoors—homes, offices, hospitals, malls, airports—where demand is dense, and expectations are unforgiving.

The same recalibration is visible in 5G. By February 2025, 5G was available in 99.6% districts through 4.69 lakh BTS, with around 25 crore subscribers using 5G services. India has demonstrated national-scale rollout velocity. But ubiquity is not the same as experience. The next test is whether networks can deliver consistent performance indoors, at the enterprise edge, and in high-density locations. In this phase, quality, latency, and resilience will matter as much as coverage maps, especially as AI workloads, real-time cloud services, and machine-to-machine traffic move into the mainstream.

This is why NFAP 2025—effective 30 December 2025—matters beyond the technicalities of frequency planning. The updated plan aligns with ITU Radio Regulations, supports 5G and satellite broadband, and recognises emerging use cases from V2X to HAPS. It is a forward-looking spectrum architecture. Yet it has also triggered a strategic debate over the 6 GHz band and what India should prioritise next: mobile IMT capacity or indoor Wi-Fi scale backed by fibre.

BIF argues that 70–80% of data usage occurs indoors and urges delicensing the entire 5925–7125 MHz band for Wi-Fi 6E/7 to keep access affordable and inclusive. COAI, meanwhile, supports identifying 6425–7125 MHz for IMT but also seeks the lower 6 GHz band, arguing telcos will need large contiguous mid-band blocks—up to 400 MHz per operator—to deliver 5G Advanced and future 6G.

For Voice&Data readers, the conclusion is clear: India's broadband milestone is a crossing, not a culmination—*sine qua non* for a digital economy, but not sufficient. The execution decade will be won by those who solve the indoor problem, deepen fibre, modernise policy through the new authorisation framework, and build networks for reliability, not just reach. In short, the future belongs to performance—*de facto*, not just on paper.

shubhendup@cybermedia.co.in

Data–AI–telecom troika: India's next growth engine

Beyond 2026, AI workloads and data growth will fuse telecom, fibre, and data centres into one infrastructure stack powering inclusive digital expansion.



BY DR BADRI GOMATAM

India's digital infrastructure is entering a defining phase. By 2026, the country is expected to see rapid growth in data usage driven by AI and national digital programs. Data centre capacity in India is projected to double from just over one gigawatt today to nearly two gigawatts by 2026, supported by investments of more than six billion dollars.

Over the longer term, total investments are expected to exceed USD 30 billion by 2030. Initiatives such as Digital India, BharatNet, and the India AI Mission are helping extend digital access to underserved regions, thereby increasing the need for faster, more reliable networks.

This growth marks a shift in how telecom networks are viewed. Networks are no longer only about connectivity. They are becoming the foundation for real-time services across manufacturing, healthcare, education, and governance. As data volumes rise, the demand for

networks that are fast, scalable, and energy efficient is becoming critical.

AI DATA CENTRES PUSH INDIA'S NEED FOR SPEED

AI is changing the role of data centres in India. High computing workloads, data localisation needs, and cloud adoption are driving strong demand for capacity. By 2030, the total data centre power capacity in the country is expected to reach eight gigawatts. Alongside large data centres, smaller facilities closer to the users are also growing to support low-latency applications such as smart cities, factories, and medical services.

These changes are pushing the industry to rethink network design. Data centres now require fibre networks that can handle large volumes of data with minimal delay while using power efficiently. Energy use has become a key concern, making efficient network infrastructure just as important as computing capacity.

As AI enters core services, telecom will be judged less by coverage and more by the ability to deliver assured performance at a national scale.



IN BRIEF

- The convergence shift moves planning from capacity adds to performance engineering—latency, uptime, energy efficiency, and security by design.
- AI will change traffic patterns: more east–west data flows between DCs, clouds, and edges, not only user-to-internet north–south flows.
- Edge growth will be driven by real-time needs—factories, healthcare, and governance—where milliseconds matter as much as bandwidth.
- Fibre becomes strategic infrastructure: rollout speed, route density, and upgradeability will decide how fast AI workloads can scale nationwide.
- Networks will evolve into programmable platforms, using automation and analytics to manage complexity across multi-cloud, edge, and enterprises.
- Inclusion will hinge on resilient last-mile delivery—affordable high-capacity access plus dependable backhaul into BharatNet-led expansion zones.

FIBRE INNOVATION IS THE NEW GROWTH BACKBONE

The rising data traffic from AI is putting pressure on existing fibre networks. To keep pace, the industry is adopting new approaches that focus on faster rollout and better use of space. Pre-connected fibre solutions are helping reduce installation time and dependence on skilled manpower, which is especially important in challenging environments.

Advanced fibre types are also gaining attention. New designs are being tested to reduce delay and increase capacity within existing network routes. These developments will be important as networks evolve to support future technologies and higher data volumes. At the same time, sustainability is becoming central to network planning, with a greater focus on reducing power consumption and supporting green data centres.

FUTURE-READY NETWORKS FOR THE NEXT DECADE

India is expected to generate a significant share of the global data in the coming years, even as its physical infrastructure remains relatively compact. This makes efficiency and smart planning essential. The next phase of telecom growth will depend on high-capacity fibre, simplified deployment models, and greater use of automation in network management.

The industry is moving away from short-term upgrades toward long-term solutions that can adapt to changing needs. Organisations across the telecom ecosystem, including Sterlite Technologies Limited Telecom, are aligning their efforts toward future-ready networks that support data centres and national broadband missions.

As India moves beyond 2026, data, AI, and telecom will become deeply interconnected. Together, they will shape a digital economy that is more inclusive, more resilient, and ready to support the country's long-term growth ambitions. 🌐

The author is the Group Chief Technology Officer of STL.

feedbackvnd@cybermedia.co.in



India's OT blind spot: The risk beneath digital growth

As connectivity and compute scale nationwide, weak OT systems in telco and data centre environments are emerging as a major security and reliability risk.



BY DAVID SEHYEON BAEK

India's digital economy is expanding at a pace matched by few other countries. Telcos are rolling out 5G across the nation, data centres are multiplying in key metros, and AI-driven services are driving record demand for compute power. Behind this surge stands a quieter but essential foundation: the operational technology that ensures the physical stability of India's digital networks.

While the country invests heavily in cloud security, application defence, and enterprise IT controls, the OT layer—the machinery powering the digital world—remains one of the most exposed and least governed areas.

This gap is becoming more consequential as digital dependency increases. The more India connects people, businesses, and public services, the more its reliability hinges on uninterrupted power, stable cooling, remote

automation, and control systems that were never designed with modern cyber risks in mind.

Many of these components offer minimal authentication, limited access control, and virtually no traceability. They prioritise uptime, not cyber protection. When these systems are breached, the incident may not resemble a headline-grabbing ransomware attack, but the consequences can be just as damaging. A single compromised controller can disrupt national capacity, degrade service availability, or trigger physical failures across a facility.

OT VULNERABILITIES IN DC AND TELCO SITES

Telecom operators rely heavily on OT systems across their networks. Cooling units in switching centres, generator controllers at tower sites, and environmental sensors

Cooling units, power systems, and automation controllers now represent high-impact targets. Compromising them can disrupt entire regions without touching IT systems.

inside fibre hubs play critical roles in ensuring network continuity. If manipulated, these components can cause outages that ripple across entire regions. Attackers do not need to breach the carrier's digital core; they only need to interfere with a cooling sequence, disrupt a fuel controller, or shut down an HVAC asset.

The problem is compounded by the fact that many devices still use shared passwords, unchanged factory credentials, or no authentication at all. A compromised laptop or an infected engineering workstation is often enough to grant adversaries access to OT devices that cannot distinguish between authorised and malicious commands.

Data centres operate under even tighter tolerances. India's capacity recently crossed 1,200 MW and is expected to exceed 4,500 MW by 2030. These facilities depend on a dense web of Building Management Systems (BMS) and Electrical Power Management Systems (EPMS) that control chillers, PDUs, generators, and switchgear.

Any disruption in thermal or electrical management can cause hardware failures, downtime, or cascading shutdowns. A single attacker-issued instruction to a PLC that regulates temperature, pressure, or fuel flow can destabilise an entire data hall. In extreme cases, it can force operators to power down hundreds of servers to prevent physical damage.

PROTOCOL FLAWS AND OT SYSTEM DESIGN GAPS

The structural issue lies in the design of OT systems. Their communication protocols often lack encryption. Standard industrial protocols such as Modbus TCP, BACnet/IP, and SNMP were built for clear-text communication and lack native encryption. Their authentication methods are often outdated or non-existent, relying on long-standing assumptions of trust inside operational zones.

In practice, these zones are no longer isolated. Over the years, through upgrades, expansions, and vendor integrations, telcos and data centres have accumulated mixed fleets of equipment, each with different security capabilities and operational behaviours. Even when new systems are added, they often inherit the weaknesses of the existing environment.



IN BRIEF

- OT systems in telcos and data centres remain the weakest link, exposing India's digital backbone to disruptions that traditional IT controls cannot prevent.
- Legacy OT devices lack authentication, encryption, and traceability, making cooling, power, and automation equipment easy targets for attackers.
- Remote access, mixed-vendor fleets, and expanding digital infrastructure increase exposure, allowing IT compromises to spill into operational networks.
- Protocols such as Modbus and BACnet rely on clear-text communication, enabling adversaries to send malicious commands without resistance.
- Securing OT requires identity systems, command verification, and access controls designed for low-bandwidth, partially offline environments.
- Strengthening OT security is vital for India's ambitions in AI, cloud, semiconductor manufacturing, and digital public infrastructure.

Meanwhile, the push for remote monitoring is widening exposure. India's telecom footprint spans tens of thousands of sites, many in remote or unmanned regions. Remote access is essential for efficiency, yet it opens more paths for intrusion. A misconfigured VPN, a weak jump server, or an exposed maintenance port can

Standard industrial protocols were never built for hostile environments. As remote access grows, attackers can exploit these gaps to cause physical disruption.

give attackers indirect visibility into OT assets. Once inside, they can move laterally through networks that were never meant to support a hostile presence.

India's broader push toward digital public services, industrial automation, and AI infrastructure is amplifying the problem. New factories, logistics hubs, energy plants, and smart cities are adding millions of connected OT devices. Many of these devices run on dated firmware and limited hardware that cannot support modern defensive tools. This means a compromise on the IT side—for example, via infostealer malware harvesting credentials—can quickly spill into the OT layer. The more digital India becomes, the more attractive its OT systems are as targets.

Regulatory frameworks are uneven. Detailed policies and compliance requirements govern enterprise IT. OT, by contrast, sits in a fragmented regulatory space. Some operators voluntarily follow international standards such as IEC 62443, but adoption differs widely across the telecom and data centre sectors. Many facilities prioritise physical resilience and operational continuity while giving limited attention to identity controls, command verification, and monitoring of engineering actions. This leaves significant gaps in systems that manage power, cooling, and automation.

Threat actors have also shifted their tactics. Advanced operations no longer require interference with OT equipment. Commodity malware can extract engineering passwords from infected devices. Open-source tools can communicate with common industrial protocols, such as Modbus. Public research has shown how attackers can manipulate environmental setpoints, disable alarms, or trigger malfunctions in automated systems. As India's digital role grows, adversaries will pay greater attention to the systems that support national connectivity and cloud infrastructure.

A significant reason this issue persists is that IT security controls cannot simply be copied into OT environments. Certificates require stable network connectivity for real-time validation, which may not be available in OT networks. Traditional MFA depends on cloud validation paths that are often unavailable. Password policies are difficult to enforce on legacy devices. Security agents

cannot be installed on low-resource controllers. Even zero-trust approaches struggle when devices cannot prove their identity cryptographically. OT requires identity systems that work reliably in low-bandwidth, segmented, or partially offline conditions.

SECURING OT AS INDIA'S DIGITAL BACKBONE

As India prepares for the next stage of digital acceleration, OT security must become a central priority. Telecom operators will need stronger identity mechanisms for engineering access at tower sites, switching hubs, and fibre nodes.

Similarly, data centre operators will need authentication frameworks that verify each command issued to systems that regulate power, cooling, and environmental control. Contractors and vendors will require access models that restrict privileges without exposing core networks. Regulators may also need to establish minimum OT cybersecurity baselines for facilities supporting national communication and compute services.

This is not merely a defensive goal. It is also critical for India's economic ambitions. The country aims to be a global centre for AI development, cloud hosting, semiconductor manufacturing, and digital public platforms. All of these rely on infrastructure that cannot compromise reliability. If OT systems remain weak, outages will increase as the infrastructure footprint expands. Attackers will choose the simpler path of targeting machinery instead of protected IT services. India's digital future depends on strong OT foundations.

Addressing this issue early will place India in a stronger position globally. Better OT security will help telcos maintain consistent national connectivity, support data centres handling AI and cloud workloads, and strengthen the country's digital backbone. The more India secures this often-overlooked layer, the more resilient and competitive its digital systems will be in the years ahead. 🌟

The author is the Founder and CEO of PygmalionGlobal. He collaborates with multiple cybersecurity companies, including NPCore in South Korea, and engages with government agencies and conglomerates across Asia.

feedbackvnd@cybermedia.co.in



Semicon PLI could de-risk India's digital infrastructure build

As India scales 5G, fibre, edge, and data centres, Semicon India aims to improve component supply, lead times, and cost stability for equipment.



BY SHETAL MEHTA

India's semiconductor strategy has moved from developmental intent to structured execution, driven primarily through Production Linked Incentive (PLI) schemes and the broader Semicon India programme. With an outlay of Rs 76,000 crore dedicated to semiconductors and display manufacturing, the policy framework is designed to reduce capital risk, strengthen domestic capacity, and anchor India within global supply chains.

For the communications ecosystem, including connectivity equipment, digital infrastructure, telecom networks, and data-driven platforms, this shift carries direct implications for the availability, cost, and reliability of core electronic components.

SEMICON INDIA TURNS CHIP POLICY INTO EXECUTION

The central semiconductor programme provides fiscal

The real DI payoff lies in fewer supply shocks—making fibre, data centre, and network builds less vulnerable to global disruptions and delays.

Domestic chip packaging can shorten the distance between design tweaks and deployment-ready gear, improving rollout speed across DI projects.

support across fabrication, compound semiconductor manufacturing, ATMP/OSAT operations, and display fabs, with support up to 50% of project cost in approved categories. Complementing this are PLI schemes for large-scale electronics manufacturing and for telecom and networking products, each offering incentive payouts linked to incremental domestic production over multi-year timelines.

This layered policy design is particularly relevant for digital infrastructure, which depends on a steady supply of RF chips, power devices, mixed-signal semiconductors, display drivers, and memory components. By lowering initial capital intensity and improving long-term feasibility for manufacturers, the PLI ecosystem aims to stabilise the supply pipeline for equipment that supports India's growing data traffic, broadband expansion, and enterprise networks.

EARLY OUTCOMES AND MEASURED PROGRESS

While the semiconductor-specific applications are still in early stages, adjacent PLIs have delivered measurable progress. Under the electronics PLI framework for large-scale electronics manufacturing, cumulative investments of Rs 13,759.44 crore had been recorded as of September 2025, with cumulative production reaching Rs 9.34 lakh crore. These figures indicate that performance-linked manufacturing incentives can successfully trigger sustained investment and scale.

For the communications ecosystem, this trajectory matters because large-scale electronics manufacturing creates the groundwork for localisation of modules, subcomponents, and specialised chip packaging used in network and connectivity equipment. Even partial localisation of these components can reduce lead times that traditionally run into months due to overseas dependencies and unpredictable logistics cycles.

STRENGTHENING THE CORE OF DIGITAL INFRASTRUCTURE

Semiconductors sit at the core of every communication architecture, supporting radio access networks, optical transport layers, switching hardware, backhaul systems, and customer-premises equipment. Even minor disruptions

in semiconductor availability can delay network rollouts and inflate equipment procurement costs.

Domestic capacity for chip fabrication, compound semiconductors, assembly and test, and display manufacturing, therefore, serves as a stabilising layer for telecom operators, data centre providers, broadband networks, and IoT infrastructure.

Local packaging and testing ecosystems, an essential part of the PLI-linked semiconductor strategy, enable shorter turnaround times for specialised chipsets that need regional frequency alignment, power management optimisation, and thermal performance tuning. This ensures higher responsiveness for network upgrades and deployment cycles.

SUPPLY RESILIENCE FOR 5G, EDGE, AND DATA CENTRES

India's digital infrastructure expansion, 5G densification, fibre-to-home scaling, edge computing nodes, and next-generation data centres depend heavily on a predictable semiconductor supply.

PLI interventions aim to resolve four longstanding challenges that have consistently constrained India's telecom and digital infrastructure build-outs.

#1

Supply security: By creating domestic manufacturing capacity, India reduces exposure to geopolitical disruptions, export controls, and global demand spikes that influence semiconductor availability.

#2

Cost predictability: Incentives effectively narrow the pricing gap between imported and locally assembled components. Over time, this may translate into reduced total cost of ownership for network equipment buyers.

#3

Lead-time compression: Local Packaging and fabrication reduce dependence on long cross-border logistics cycles, improving equipment rollout timelines for operators and integrators.

India could turn digital infrastructure planning from reactive procurement to predictable execution by stabilising critical component supply cycles.

#4

Customisation capability: Regional manufacturing enables faster design iterations for telecom-grade components, particularly when spectrum bands, power classes, or interoperability standards differ from global defaults.

These benefits create momentum for rapid and scalable digital infrastructure development across India.

HOW PLI DESIGN ALIGNS WITH DI EQUIPMENT NEEDS

Several structural elements within PLI programmes align with the operational requirements of digital infrastructure manufacturers by linking incentives to scale, synchronising support across the component-to-equipment stack, and reducing risk in high-capex segments. This improves feasibility for domestic suppliers to invest in capacity, tooling, and production upgrades that match telecom procurement cycles and reliability expectations.

Incremental incentive structure: Performance-linked payouts ensure that incentives scale with production output, providing manufacturers a clear path to improve unit economics as volumes increase.

Multi-scheme coherence: The combination of semiconductor, electronics, and telecom PLIs ensures alignment across the value chain, from chip to module to finished equipment, creating an integrated domestic manufacturing ecosystem.

Capital support for strategic layers: High-value segments such as fabs and display facilities receive cost-sharing support, reducing entry barriers and enabling deeper participation in areas critical to advanced communication systems.

Long-term manufacturing visibility: The multi-year framework of PLI schemes provides predictable timelines for investment planning, tooling cycles, and migration of design operations closer to production sites.

For stakeholders in telecom equipment and digital infrastructure, this policy consistency enables planning

across network cycles, procurement strategies, and domestic sourcing roadmaps.

ENABLERS FOR SUSTAINABLE SEMICONDUCTOR CAPACITY

While fiscal support offers a strong foundation, long-term semiconductor and communication equipment competitiveness depends on structural enablers developing in parallel. These include a steady supply of high-skilled talent, ecosystem development across chemicals and substrates, and advanced testing and certification infrastructure aligned with global telecom standards.

Demand aggregation through public digital infrastructure projects, enterprise digitalisation, and national broadband initiatives will also be essential to secure scale. For communication networks, where reliability is paramount, domestic manufacturing must align with rigorous testing protocols and interoperability benchmarks to ensure seamless deployment.

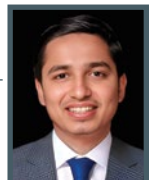
WHAT DOMESTIC CHIPS CHANGE FOR DI BUILD-OUTS

India's PLI-driven semiconductor strategy is not solely an industrial policy initiative; it is also a digital infrastructure strategy. As connectivity needs rise, semiconductor security becomes a strategic prerequisite for network resilience, equipment affordability, and long-term technology independence.

If the current momentum is sustained, with coordinated ecosystem building, skills development, and continuous alignment between policymakers and industry, India can build a semiconductor manufacturing base that directly strengthens the nation's communication networks. The outcome will be a more reliable supply chain, reduced import dependency, and greater capability to design, customise, and deploy next-generation digital infrastructure equipment at scale. 🌟

The author is the Co-Founder of Suchi Semicon.

feedbackvnd@cybermedia.co.in



Premium phones: India's aspiration meets affordability

India's premium smartphone demand is rising, driven less by status and more by value, longevity, access to financing, and resale confidence.



BY JAYANT JHA

There is a quiet shift underway in how Indians buy premium smartphones, and you can feel it the moment you step into a store. The excitement has not vanished, but it has matured. Customers do not rush to hold the most expensive device or marvel at its shine. They pause. They listen. They calculate.

Conversations that once revolved around camera specs and status now centre on longevity, software updates, battery health after a year, and what the phone will be worth when it is time to move on. This is not about impulse or aspiration. It is intent.

The modern Indian smartphone buyer is not chasing luxury for show. They are evaluating value, flexibility, and future-proofing. What looks like a premium purchase on the surface is, in reality, a carefully considered decision, one that reflects a broader shift in how ownership itself is being redefined.

ASPIRATION EVOLVES FROM STATUS TO UTILITY

Aspiration in India has matured. It is less noisy and more self-aware. A premium smartphone still carries social meaning, but it is not bought only to be seen. Increasingly, it is bought to avoid friction. Lag, poor cameras, short

Premium smartphones are no longer impulse buys in India—buyers are calculating longevity, updates, and resale before upgrading.

The new premium buyer is not chasing luxury; the phone is a work tool where performance and reliability matter more than shine.

software support, and unreliable performance are viewed as daily irritants, not minor compromises.

Counterpoint data indicates that in the July-September quarter of 2025, shipments of smartphones priced above Rs 30,000 rose 29% year-on-year, sharply outpacing the market's overall volume growth of 5%. At the same time, the total market value jumped 18%, indicating buyers are deliberately shifting toward higher-value devices.

Lag, poor cameras, short software support, and unreliable performance are viewed as daily irritants, not minor compromises. This is especially true among young professionals and independent workers. The phone is often their primary work device. It handles client calls, documentation, payments, social media presence, and video meetings.

In that context, a premium device is not a lifestyle upgrade. It is a work tool. Aspiration here is practical. It is about being prepared, not showing off.

AFFORDABILITY SHIFTS FROM PRICE TO ACCESS

India remains a value-for-money market. That has not changed. What has changed is how affordability is measured. Upfront price matters less than before; financing options such as no-cost EMIs and structured payouts have expanded significantly, enabling more buyers to consider phones above traditional price thresholds.

A Counterpoint report highlights that the premium smartphone category—above Rs 30,000—is expected to comprise over 20% of the Indian smartphone market's value, up from roughly 10–12% just a few years earlier.

This does not mean consumers are ignoring cost. They are simply managing it differently. A phone that feels unaffordable at once can feel reasonable when spread over time, especially if it replaces multiple needs. The phone becomes a camera, a wallet, a navigation system, and a workstation. That bundling effect is rarely acknowledged, but it plays a central role in the decision.

There is also a strong awareness of value retention. Buyers talk about resale value openly. According to Cashify's 2025 Annual User Behaviour Survey, nearly 63% of refurbished smartphone purchasers in early 2025 preferred Apple devices. This is a strong indicator of resale preference.

PREMIUM BUYERS BECOME SHARPER, LESS LOYAL

India's premium smartphone buyer is no longer easily impressed. Brand loyalty exists, but it is conditional. Incremental upgrades are questioned. Price increases are noticed. Marketing promises are tested against daily use.

This has made the premium segment less forgiving. Buyers expect stability, consistent performance, and long-term support. They are willing to pay, but only if the experience holds up. For manufacturers, this is both an opportunity and a warning. Premium demand will continue, but only for brands that respect the intelligence of the buyer.

Financing platforms and access models have become central to this ecosystem, not peripheral. They often act as the bridge between desire and decision. Without them, much of the premium demand would remain aspirational rather than transactional.

At a broader level, premium smartphone demand reflects a deeper truth about today's Indian consumer. Ambition is intact but tempered. People want better tools, not excess. They want reliability, not novelty. They want progress that does not destabilise their finances.

This is not a market that is chasing luxury. It is a market negotiating control. Aspiration and affordability are not in conflict here. They are being balanced, consciously and repeatedly, one purchase at a time. 🧠

The author is the Founder of BytePe.

feedbackvnd@cybermedia.co.in



TV RAMACHANDRAN

INDIA'S 2030 SPECTRUM PLAN BACKS 6G, STUMBLES ON WI-FI

NFAP 2025 charts spectrum priorities till 2030 for IMT, satcom, and HAPS, but the missing lower 6 GHz band risks slowing next-gen Wi-Fi.



As India progresses towards its vision of becoming a Viksit Bharat by 2047, the telecommunications sector is a foundational enabler of this transformation. With over 96% of broadband connections dependent on mobile or wireless networks, the country remains largely mobile-first. In such a context, radio-frequency spectrum—a finite and valuable natural resource—becomes critical to realising the goals of digital connectivity and deep tech integration.

The spectrum, which enables mobile and wireless communication, is globally regulated under the International Telecommunication Union's Radio Regulations (ITU-RR). In India, its allocation and management fall under the jurisdiction of the Wireless Planning and Coordination (WPC) Wing, functioning within the Ministry of Communications. The guiding document for spectrum planning is the National Frequency Allocation Plan (NFAP), published every four years. This plan is not merely a technical manual; it is a policy instrument reflecting India's technology

“

India has secured spectrum for 6G-era networks and satcom scale; now the lower 6 GHz decision must match the ambition of digital inclusion.



NFAP 2025 sharpens India's spectrum architecture for IMT, satcom, IFMC, and HAPS—setting the operating map for telecom growth through 2030.

ambitions, regulatory vision, and alignment with global standards.

The latest version, NFAP 2025, serves as a roadmap for managing India's spectrum resources in accordance with international norms while addressing domestic digital priorities. It lays down allocations across the frequency range from 8.3 kHz to 3000 GHz and outlines specific provisions for mobile broadband, satellite communications, and emerging technologies such as Vehicle-to-Everything (V2X) communication, High Altitude Platform Stations (HAPS), and In-Flight and Maritime Connectivity (IFMC).

FOCUS: IMT, SATELLITES, AND EMERGING TECHNOLOGIES

NFAP 2025 introduces several key changes designed to support India's digital transformation and to prepare the spectrum ecosystem for upcoming technologies, including 5G Advanced and 6G. A critical change in the plan is the identification of the 6425–7125 MHz frequency band, commonly known as the Upper 6 GHz band, for International Mobile Telecommunications (IMT). This allocation meets the growing demand for mid-band spectrum, which is crucial to supporting high-capacity, low-latency mobile broadband services.

The plan also strengthens satellite communications, an increasingly vital component of India's digital infrastructure, especially in remote and underserved regions. It has reserved the Ka (27.5–31 GHz), Q (33–50 GHz), and V (40–75 GHz) bands for satellite services. These bands are essential for supporting both Geostationary Orbit (GSO) satellites and large constellations of Low and Medium Earth Orbit (LEO/MEO) satellites, enabling high-throughput and low-latency connectivity.

In addition, NFAP 2025 has allocated spectrum for In-Flight and Maritime Connectivity (IFMC), ensuring broadband access is available not only on land but also in the air and at sea. This is seen as a significant step in creating uninterrupted, ubiquitous access to digital services.

The plan also accounts for future use cases by earmarking spectrum for emerging technologies.

This includes allocations for V2X communications, High Altitude Platform Stations (HAPS), and other innovative applications that demand high reliability and broad coverage.

HAPS AND V2X GET BOOST WITH GLOBAL HARMONISATION

Among the notable allocations is the 5.9 GHz band for V2X communication, which supports technologies such as Cellular Vehicle-to-Everything (C-V2X). Based on 3GPP global standards, C-V2X enables real-time communication between vehicles, infrastructure, pedestrians, and networks. This can play a pivotal role in reducing road accidents, improving traffic management, and developing Intelligent Transport Systems (ITS). With India experiencing a high number of traffic-related fatalities each year, the deployment of V2X systems aligns well with the national goal of 'Vision Zero'—a future with zero road fatalities.

In addition to ground-based innovations, NFAP 2025 introduces significant changes in spectrum allocation for High Altitude Platform Stations (HAPS). These platforms operate in the stratosphere and can deliver broadband over vast areas. In India, HAPS are being considered for various applications, including rural broadband coverage, disaster recovery, broadcasting, temporary event connectivity, and as redundancy networks for terrestrial backhaul.

However, earlier efforts to commercialise HAPS were impeded by technical and regulatory challenges. Many previously identified bands, such as the 28/31 GHz band, were region-specific and lacked harmonisation. This made it difficult to achieve cost-efficient global deployment, and operators often faced complex interference mitigation requirements between fixed-satellite services and terrestrial systems. Additionally, higher mmWave bands like 38 GHz and 47/48 GHz—though identified for HAPS—are vulnerable to rain attenuation, especially in tropical regions like India, thereby limiting coverage and service reliability.

Recent global regulatory developments have sought to address these issues. At WRC-19, the 31–31.3 GHz and

The roadmap strengthens mid-band IMT and satellite spectrum, signalling a deliberate pivot to hybrid connectivity for coverage, resilience, and capacity expansion.

38–39.5 GHz bands were globally identified for HAPS, adding to the previously harmonised 47.2–47.5 GHz and 47.9–48.2 GHz bands. Even more significantly, WRC-23 allowed the use of lower IMT bands (700–900 MHz, 1.7 GHz, and 2.6 GHz) for HAPS operations.

These lower frequencies are far less susceptible to weather disruptions and can connect directly to standard mobile devices, eliminating the need for customised user equipment and thereby lowering capital and operating costs. This development marks a turning point in making HAPS a commercially viable and scalable connectivity solution for India.

ENABLING BACKHAUL AND WI-FI WITH E AND V BANDS

The introduction and growth of 5G—and eventually 6G—have led to significant increases in data consumption per site. The co-location of multiple generations of mobile technologies (2G to 5G) on a single physical tower has intensified the demand for high-capacity backhaul solutions. Traditional microwave systems are unable to keep pace with this exponential capacity growth. In response, NFAP 2025 supports the use of E-band (71–76 GHz and 81–86 GHz) for high-capacity point-to-point terrestrial backhaul links. These bands are well-suited for urban environments where quick deployment is essential.

Further, the lower V band (57–66 GHz) has been identified as a potential candidate for delicensing. This move could support the deployment of millions of public Wi-Fi hotspots across India, in alignment with various government programmes promoting digital inclusion. Globally harmonised for Wi-Fi applications, this band provides up to 9 GHz of spectrum, nearly 70 times more than the currently available delicensed Wi-Fi bands. TRAI has supported this move in its recent recommendations on backhaul spectrum.

These spectrum provisions could transform India's last-mile connectivity and support the growth of data-intensive applications such as video streaming, online education, and remote work, especially in Tier II and Tier III towns.

OMISSION OF THE LOWER 6 GHZ BAND RAISES CONCERNS

Despite several forward-looking provisions, NFAP 2025 has drawn criticism for excluding the lower 6 GHz band (5925–6425 MHz), which had been earmarked for Wi-Fi in India's 6G Vision document released in March 2023. A draft gazette notification issued on 16 May 2025 also proposed delicensing this band. However, the final plan makes no reference to it, raising policy concerns.

This absence undermines India's efforts to ensure sustainable and inclusive digital connectivity. Wi-Fi remains the most widely used and cost-effective broadband access method in the country, particularly for indoor and public network usage. Advanced Wi-Fi technologies like Wi-Fi 6E and Wi-Fi 7 rely on wide, contiguous spectrum blocks, which only the lower 6 GHz band can provide.

Without access to this band, India risks falling behind in key areas such as digital education, telemedicine, immersive technologies (AR/VR/XR), cloud gaming, digital twins, and metaverse services—all of which require high-throughput, low-latency connections.

The lower 6 GHz band also holds the key to overcoming the indoor coverage limitations of high-frequency 5G and future 6G networks. With 70–80% of data consumed indoors, relying solely on dense small cell deployments for indoor coverage may prove cost-intensive. Instead, wide deployment of next-generation Wi-Fi technologies, supported by the lower 6 GHz band and a robust fibre backbone, can deliver seamless connectivity across homes, enterprises, campuses, and public venues.

NFAP 2025's silence on this issue not only contradicts earlier policy directions but also casts uncertainty on India's long-term innovation and broadband strategy. The lack of clarity may delay the rollout of next-gen Wi-Fi, curtailing digital inclusion and hindering socio-economic progress. 🌐

The author is Hon. FIET (London) & President of Broadband India Forum.

(Views are personal.)

Research inputs by Debashish Bhattacharya.

feedbackvnd@cybermedia.co.in

Trusted photonics: Securing India's optical backbone

India needs a trusted photonics framework to prevent foreign components from becoming hidden points of failure across digital and defence communications.



BY DR JAIJIT BHATTACHARYA, RANJAN KHANNA & DIPANJAN GHOSH

India's digital and strategic transformation is progressing at a scale and speed few countries have experienced. National programmes such as BharatNet, the rollout of 5G networks, and the digitisation of defence communications are reshaping how the state, economy, and society function.

Beneath these visible layers of connectivity lies an often-overlooked foundation: photonics. Optical fibre, optical fibre preforms, and active optical components such as transceivers form the physical layer on which India's digital economy and emerging network-centric

military capabilities depend. Despite their centrality, these components remain largely imported and insufficiently verified.

IMPORT DEPENDENCE WEAKENS TRUSTED PHOTONICS

India today depends on external suppliers for over 70% of its optical fibre preforms, with imports concentrated primarily from China. Optical transceivers are almost entirely sourced from abroad. Regulatory and customs classifications have compounded this dependence by treating active optical transceivers as "parts" rather

If India cannot trust its optical layer, it cannot trust Digital India. Photonics is the un-seen frontier where security, uptime, and sovereignty collide.

than a complete communication apparatus, enabling duty-free imports and weakening incentives for domestic manufacturing.

The result is a structural vulnerability that goes well beyond trade balances. It raises a fundamental strategic question: can India's digital and defence ambitions rest securely on infrastructure whose most critical physical inputs are externally controlled and not fully trusted?

The answer becomes clearer when examined through the lens of modern warfare and strategic competition. Military doctrine worldwide has shifted toward network-centric operations, in which operational effectiveness depends on uninterrupted, real-time data exchange among sensors, command centres, and deployed assets. India's own defence architecture reflects this shift.

Fibre-based backbones and secure communication networks now underpin command, control, intelligence, surveillance, and reconnaissance functions. In such an environment, the integrity of the physical communication layer is not a technical footnote. It is a strategic determinant.

Even marginal degradation in optical performance can produce disproportionate operational consequences. Small increases in signal attenuation can reduce network reach, increase dependence on repeaters, and compromise latency-sensitive applications. In geographically challenging regions, including mountainous border areas, fibre repair and replacement are complex, time-consuming, and costly. Long-term reliability, therefore, becomes as important as initial performance.

FOREIGN OPTICS RISK DEFENCE AND CIVILIAN GRIDS

International experience underscores these risks. Several advanced economies have restricted the use of certain foreign-sourced optical components in sensitive networks after identifying concerns related to engineered material degradation, opaque manufacturing practices, and concentrated supply chains. These risks may not surface during initial testing. They often emerge years after deployment, when infrastructure is deeply embedded and difficult to replace.

These concerns are not confined to defence. Civilian critical infrastructure relies on the same photonic foundations. Smart grids use optical fibre for supervisory control and real-time monitoring. Financial systems depend on high-integrity fibre networks for secure, low-latency transactions. Healthcare, emergency response, and public safety platforms increasingly assume uninterrupted digital connectivity.

In each of these domains, the long-term trustworthiness of photonic components directly affects economic stability and public welfare. Dependence on a narrow set of foreign suppliers, therefore, represents a systemic exposure, not merely a commercial preference.

The industrial consequences of this dependence are equally serious. India is the world's second-largest consumer market for optical fibre, yet domestic manufacturers operate at low-capacity utilisation. Imported preforms, often priced below sustainable production costs, constrain domestic value addition. Anti-dumping measures imposed on finished fibre have, in several instances, shifted competitive pressure upstream rather than correcting underlying distortions.

Over time, this has weakened incentives for capital investment in advanced photonic manufacturing and eroded opportunities for high-skill employment in materials science, precision engineering, and process control. Each kilometre of fibre laid using imported critical inputs captures only a fraction of its potential economic value within India, resulting in significant cumulative losses across national infrastructure programmes.

This dependence persists even as the global photonics market enters a phase of rapid expansion. Demand for optical transceivers is being driven by data-centre interconnects for artificial intelligence workloads, dense 5G backhaul networks, and new submarine cable systems. This segment alone is projected to cross Rs 100,000 crore globally by the end of the decade.

India has begun to see the emergence of domestic capability in this area, including local manufacturing initiatives led by globally experienced talent. Yet this

Today's fibre may pass tests—and fail years later. The risk is not speed, but integrity: hidden degradations can become strategic weak links.

capability remains nascent and is immediately exposed to zero-tariff imports, highlighting how narrow the window for building domestic scale may be.

TRUSTED PHOTONICS NEEDS STANDARDS, TRACEABILITY

Against this backdrop, the case for a Trusted Photonics Ecosystem becomes compelling. The objective is not blanket protectionism or reliance on tariffs, which are legally and diplomatically complex. Instead, the focus should be on procurement policy, standards, and supply-chain verification. India already applies trusted-source requirements to active telecom equipment under its national security framework. Extending this logic to core photonic components—optical fibre, preforms, and transceivers—would align security policy with technological reality.

A trusted photonics framework would rest on three interlinked pillars. First, trusted-source certification should ensure transparency in ownership, manufacturing location, and supply-chain routing, reducing exposure to opaque control and state-backed distortions.

Second, performance standards should combine international benchmarks with India-specific requirements for durability and reliability under local environmental conditions, addressing risks that conventional testing may not capture. Third, batch-level traceability would enable long-term monitoring of component performance, allowing early identification of systemic degradation or anomalous failure patterns. Procurement policy is the most effective lever for implementation. Government-funded projects—from BharatNet and defence communications to power-grid modernisation—represent a large and predictable market.

Aligning procurement preferences with verified domestic value addition and demonstrated capability would encourage manufacturers to invest in design depth, process know-how, and quality systems within India. Importantly, procurement classifications must reward genuine capability rather than contractual arrangements that substitute form for substance. In deep-technology sectors such as photonics, capability creation must precede and justify preferential access.

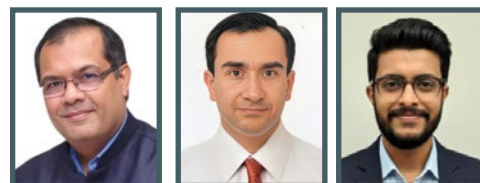
GLOBAL MODELS SHOW NON-TARIFF PATHWAYS WORK

International practice offers useful parallels. The United States' Build America, Buy America (BABA) framework and the European Union's trusted connectivity initiatives rely on procurement rules and standards rather than overt protectionism. These approaches support domestic manufacturing while remaining consistent with international trade obligations. India can adapt similar principles to its own context, leveraging scale, standards, and strategic intent rather than tariffs.

The costs of such an approach are modest compared to the scale of India's infrastructure investments. Incremental increases in component costs are likely to be small relative to the benefits of supply-chain resilience, strategic autonomy, and domestic value capture. The long-term returns—in skilled employment, research capability, and reduced vulnerability to external leverage—extend well beyond immediate financial considerations.

India's digital future is not optional. The question is whether it will rest on foundations that are trusted, resilient, and domestically anchored, or on supply chains shaped by external priorities. Building a Trusted Photonics Ecosystem offers a coherent pathway to align national security, industrial development, and infrastructure reliability.

As network-centric paradigms increasingly define both economic competitiveness and military capability, securing the optical layer is no longer a peripheral concern. It is a strategic choice that will shape India's technological sovereignty for decades to come. 🌐



(From L to R) Dr Bhattacharya is the President of the Centre for Digital Economy Policy Research (C-DEP); Khanna is the Principal Additional Director General in the Directorate General of Export Promotion, CBIC; and Ghosh is Policy Analyst at C-DEP.

feedbackvnd@cybermedia.co.in

[COVER STORY]

6G STANDARDS

METEOROID, METEOR— OR METEORITE?



Release 20 studies are underway, but experts warn 6G may fracture into variants unless interoperability, AI standards, and coexistence are nailed early.

BY PRATIMA HARIGUNANI

What would happen if left-side driving cars ran on the same roads as right-side ones? What if trams did not have dedicated tracks? Imagine the chaos if trains dashed around without all those railroads?

Picture a shoe store with all shoe sizes stacked together without any of those 5, 6, or 7 labels? Take a moment of silence if anyone has shopped for any Ikea furniture without those manuals that tell what goes where.

Sounds strange? No. Scary is more like it. Yeah. And that is exactly why standards matter so much. Even if a technology has become too suave, too futuristic, and too cool for all the nuts-and-bolts paperwork, it helps to have some blueprints. 6G is facing that very moment as the world gears up for this big meteoroid sitting somewhere

in the future to actually make its way into the telecom universe. Whether it lands well on the concrete set up by 5G and 5G SA, or just passes by—that is a question still hanging out there.

WHY STANDARDS MATTER NOW?

It is a major once-in-a-decade meteor heading towards the industry. The 6th-generation wireless technology, 6G, that will succeed 5G is imminent and inevitable.

As of now, 6G seems to be in the early stages of standardisation, with major groundwork being done by 3GPP, ITU, IEEE, ETSI, and the O-RAN Alliance. The rough calendar mark here is 2030, with specifications solidifying in 3GPP Releases 19–21. The scope of 3GPP Release 20 has been outlined, entailing the official technical study projects that will focus on foundational wireless technology areas crucial for the 6G Work Items

6G is not just a tech leap—it is a governance test. The next few years will decide how interoperable and scalable future networks will become.



“AI-native 6G needs standards for interfaces and data models, so AI works across vendors, domains, and networks—at a global scale.”

THOMAS VAN BRIEL

Chief Network Architect – Group Technology, Deutsche Telekom



IN BRIEF

- 6G standardisation has entered early execution, with 3GPP, ITU, IEEE, ETSI, and O-RAN working towards the 2030 horizon.
- 3GPP Release 20 study projects have begun and are expected to be completed by June 2027, shaping the path to Release 21 work items.
- Experts expect peer analysis through 2026, with key calls on spectrum, air interface, and interworking across 4G/5G/Wi-Fi and IoT.
- I-native 6G needs coherent standards for interfaces and data models to ensure cross-vendor interoperability and autonomous operations.
- O-RAN and 3GPP are likely to coexist in 6G: an O-RAN study suggests 86% expect mixed deployments, not pure 3GPP networks.
- India's Bharat 6G Mission aims to influence global frameworks—interoperable, secure, and scalable—while building domestic R&D and IP.

expected in the subsequent standard, 3GPP Release 21. Release 20 has begun and is expected to be complete by June 2027.

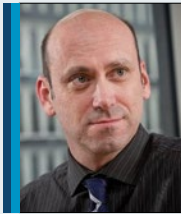
6G has yet to be defined and standardised, reminds Thomas van Briel, Chief Network Architect at Group Technology of Deutsche Telekom. “Standardisation is helping to provide global scale to any mobile communications system. 3GPP, IETF, TM Forum, O-RAN Alliance, and other standardisation bodies are already working under the ITU 2030 horizon to prepare the 6G standards.”

Technical studies that kick-start the 6G standardisation process only got underway in August–September 2025; it will take more than a year of peer analysis by major tech vendors before the main standards bodies will be able to decide on key issues such as spectrum requirements, air interface protocols, and handover to other standards—such as 4G, 5G, Wi-Fi, Zigbee, and Bluetooth—augurs Andrew Kitson, Director, Technology, BML.

Briel underscores the importance of standardisation. “To enable native and large-scale adoption of AI within 6G, a coherent set of standards is required—particularly for interfaces, data models, and data translation. Such standardisation is critical to ensuring that AI can be seamlessly integrated, interoperable across vendors and domains, and effectively leveraged for intelligent, autonomous, and adaptive 6G network operations,” Briel argues.

Pinkesh Kotecha, MD and Chairman of Ishan Technologies, echoes that thought while introducing the indigenisation angle. “For 6G, standardisation will play a big role in deciding whether India builds long-term capability or continues to rely on imported technologies.”

Kitson opines that the process may well be much more difficult this time around, as any contributions made by mainland Chinese technology companies would need



“6G standard studies began in late 2025; it will take a long peer analysis before bodies decide on spectrum, air interfaces, and multi-standard handovers.”

ANDREW KITSON

Director, Technology, BMI

to be scrutinised in exceptionally fine detail in light of current geopolitical tensions. “BMI does not expect the 6G standard to be formalised before late 2027/early 2028, and it may well be that—as was the case with 3G—several different 6G standards will emerge.”

BMI does not have the scope to assess the technical parameters of communications standards. Kitson adds a disclaimer that his answers might be superficial and somewhat pessimistic as they are based on limited insights into 4G and 5G deployments disclosed by network operators. “However, generational standards have always tended to be overhyped and under-deliver.”

WHAT 5G GOT WRONG, 6G MUST FIX

6G is like the fastest lane on the communication highway of this decade. With the right steering skills and timely indicator lights, the industry can make sure it is a happy switch. But for that, it has to look in the rear-view mirror a bit.

Previously, there have been gaps highlighted in industry concerns around 5G specifications, especially related to rigidity, integration and interoperability hassles, roaming-related struggles, multi-vendor compatibility, and the problem of being stuck in siloes. Too many prescriptions for architecture, rather than maintaining focus on functional requirements, have also been pointed out as an area where 5G standards became clunky and hindered deployments.

Also, in the next Generation Research Group (nGRG), a task force within the O-RAN Alliance, 86% believe there will be a mix of O-RAN components alongside 3GPP and legacy deployments. In contrast, only 14% believed that the 6G mobile network will be only 3GPP-based.

3GPP and O-RAN coexistence—as explained further in the study—can be achieved by having 3GPP standardise 6G networks and O-RAN complement 3GPP with additional standardisation; hence, it is expected that 6G networks will include O-RAN components alongside 3GPP deployments.

INDIA’S AMBITION HINGES ON THE RULEBOOK

Equally important is alignment between spectrum policy, standards, and local engineering capability, Kotecha contends. “Without this, 6G networks risk becoming fragmented and difficult to scale beyond dense urban centres, which would limit their impact in a country like India, where affordability and nationwide reach matter as much as peak performance.”

He adds that AI will be a key differentiator in this evolution. “Unlike 5G, where AI is largely applied to network optimisation and operations, 6G is expected to embed AI more deeply into network design itself, shaping how radio resources are allocated, how networks self-optimize, and how services are orchestrated end-to-end.”



“6G standardisation must move faster. Hardware refresh cycles and government concerns will take time, but early rules will drive telecom innovation.”

SANJAY SEHGAL

CEO & MD, TP-Link India



“For India, 6G standards will decide whether we build long-term capability and IP—or stay dependent on imported technologies and ecosystems.”

PINKESH KOTECHA

MD & Chairman, Ishan Technologies



With the world moving towards impending smart connectivity, IoT, and AI/ML-based controls, better connectivity is the need of the hour, and 6G standardisation should be implemented sooner rather than later, stresses Sanjay Sehgal, CEO and MD, TP-Link India.

“Since the total roll-out will take time, about standardisation (3GPP) and various governments having their concerns, and the fact that the software and hardware will need to be refreshed. All said, this will lead to more innovation in the field of IT and telecom.”

THE LONG RUNWAY TO 2030 BEGINS NOW

Note that India is very ambitious about this jump. The Bharat 6G Mission shows how the 6G roadmap envisions the sector bringing in nearly USD 1.2 trillion to the national GDP by 2035, with the country targeting 10% of global 6G patents. A joint declaration on the 6G Principles was also released on 10 October 2025.

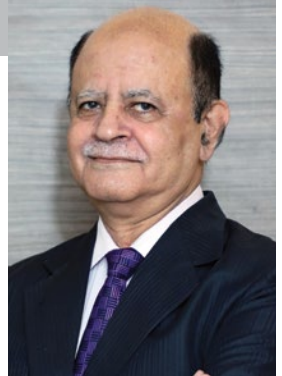
Kotecha points out that, as outlined in the Bharat 6G Vision, India's approach is to actively shape global standards. Hence, future networks remain interoperable across vendors, secure by design, and economically scalable. “The goal is not to create parallel or localised standards, but to influence global frameworks while building domestic R&D depth, developing home-grown intellectual property, and preparing the ecosystem for large-scale deployment. Getting standardisation right at this stage will ultimately determine how open, interoperable, and future-ready India's 6G networks are.”

Let us hope that 6G turns out to be a star that the industry can all make big wishes upon. If not anything else, at least a Chicxulub that kills the dinosaurs of this industry. And only the dinosaurs. 🦖

pratimah@cybermedia.co.in

LT GEN DR SP KOCHHAR

BEYOND UPTIME: REDESIGNING TELECOM FOR DISASTERS



India is shifting from post-crisis restoration to engineered resilience—hardening sites, ring fibre, hybrid power, satellite backup, and PPDR.

Telecom networks have quietly become India's most critical safety net. In every flood, cyclone, or landslide, people instinctively reach for their phones to seek help, locate family, and access essential services, turning connectivity into a lifeline for citizens and a core instrument of national security and disaster response.

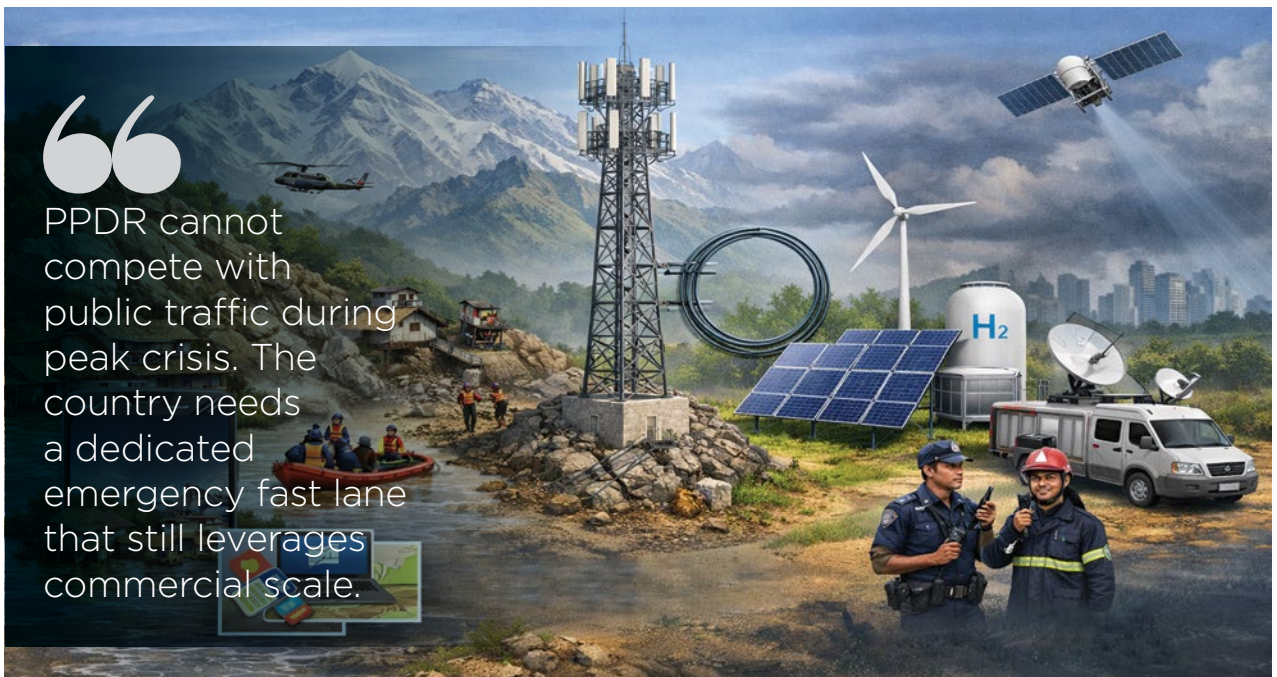
Over the past few years, there has been a clear policy shift in that direction. The Department of Telecommunications, working with the Coalition for Disaster Resilient Infrastructure, has put in place a Disaster Risk and Resilience Assessment Framework that maps the vulnerability of towers, fiber, and power

in high-risk states such as Odisha, Uttarakhand, Assam, Tamil Nadu, and Gujarat.

The assessment speaks in the language of cyclonic wind speeds, storm surges, landslides, and earthquakes because that is the operating environment for the networks. For the industry, this means moving from “best effort uptime” to networks that are deliberately designed for resilience under stress.

LESSONS FROM RECENT DISASTERS IN INDIA

Recent disasters have shown both how far the sector has come and what remains to be done. During the Tripura floods in August 2024, unprecedented rainfall and swollen



Tripura proved that services can be restored quickly—if the necessary roaming, permissions, spares, and SOPs are in place before the disaster hits, not after.



IN BRIEF

- DoT's resilience framework maps tower, fibre, and power risks in high-risk states, shifting networks from reactive repair to planned resilience.
- Tripura floods (Aug 2024) demonstrated rapid recovery when roaming, validity relief, and real-time coordination are built into SOPs.
- Uttarakhand landslides (2025) exposed Himalayan fragility—resilience there demands hyperlocal designs and logistics-backed restoration.
- Infrastructure hardening and redundancy are central: higher wind-load towers, seismic compliance, and diverse ring fibre routes reduce failures.
- Power backup is being redesigned: diesel dependence is giving way to solar-battery hybrids and pilots like hydrogen for longer clean autonomy.
- Satellite links and PPDR planning are becoming essential for the “worst day”, when public networks cannot carry emergency traffic reliably.

rivers damaged roads, power lines, and telecom sites across multiple districts. Within a few days, more than 94% of telecom services were restored as operators worked with the Department of Telecommunications and the State administration to replace equipment, reroute traffic, and

keep people connected. Intra-circle roaming was activated so subscribers could latch on to any available network, prepaid validity was extended, and relief workers could coordinate food, shelter, and medical aid.

The response to the 2025 Uttarakhand cloudburst and landslides was even more intense. Entire towers were washed away in the Bhatwadi–Gangotri belt, and fiber routes snapped at several locations, leaving entire valleys dark in a matter of minutes. Restoration required the Army and ITBP to airlift optical fiber cables, set up temporary routes, and coordinate closely with the State Disaster Management teams before even basic connectivity could be brought back. Experiences like these make it clear that resilience in the Himalayas looks very different from resilience on the Odisha coast and that planning has to be hyperlocal.

Seen together, these events underline a simple truth. When good frameworks, permissions, and coordination exist, operators can and do move on a war footing. The task now is to embed that level of responsiveness into how networks are designed and run every day, rather than waiting for the next red alert.

HARDENING INFRASTRUCTURE AND BUILDING REDUNDANCY

From the industry's perspective, resilient telecom rests on a few clear pillars. The first is infrastructure hardening and redundancy. Towers in cyclone-prone belts need to be engineered for higher wind loads and storm-surge risks, while towers and exchanges in seismic zones must comply with appropriate structural standards.

Critical fiber routes should not be single points of failure and increasingly are being built in ring topologies with diverse paths, often using underground ducts for extra protection. The BharatNet programme, which has laid lakhs of kilometers of optical fiber and connected over two lakh gram panchayats, plays a quiet but central role here, as rural backhaul depends on its robustness.

POWER BACKUP: FROM DIESEL TO HYBRID RESILIENCE

The second pillar is power resilience. India's tower ecosystem has historically relied on diesel generators,

Resilient telecom is now designed like critical infrastructure: wind-load towers, ring fibre routes, and protected backhaul, not patchwork.

which are both expensive and environmentally challenging, especially during prolonged grid outages after a cyclone or flood.

Regulatory nudges and operator commitments are now pushing these sites toward hybrid solutions that blend grid power, solar panels, advanced battery storage, and, in some pilots, hydrogen fuel cells that can offer longer, cleaner backup. Large tower companies already report thousands of “diesel-free” sites, and the share is growing, although there is still a long way to go before backup power is no longer a weak link in disaster response.

SATELLITE REDUNDANCY AND PPDR COMMUNICATIONS

Third comes redundant connectivity through satellite and dedicated public protection and disaster relief networks. When roads are cut off and towers are lost completely, a satellite link is often the only way to get voice and data out of a district. Fixed VSAT terminals and satellite phones at Emergency Operation Centres, set up with National and State Disaster authorities, have already shown their value in hill states and remote regions.

At the same time, India is working toward next-generation Public Protection and Disaster Relief (PPDR) systems so that police, fire, ambulances, and other first responders do not have to compete with public traffic when every second counts. Proposals for a shared 4G and 5G network on suitable spectrum for PPDR use can create a dedicated fast lane for emergency communications while leveraging commercial infrastructure for scale economics.

CYBER RESILIENCE THROUGH TESTING AND ASSURANCE

The fourth pillar is digital and cyber resilience. As networks become software-defined and cloud native, with 5G cores, open interfaces, and API exposure, the security threat surface also expands. India has responded by building its own security assurance regime through Indian Telecom Security Assurance Requirements and an indigenous testing and certification ecosystem.

The recognition of the IIT Madras Pravartak lab as the first authorised facility to test 5G core network functions is a strong signal that the country intends to secure its

networks on its own terms. Complementing this is the evolution of telecom cybersecurity rules that define how incidents are reported, how identifiers are validated, and how different agencies collaborate to combat fraud and attacks.

GOVERNANCE, SOPs, AND MASS ALERT READINESS

Standard operating procedures now require round-the-clock control rooms at the Department of Telecommunications during major events like cyclones and set expectations for fuel reserves, emergency teams, and intra-circle roaming among operators. Nationwide testing and rollout of an indigenous cell broadcast system and the SACHET integrated alert platform have created a reliable way to reach millions of citizens quickly on any handset. These policy instruments may look technical, but on the ground, they translate directly into faster warnings, clearer coordination, and saved lives.

Looking ahead, there is an opportunity for India not just to be the world’s largest data market but also to become a reference model for disaster-ready, security-resilient digital infrastructure. By 2030, the aim should be that whenever the next major cyclone hits the east coast, or a cloudburst strikes the Himalayas, connectivity for citizens, first responders, and critical services is restored swiftly and predictably. Getting there will require sustained investments, supportive policies, smarter risk sharing, and continuous learning from every event.

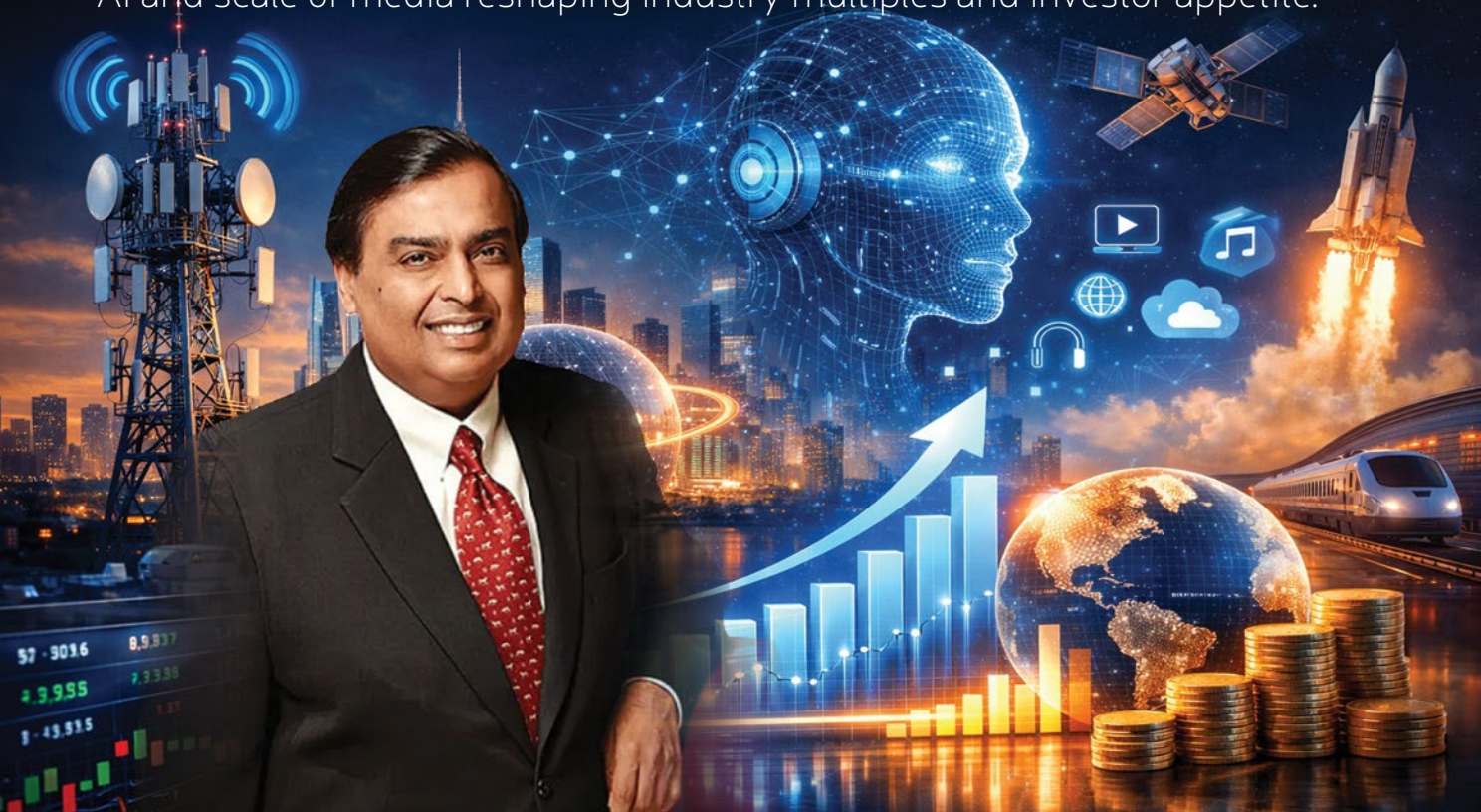
For citizens, the test of success is simple. In their moment of greatest need, their phone should work. For the industry and for policymakers, that simple expectation is becoming the guiding principle. Resilient telecom networks will not just carry voice and data, they will carry trust, stability, and the confidence that India can face crises without losing its digital heartbeat. 🌟

The author is a decorated military veteran who retired as the Signal Officer-in-Chief, the head of the Indian Army’s ICT division. He was also the first CEO of the Telecom Sector Skill Council and is the Director General of the Cellular Operators Association of India (COAI).

feedbackvnd@cybermedia.co.in

Can the techco pivot drive Reliance Jio's USD 170 B bid?

Reliance Jio IPO will test whether telecom can be valued as a platform, with AI and scale of media reshaping industry multiples and investor appetite.



BY JAIDEEP GHOSH

The impending Initial Public Offering (IPO) of Reliance Jio Infocomm (Jio), tentatively scheduled for 2026, is not merely a capital markets event; it represents a structural inflection point in the history of corporate India. With investment bankers and analysts proposing a valuation range between USD 130 billion and USD 170 billion, the listing is poised to be the largest in the country's history, potentially eclipsing the market capitalisation of established giants such as Bharti Airtel and challenging global telecommunications benchmarks.

However, viewing this solely as a telecom listing provides a limited perspective. The narrative Reliance Industries Limited (RIL) is constructing—and asking

the market to underwrite—is a transition from a 'Telco' (utility connectivity provider) to a 'Techco' (digital ecosystem platform).

This pivot is anchored in what Morgan Stanley describes as 'Monetisation 4.0'. The phase is characterised by the simultaneous maturation of deep-tech investments, large-scale AI infrastructure deployments, media consolidation through the Disney (Star/Hotstar) merger, and a decisive shift in capital allocation—from aggressive capex to sustained free cash flow (FCF) generation.

For the first time in three decades, all three of RIL's growth engines—Energy, Retail, and Telecom—are projected to be FCF positive simultaneously by 2026.

Jio's IPO narrative fuses AI ambition, media control, and network scale into a platform story that few global telecom majors can credibly claim today, too.

THE INDIAN IPO ENVIRONMENT: LESSONS FROM 2024-2025

While 2025 surpassed 2024 with record fundraising of over USD 20 billion, liquidity during the period was highly selective. The Indian bourse has evolved from speculative exuberance to more discerning capital allocation. Three distinct archetypes of listings emerged, offering important lessons for Jio.

#1

HYUNDAI MOTOR (THE AGGRESSIVE INCUMBENT)

As the largest IPO of its time at USD 3.3 billion, Hyundai Motor India was expected to be a bellwether. Instead, it was listed at a discount. The structural flaw was a pure Offer for Sale (OFS) combined with 'perfection pricing', which left no upside for investors. The market delivered a clear signal—even for dominant incumbents, it is unwilling to pay a valuation that captures all future gains on day one.

Implication for Jio: Reliance must avoid the 'Hyundai trap'. A USD 170 billion valuation is ambitious; if priced to perfection, it risks a muted response irrespective of brand strength.

#2

LG ELECTRONICS (THE VALUE MULTINATIONAL)

In stark contrast to Hyundai, the listings of LG Electronics India and Tata Capital in 2025 demonstrated the market's appetite for reasonably valued, high-governance assets. LG Electronics India saw a 50% surge on debut, driven by scarcity premium and reasonable pricing. The key driver was scarcity premium—given the limited presence of listed consumer durable MNCs of this scale—combined with a valuation that appeared to be optically cheaper than that of contract manufacturers such as Dixon Technologies or Voltas.

Implication for Jio: To mirror LG's success, Jio must emphasise its scarcity value while ensuring pricing leaves visible upside for public market investors. Articulating its Techco identity clearly will be central to this positioning.

#3

TATA CAPITAL (THE CONGLOMERATE COMPOUNDER)

The Tata Group's financial services arm's Rs 15,511 crore



IN BRIEF

- Jio's 2026 IPO is positioned as a structural shift, not a routine telecom listing, testing India's appetite for platform-scale digital assets.
- The USD 170 B valuation hinges on repositioning Jio from a utility telco to a techco spanning AI, media, cloud, and connectivity.
- IPO lessons from Hyundai, LG, and Tata Capital highlight the risks of perfection pricing and the power of scarcity and governance.
- Jio's Standalone 5G, AirFiber scale, and enterprise bundling form a durable connectivity moat beyond consumer ARPU.
- The Nvidia-backed sovereign AI strategy aims to monetise intelligence, not bandwidth, across India-specific use cases.
- JioStar's control of premium sports and content strengthens pricing power, churn control, and long-term platform economics.

IPO saw robust subscription (1.95x overall) and a stable listing. This underscored the deep trust institutional investors place in conglomerate-backed NBFCs with clean loan books and clear ownership structures.

Implications for Jio: Jio can draw on Reliance's conglomerate halo, but must also recognise the inevitable holding-company discount. Transparency, governance

Unlike past mega listings, Jio's market test hinges less on subscriber growth and more on how convincingly it sells long-term digital relevance at scale.

clarity, and capital discipline will be critical in sustaining investor confidence post-listing.

STRUCTURAL TRANSFORMATION: FROM TELCO TO TECHCO

Jio's USD 170 billion valuation ambition sits uneasily with traditional telecom benchmarks. Global telcos typically trade at 6–8x EV/EBITDA. To justify a multiple closer to 15–18x, Jio is deliberately decoupling its identity from that of a regulated utility and repositioning itself alongside global technology platforms.

If valued strictly as a telco, Jio might command USD 80–90 billion. It is the addition of the 'AI Premium' and the 'Media Monopoly Premium' that bridges the gap to the USD 170 billion target. Jefferies has already rolled forward its valuation to FY27, estimating an Enterprise Value (EV) of USD 180 billion based on this sum-of-the-parts 'techco' logic.

Global private markets in 2025 provide a useful reference point. The AI supercycle has driven benchmark

valuations to unprecedented levels, with OpenAI reportedly valued at USD 500 billion and SpaceX, anchored by Starlink, approaching USD 800 billion. If valued strictly as a telco, Jio is on that path toward a high valuation (see the table Global Private Market Valuation Benchmarks Vs Reliance Jio).

Jio's narrative synthesises three interlinked pillars. The first is an infrastructure moat (like SpaceX), built around what is positioned as the world's largest private data network spanning 5G and fibre.

The second is an intelligence layer (like OpenAI), centred on sovereign AI models and AI-as-a-service capabilities developed in partnership with Nvidia. The third is control over media and attention (like ByteDance), reinforced by unrivalled content dominance through the JioStar platform. Together, these elements underpin Jio's attempt to be valued not as a telco, but as a converged digital platform.

THE 'JIOBRAIN' AND THE NVIDIA ALLIANCE

Reliance has correctly identified that in a post-5G world,

IPO ARCHETYPES (2024–25) AND STRATEGIC LESSONS FOR JIO

IPO Archetype	Representative Cases	Key Characteristics	Outcome	Strategic Lesson for Jio 2026
The Aggressive Incumbent	Hyundai Motor India (USD 3.3 B OFS)	Pure OFS, Full Valuation, Mature Sector	Discounted Listing; Tepid Institutional Demand	- Avoid 'priced to perfection' valuations. - Ensure the 'growth' narrative overpowers the 'exit' narrative.
The Value Multinational	LG Electronics India (USD 1.3 B)	MNC Brand, Scarcity Premium, Reasonable Pricing	+50% Listing Gains; Valuation > Parent Co.	- Leave money on the table to generate retail frenzy. - Leverage the 'market leader' scarcity premium.
The Conglomerate Compounder	Tata Capital (Rs 15,512 Cr)	High Trust, Clean Governance, Sector Growth	Stable Listing; Strong QIB Support	- Highlight governance standards and RIL ecosystem stability to court long-term pension/sovereign funds.
The Profitable Platform	Meesho (USD 600 M)	Asset-Light, Path to FCF, Digital Scale	+95% Post-Listing Rally; Valuation Re-rating	- Emphasise the 'Platform' nature of Jio (Commerce + Ads + Cloud) over the 'Telco' nature to command tech multiples.

SEBI's relaxed dilution rules reshape the IPO equation, enabling Jio to engineer scarcity and pricing power instead of flooding markets with new paper.

connectivity is a commodity, but intelligence is value-added. The partnership with Nvidia is the cornerstone of this strategy.

On the infrastructure front, Jio is constructing a gigawatt-scale, AI-ready data centre in Jamnagar designed to house Nvidia's latest GH200 Grace Hopper Superchips.

The strategic thesis is 'sovereign AI'—unlike global LLMs trained primarily on English datasets, Jio is building foundational models on India's diverse linguistic corpus. This unlocks 'AI-as-a-Service' for Indian use cases, such as vernacular voice banking, multilingual customer service, or agricultural advisory, where US-centric models remain structurally constrained.

Internally, 'JioBrain' is being deployed to automate network planning and customer support, decoupling revenue growth from headcount growth and strengthening operating leverage.

THE CONNECTIVITY MOAT: 5G AND AIRFIBER

While AI represents the future, connectivity remains the cash engine. Jio has consolidated leadership with over 506 million subscribers as of late 2025. A core differentiator is its capital-intensive Standalone 5G (SA) architecture.

In contrast to Airtel's Non-Standalone (NSA) path, Jio's SA network enables network slicing—dedicated virtual networks for enterprise customers—creating a clearer path to monetisation beyond consumer ARPU.

The second pillar is AirFiber. Fixed Wireless Access (FWA) has effectively solved the last-mile bottleneck,

allowing Jio to capture an estimated 75–80% share of the FWA market and add significant wireline subscribers through late 2025. This expands the 'home broadband' funnel, typically associated with higher ARPU and lower churn than mobile prepaid.

Jio's enterprise push further deepens this moat. Through its Microsoft Azure partnership, JioBusiness bundles cloud and connectivity, reducing digitisation barriers for MSMEs. This segment is expected to be a primary driver of the 18% revenue CAGR forecast through FY28.

THE MEDIA MONOPOLY

The merger of Viacom18 and Disney's India assets into JioStar creates an unrivalled media hegemon. By combining Star India's linear distribution strength with JioCinema/Hotstar's digital dominance, the entity controls an estimated 35–40% of viewership and nearly 70% of premium advertising inventory.

More importantly, with rights to the IPL and ICC tournaments, JioStar has cornered cricket—the single most valuable asset in Indian media—granting extraordinary pricing power with advertisers.

For the IPO narrative, JioStar serves as both a retention engine (reducing churn) and an indirect tariff lever, by shifting premium content behind paywalls and normalising higher consumer spending.

VALUATION ANALYSIS: AIRTEL VS. JIO

The primary pushback against Jio's USD 170 billion valuation is the comparison with Bharti Airtel. The arch-

GLOBAL PRIVATE MARKET VALUATION BENCHMARKS VS. RELIANCE JIO

Company	Core Competency	Valuation/Market Cap	Revenue Multiple
OpenAI	AI Foundation Models	USD 500 B – 750 B	~167x (on USD 3 B revenue)
SpaceX	Satellite Internet (Starlink)	USD 350 B – 800 B	~20–25x
ByteDance	Algorithmic Media (TikTok)	~USD 300 B	~2x (on USD 155 B revenue) but high profit
Bharti Airtel	Telecom Connectivity	~USD 143 B (Rs 12.7 T)	~8–10x EV/EBITDA
Reliance Jio	Integrated Telecom & Techco	Target ~USD 170 B	Target: 15–18x EV/EBITDA

The real valuation debate is not Jio versus Airtel, but whether Indian capital markets are ready to price telecom as national digital infrastructure soon.

COMPARATIVE FINANCIAL METRICS: JIO VS. AIRTEL (ESTIMATED FY25/26)

Metric	Reliance Jio (Projected)	Bharti Airtel (India)	Observation
Subscriber Base	~506 Million	~450 Million	Jio leads in pure volume, critical for platform monetisation.
ARPU (Rs)	Rs 211	Rs 256	Airtel wins in premiumisation; has scope for tariff increase.
5G Strategy	Standalone (SA)	Non-Standalone (NSA)	Jio has higher initial Capex but lower ongoing migration costs.
Broadband Share	~50% Market Share	~25–30%	Jio dominates home broadband via Fiber and AirFiber.
ROCE	~9.4%	~11.6%	Airtel is currently more capital-efficient, but Jio's 2026 FCF projections may reverse that.
Valuation	USD 170 B (target)	USD 143 B (listed)	Jio's premium prices in the 'Media monopoly' and 'Techco' shift.

rival Airtel typically trades at a premium due to its 'quality' subscriber base and higher ARPU (Rs 256 versus Jio's Rs 211) [see Comparative Financial Metrics: Jio vs. Airtel (Estimated FY25/26)].

Investment bankers, however, argue that Jio deserves a premium based on its future trajectory. First, Jio's capex cycle is peaking, with its 5G rollout largely complete, whereas Airtel still faces elevated spending to transition from NSA to SA. This implies Jio will generate stronger free cash flow in FY26–28.

Second, a structural tariff hike is widely anticipated in late 2025 or early 2026. While Jio has historically played the price warrior, the IPO creates an incentive to lead tariff hikes, improve the P&L profile, and reframe the market's valuation lens.

REGULATORY TAILWINDS AND STRATEGIC OUTLOOK

The regulatory landscape offers bespoke advantages. Recognising the liquidity risks of a mega-IPO, SEBI has amended its rules for issuers with a market capitalisation above Rs 5 lakh crore (USD 60 B+).

The minimum public offer (MPO) requirement has been reduced from 10% to 2.5%, while issuers have been

granted up to 10 years to reach the 25% minimum public shareholding threshold.

This allows Reliance to list Jio with a float of roughly USD 4.3 billion, rather than a market-disrupting USD 17 billion. The reduced float improves price discovery and reinforces a 'scarcity premium', supporting stronger demand dynamics.

The 2026 IPO of Reliance Jio is poised to be the coronation of India's premier digital infrastructure asset. The USD 170 billion valuation is based on a perfect execution of the 'techco' pivot and successful media integration. To succeed, Jio must convince investors it is not a utility piping data, but a platform processing intelligence and commanding attention.

With SEBI's favourable framework and a supportive global appetite for tech assets, the stage is set. However, sustained ARPU growth amidst a competitive duopoly remains the key risk. Ultimately, the IPO will test—and potentially validate—Reliance's strategy of building a dominant digital ecosystem, cementing Jio's leadership in India's next-gen landscape. 🍌

*The author is a former Partner at KPMG in India.
Views are personal.*

feedbackvnd@cybermedia.co.in



DATAQUEST JANUARY 2026 EDITION: ENTERPRISE TECHNOLOGY PREDICTIONS 2026

ALSO READ MORE ON

- How AMD is shaping the future of AI Compute - Jaya Jagadish, AMD India
- India's Third Tech Wave: Tech Predictions for 2026 Through an Impact Lens
 - Tiny AI: The New Oxymoron in Town, Not Really!
- Why 2026 Will Force Indian Enterprises to Rethink Data, AI, and Infrastructure Strategy
 - Coforge-Encora and the AI-Driven M&A Pivot in Indian IT
 - Ten Tech Trends for 2026
- Identity is the new must have security perimeter for Indian enterprises
- Abhishek Gupta, SailPoint



Scan QR Code
& Subscribe now...

DATAQUEST 40+ YEARS CELEBRATIONS:
GET 40% EXCLUSIVE DISCOUNT ON
DATAQUEST PRINT SUBSCRIPTION
AND DATAQUEST DIGITAL
SUBSCRIPTION AT FLAT 420/- ONLY.
AVAIL THE OFFER NOW

<https://shorturl.at/vn6tN>

**FOLLOW DATAQUEST FOR REGULAR
AND LATEST UPDATES ON THE
BUSINESS OF ICT ECOSYSTEM.**



Dataquest



dataquestindia

Leverage Dataquest platform & network

Ajay Dhoundiyal | ajaydh@cybermedia.co.in | +91 99535 40318



#ImpactingICTfor4Decades

For Subscription queries:



subscriptions@cybermedia.co.in



9289870545



AWS custom silicon: turning AI into infrastructure

Purpose-built cloud chips are cutting AI cost and latency—turning GenAI from pilots into scalable infrastructure for Indian enterprises.

SATINDER PAL SINGH

Director, Solution Architecture, AWS India and South Asia

When Zomato processes 10,000 restaurant images a day using AI chips with better price performance and lower latency, it is not just about prettier photos—it is about democratising technology for small businesses across India. A street-side eatery armed with only a mobile phone camera can now compete with upmarket restaurants that rely on professional photography equipment, thanks to image upscaling powered by custom silicon.

*This is the new reality of India's AI revolution: custom chips are no longer the exclusive domain of tech giants, but tools that enable businesses of every scale to compete on innovation rather than capital. **Satinder Pal Singh**, Director, Solution Architecture, AWS India and South Asia, explains how AWS's custom silicon strategy is reshaping the competitive landscape—delivering not just incremental gains, but order-of-magnitude improvements in price-performance that are unlocking entirely new categories of*

*AI applications across Indian enterprises. Excerpts from his interaction with **Thomas George**:*

THE EVOLUTION OF CUSTOM SILICON

AWS's journey into custom silicon began more than a decade ago, driven by a clear objective: enabling more workloads to run efficiently on cloud infrastructure. "We started in 2013 with Nitro," explains Singh. "Nitro offloaded hypervisor capabilities and storage and networking functions, allowing customers to run workloads with consistent performance. That really opened up the kinds of workloads that could be supported on the cloud."

This foundation paved the way for Graviton, AWS's Arm-based, general-purpose compute processor, launched in 2018. Now in its fourth generation, with the fifth recently announced, Graviton has achieved significant market penetration. "For the last three years,

The shift is from generic compute to workload silicon—cutting AI unit costs so Indian firms scale use cases, not just experiments.

more than 50% of the compute that we have launched in our regions worldwide has used Graviton,” Singh notes. The latest Graviton4 processor delivers 30% better performance, 50% more compute cores, and 75% more memory than its predecessor.

AI ACCELERATORS: TRAINIUM AND INFERENTIA

The progression from general-purpose computing to AI-specific accelerators reflects AWS’s response to the exponential growth in machine learning workloads. The Trainium family, purpose-built for training AI models, has advanced rapidly. Trainium2 instances deliver approximately 20 petaflops of performance each, while the Ultra Server configuration provides over 80 petaflops in a single unit.

The scale is staggering. “AWS and Anthropic’s Project Rainier uses over 500,000 Trainium2 chips,” Singh reveals. “It is one of the world’s largest AI supercomputers, built entirely on Trainium.” The recently announced Trainium3 Ultra Server delivers 4.4 times the performance, four times the memory, and operates with four times less power, while improving latency—reaching 360 petaflops.

For inference workloads, Inferentia2 delivers 10x lower latency than its predecessor, addressing the critical need for real-time AI applications.

CHOICE ARCHITECTURE: MATCHING CHIP TO WORKLOAD

When asked about comparisons with Nvidia’s H100, Singh emphasises AWS’s philosophy of providing choice rather than promoting a single solution. “Our mental model is to provide choice to our customers. We want to provide the right tool for the job. This broad selection allows customers to choose the right workload and chipset for their needs. In certain cases, it can be Nvidia. In other cases, it can be Trainium or Inferentia.”

This approach reflects a maturing cloud market, where one-size-fits-all solutions are giving way to more nuanced architectural decisions.

INDIA OUTCOMES: PERFORMANCE AND COST AT SCALE

The adoption of custom silicon by Indian enterprises delivers tangible business outcomes. Paytm runs Graviton

on databases powering its payment gateway for real-time transactions, reporting a 30% performance improvement and a 35% cost reduction. Zomato has delivered similar gains through its data lake platform, running Trino and Druid on Graviton2 to improve performance by 25% while reducing costs by 30%.

Perhaps the most compelling example is Zomato’s use of Inferentia for image upscaling. The company maintains a policy against AI-generated images, aiming to present authentic restaurant photos. However, smaller restaurants often lack professional photography equipment. “How do they democratise the technology?” Singh asks. “They used Inferentia for image upscaling, so that the real image looks more appealing to the user.” By processing 10,000 images daily, 50% better price performance and 25% lower latency.

In conversational AI, Gupshup uses Amazon SageMaker and Trainium to cut model training time from days to hours.

MULTIMODAL AND REASONING-INTENSIVE WORKLOADS

The announcement of Nova Omni marks a significant advance in multimodal AI capabilities. “First in the industry, multimodal reasoning capabilities,” Singh emphasises. “You can have video, audio, text, and images as inputs—all four modes—with reasoning on top, outputting either images or text.”

Combined with Trainium3’s performance improvements, these capabilities enable previously impractical use cases. Singh points to a demonstration of real-time video generation using Trainium3, illustrating how improved latency and performance unlock new possibilities.

AGENTIC AI MOVES INTO TRADITIONAL ENTERPRISES

Whilst large digital natives and fintech companies are obvious beneficiaries, Singh also highlights that traditional enterprises are leveraging these technologies. Apollo Tyres offers a striking example. During tyre manufacturing, the “dry cycle time” between curing presses represents underutilised capacity. When problems occur, traditional root cause analysis requires examining millions of data points and coordinating across teams—often a seven-hour process.

Five Questions an Organisation Must Ask Before Choosing Custom Silicon	Red Flags/Actions/ Checks/ Smart Tips
1. What is the real TCO?	
Advertised savings of 30-40% ignore hidden costs. Calculate migration expenses, recompilation time, staff training, and licensing changes. If optimisation takes over 6 months, ROI may not materialise for 2 years.	Extensive custom code optimisation is needed upfront.
2. Is your app compatible?	
ARM architecture (Graviton) is mostly plug-and-play. Java, Python, and Go transition smoothly. Legacy .NET and older databases struggle. Check if your Docker images, libraries, and dependencies support ARM64.	Pilot one non-critical workload first, like current customers did.
3. Do you have the skills?	
Trainium and Inferentia use AWS Neuron SDK, not CUDA. Your ML team needs retraining. Indian enterprises report 3-6 month learning curves. Budget for training or professional services.	Can the team optimise for ARM microarchitecture?
4. What is your baseline?	
Measure before migrating. Track latency (p95, p99), throughput, training time, and cost per 1,000 inferences. Aim for 20%+ improvement to justify effort.	25% latency gain will mean something if the user organisation has baseline metrics.
5. What is your exit plan?	
Custom silicon creates a deeper level of vendor lock-in than standard instances. Can you revert to x86? What if pricing changes? Keep control workloads on standard instances as a hedge.	Avoid proprietary APIs that do not translate to other platforms.
Bottom Line: Start small, measure obsessively, scale when data proves ROI. Treat this as a strategic initiative, not a procurement checkbox.	

Using Amazon Bedrock’s agentic capabilities, Apollo Tyres developed a “Manufacturing Reasoner” that reduced the dry cycle time to 10 minutes. “Think of the impact on dry cycle time and overall equipment effectiveness,” Singh notes. Similarly, DTDC launched DIVA 2.0, an agentic chatbot that helps customers track shipments and obtain pricing information, reporting a 50% efficiency improvement.

PRIME DAY PROOF: INFERENCE AT MASSIVE SCALE

Looking ahead, Singh sees generative AI adoption accelerating across sectors in the next two years. “Whether it is fintech, digital natives, or traditional enterprises, they are seeing the benefits of using generative and agentic AI technologies. We are at very early stages, and with agentic AI, more such use cases will emerge.”

The retail sector offers a glimpse of this future. Amazon’s Rufus, a generative AI shopping assistant, runs on Inferentia. During US Prime Day sales, over 80,000 instances of Inferentia and Trainium powered the experience, handling queries on product choices, reviews, and specifications.

SILICON STRATEGY: CLOUD’S NEXT PLATFORM SHIFT

The custom silicon strategy marks a fundamental shift in how cloud infrastructure is conceived and delivered. By developing purpose-built chips optimised for specific workload types, AWS is not merely competing on price; it is enabling entirely new categories of applications.

For Indian enterprises, this translates into practical advantages: reduced costs, improved performance, and access to capabilities previously available only to the largest technology companies. As Singh concludes, “We are thinking holistically about how to remove undifferentiated heavy lifting that our customers are doing and innovating on their behalf, giving them all the toolsets with the right choice so they make the right decisions.”

In an era where computational efficiency and AI capabilities increasingly determine competitive advantage, AWS’s silicon strategy offers Indian businesses a credible path to innovation at scale. 🌟

thomasg@cybermedia.co.in

Laser nanowire films promise EMI shielding for 6G devices

Glasgow researchers create transparent, flexible silver nanowire films that cut EMI across 2.2–6 GHz, enabling denser radios in future devices.



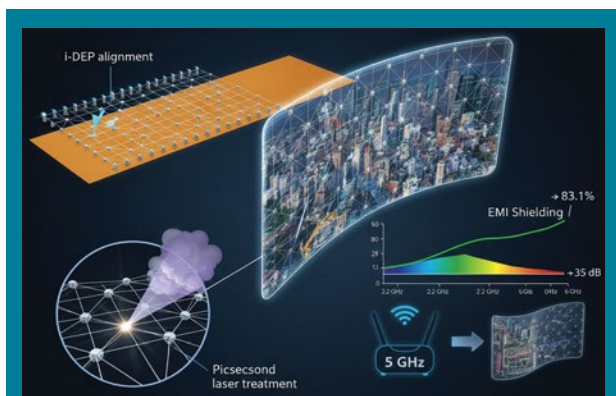
BY SHUBHENDU PARTH

A new nanofabrication method developed at the University of Glasgow could influence how next-generation electronic devices are designed to cope with electromagnetic interference (EMI), especially for upcoming technologies such as 6G wireless communication networks, Wi-Fi systems, radar, and biotelemetry.

Published in the December 2025 issue of ACS Nano, the research outlines a dual-process innovation combining interfacial dielectrophoresis (i-DEP) with non-contact picosecond laser processing to fabricate ultrathin, transparent, and flexible EMI shielding films using aligned silver nanowire (AgNW) networks.

A cleanroom-free, maskless route could let OEMs add EMI shielding without sacrificing thin, transparent form factors in new wireless devices.

Capacitively coupled nanogaps provide an EMI-shielding mechanism beyond conductivity, suggesting smarter passive suppression for dense RF design.



IN BRIEF

- Researchers have developed a dual-step process to build ultrathin, transparent, flexible EMI shielding films using aligned Ag nanowires.
- i-DEP aligns nanowires on polyimide in precise patterns, enabling controlled geometries suited to scalable EMI shielding in compact electronics.
- Picosecond laser treatment fuses nanowire junctions and removes PVP insulation, boosting both conductivity and transmittance.
- Films deliver 46× lower sheet resistance and 10% higher transparency, reaching 83.1% transmittance at 550 nm after treatment.
- Shielding exceeds 35 dB across 2.2–6 GHz, covering Wi-Fi 6/7, mid-band 5G, radar bands, and early 6G use cases.
- Real-world testing shows a 15 dB drop in 5 GHz Wi-Fi signal strength, implying a ~30× reduction in signal power when shielded.

The method provides a solution to a longstanding material challenge—achieving high shielding effectiveness without compromising optical transparency or requiring complex manufacturing steps.

SCALABLE EMI SHIELDING FOR NEXT-GEN WIRELESS DEVICES

As wireless spectrum becomes more crowded and transmission power increases across consumer, industrial, and healthcare domains, EMI shielding has become critical to ensure signal integrity and device safety. Traditional shielding materials, such as metal foils, are rigid, opaque, and unsuitable for modern flexible electronics.

The University of Glasgow's James Watt School of Engineering team, led by researchers at its Microelectronics Laboratory (meLAB), addressed this gap by designing a method that allows nanowires—each a thousand times thinner than a human hair—to be arranged in precise geometries onto thin polyimide (PI) substrates, using electric fields to guide their positioning.

This first step, the i-DEP, uses a non-uniform AC electric field to orient nanowires both translationally and rotationally across predefined patterns. The research demonstrated programmable assemblies spelling out “NANO” and “UOG” to validate directional control.

In the second step, ultrafast picosecond laser pulses were applied to the aligned nanowire films. This laser post-treatment fused junctions between wires and removed residual polyvinylpyrrolidone (PVP) insulating layers, thereby enhancing both electrical conductivity and optical transmittance. Notably, the films achieved a 46× reduction in sheet resistance and a 10% increase in transparency, reaching 83.1% at 550 nm.

Tests showed that the films provide over 35 dB shielding effectiveness across the 2.2 to 6 GHz frequency band. This range includes signals used by Wi-Fi 6/7, mid-band 5G, radar systems, and emerging 6G applications, making the films highly relevant for future-proofing telecom equipment.

The ultra-thin 5.1-micron films can bend and wrap without losing performance—useful for foldables, smart wearables, and curved surfaces.

OVERCOMING THE CONDUCTIVITY-TRANSPARENCY TRADE-OFFS

“This is the first time anyone has overcome the longstanding trade-off between electrical conductivity and optical transparency in metallic nanowire networks,” said Jungang Zhang, lead author of the study. “After our laser post-treatment, both the conductivity and transparency improve simultaneously.”

A core innovation lies in the creation of a capacitively coupled interwire network. The aligned structure leaves nanogaps between wires, forming microscopic capacitors that enhance local electric-field coupling and displacement current. This mechanism contributes significantly to EMI shielding—well beyond the role of conductivity alone.

Compared to randomly oriented drop-cast networks, the aligned and laser-treated films deliver a 1000× improvement in shielding effectiveness. The total film thickness is just 5.1 microns, allowing the films to bend, wrap, and conform to surfaces without loss of performance, making them suitable for wearables, foldable displays, transparent antennas, and implantable medical devices.

USE CASES: FROM WIRELESS HEALTHCARE TO SMART INFRASTRUCTURE

The transparent and flexible EMI shielding material could play a key role in several high-growth telecom-related domains.

- **6G and Wi-Fi 7 base stations:** With higher frequencies and antenna densities, these systems face more cross-talk and need passive EMI suppression at the component level.
- **Transparent user interfaces:** In smart glasses, head-up displays, or foldable phones, display-integrated antennas and sensors require shielding layers that do not block light or interfere with form factor.
- **Wearables and implantables:** Devices for remote patient monitoring, such as ECG patches or

neural sensors, often suffer from interference caused by nearby smartphones or Wi-Fi routers. These films could serve as bio-compatible shielding enclosures.

- **Radar and edge computing:** In automotive or industrial IoT applications, especially those using radar or mmWave communication, the films can prevent performance degradation due to environmental EM noise.

In real-world testing, the researchers demonstrated the material’s effectiveness by blocking a 5 GHz Wi-Fi signal in an anechoic chamber. A mobile phone acting as a hotspot saw a 15 dB drop in signal strength when shielded by the AgNW film, indicating a 30-fold reduction in signal power at that frequency.

ENABLING TELECOM HARDWARE INNOVATION WITHOUT A CLEANROOM

Beyond the material performance, the fabrication approach offers advantages in cost and scalability. The maskless, cleanroom-free laser ablation process enables fast production of customised electrode geometries for large-area nanowire assemblies. The researchers demonstrated prototypes measuring up to 80 cm², with the potential to scale further using roll-to-roll techniques.

“The EMI shielding performance of the materials we created improves on the performance of non-aligned nanowires by more than a thousand times,” said Professor Hadi Heidari, corresponding author and head of meLAB.

The research was funded by the UK’s Engineering and Physical Sciences Research Council (EPSRC), and the team plans to explore integration with multilayered and conductive top-coating systems to further enhance shielding performance in complex electromagnetic environments. 🌟

shubhendup@cybermedia.co.in

From dumb pipes to intelligent telecom platforms

As consumer monetisation plateaus, telcos are shifting from pipes to programmable networks—selling APIs, trust, and outcomes as software platforms.



BY SUNIL DAVID

For decades, the telecom playbook was crystal clear: build networks, add coverage, sell voice and data plans, and optimise cost per bit. But that playbook is running out of runway. Data consumption keeps climbing, network upgrades remain capital-intensive, and consumer monetisation has

natural limits. The result is a global and increasingly Indian pivot: telecom is becoming a software and platform industry.

This transformation is not merely a slogan. It is a structural shift in how networks are engineered, built,

The telecom business is moving beyond pipes. The next revenue layer is software—network APIs that enterprises can consume like cloud services.

“Intelligent platforms” is not jargon: it is how telcos monetise identity, location, and device signals as programmable building blocks for apps.

operated, and monetised. In the platform era, telcos are no longer just connectivity providers. They are turning network capabilities into programmable services—exposed via APIs, embedded into enterprise workflows, and sold through developer ecosystems. That is where the next wave of telecom value is being created, and that is where new monetisation opportunities are emerging in a hyper-competitive marketplace.

WHY THE PLATFORM SHIFT IS HAPPENING NOW

Three forces are converging clearly. First, the economics of connectivity are tightening. Even with strong data growth, the incremental value of “more bandwidth” is harder to monetise purely through consumer plans. Network investments remain substantial, but consumer revenue growth has limits. Telcos, therefore, must look beyond traditional monetisation and identify revenue pools that scale without simply scaling capex.

Second, enterprises increasingly want business outcomes—not just bandwidth. Banking and financial institutions, e-commerce platforms, transportation and logistics players, manufacturers, and healthcare providers are digitising faster than before. What they require from telecom providers is not just connectivity comprising SIMs and telecom pipes, but programmable network capabilities such as identity verification, device intelligence, accurate location-based services, quality-on-demand connectivity for low-latency and high-speed use cases, and secure messaging.

Third, telecom architecture is finally ready. Cloud-native cores, automation, and standardised APIs have reached a point where network functions can be exposed safely and consistently across geographies and operators. GSMA’s Open Gateway framework and the CAMARA open-source API project are central to this shift because they standardise how developers access telco capabilities.

GSMA Open Gateway is a global framework of common network APIs that provides simplified access to mobile providers’ networks. By enabling developers and cloud service providers to use a single access model



IN BRIEF

- Telecom service providers are shifting from bandwidth-led growth to software-led monetisation through programmable network capabilities.
- Enterprise digitisation demands more than connectivity—identity, device intelligence, location, and quality on demand.
- Network exposure via APIs is turning telco assets into reusable software services across industries.
- Open Gateway and CAMARA reduce fragmentation by standardising network APIs across operators and geographies.
- Modern modular OSS/BSS and open architectures are essential for commercialising telecom capabilities, such as software products.
- The winners will sell outcomes—trust, onboarding security, IoT management—rather than access and data packs.

In the platform era, networks are not just engineered—they are exposed, packaged, and sold as software capabilities through developer ecosystems.

for operator networks, Open Gateway helps accelerate service deployment and fosters innovation. It supports application portability and seamless user experiences, and helps the telecom and technology industries realise the potential of 5G to the fullest extent.

CAMARA complements this by defining standard, developer-friendly network APIs for 4G/5G. It is a Linux Foundation- and GSMA-led open-source effort designed to simplify access to telco functions, such as location, device intelligence, and quality of service, for cloud-native applications. CAMARA also supports global service consistency through “app roaming” and promotes secure integration between applications and operator networks through common interfaces.

WHAT TELECOM AS A PLATFORM REALLY MEANS

To understand this transition, it helps to look at telecom platforms across four layers. The first layer is the programmable network layer, where network capabilities are exposed as consumable APIs. The second is the digital architecture layer, where OSS/BSS and IT systems shift from monolithic stacks to modular components designed for continuous change. The third is the developer and partner ecosystem layer, where adoption and usage determine platform value. The fourth is the vertical solutions layer, where telco capabilities are packaged into repeatable outcome-oriented solutions for industries.

These layers are not theoretical constructs. They provide a practical way to understand how telecom operators shift from connectivity companies to platform businesses. The platform telco’s business model becomes less about selling access and more about selling reusable network capabilities.

LAYER 1 PROGRAMMABLE NETWORKS AND NETWORK APIS

Modern networks are increasingly software-defined and programmable. But the larger shift is network exposure: allowing trusted partners to access selected network capabilities through secure APIs. These capabilities may include device status checks, SIM

swap detection, anti-fraud verification, number verification, location confirmation, or quality-on-demand triggers. In this model, the network becomes a programmable service.

GSMA Open Gateway is one major global initiative supporting this shift. It is designed to simplify developer access to operator networks through common APIs, reducing fragmentation and enabling faster adoption.

In India, this is becoming tangible. GSMA has announced an initiative where mobile operators will support federated network services to help online businesses combat scams and identity theft. This is an example of the network becoming a software service for digital trust, aligned to India’s high-scale digital transaction environment.

A complementary approach is 3GPP CAPIF (Common API Framework), which supports flexible and authorised API invocation for northbound APIs—an essential capability when telecom functions are consumed by applications across industries. CAPIF’s emphasis on authorisation becomes particularly relevant in high-risk domains such as identity and fraud control.

LAYER 2 DIGITAL ARCHITECTURE BUILT FOR PLATFORMS

A platform telco cannot be powered by brittle, monolithic OSS/BSS stacks. Traditional telecom IT was built for long cycles, heavy integration, and customisation. In the platform era, that becomes a constraint. Network APIs and enterprise-facing digital experiences require modularity, speed, and consistency.

That is why frameworks such as TM Forum’s Open Digital Architecture (ODA) matter. ODA promotes modular, component-based architecture with standardised open APIs. The approach reduces integration complexity, speeds up change, and enables plug-and-play ecosystems.

This layer may not carry the glamour of 5G headlines, but it is foundational. Without modern IT architecture,

As bandwidth becomes a commodity, telecom's edge shifts to intelligence—trust services, QoS on demand, and API-driven enterprise integration.

network APIs cannot be commercialised at scale, partner onboarding becomes slow, and enterprise experiences remain fragmented.

LAYER 3 DEVELOPER ECOSYSTEMS DRIVE PLATFORM VALUE

Platforms win when developers adopt them. That makes developer experience, onboarding, documentation, sandboxes, versioning, and governance central. These are disciplines associated with software product companies and are essential for telecom operators pursuing platformisation.

In Europe, multi-operator commercial launches of Open Gateway anti-fraud APIs in Spain illustrate how adoption can scale across operator footprints. Operators such as Telefónica, Vodafone, and Orange have participated in these initiatives, highlighting the value of aligned APIs across networks.

Similarly, Deutsche Telekom has highlighted standardised CAMARA-aligned APIs such as device location and device status. The intent is to help partners embed network capabilities into products and workflows, making telecom functions reusable building blocks for digital ecosystems.

LAYER 4 VERTICAL SOLUTIONS DELIVER BUSINESS OUTCOMES

The most monetisable use cases tend to be vertical and problem-led. Enterprises buy outcomes, not telecom primitives. This is where telecom stops “selling technology” and starts “selling business outcomes”.

In BFSI, the focus is on identity and anti-fraud services, where SIM swap detection, number verification, and device intelligence become controls for onboarding and transaction security. In retail and e-commerce, network capabilities can support trusted onboarding, payment security, customer engagement, and personalisation. In manufacturing and logistics, IoT devices and connectivity management platforms enable supply chain visibility

and predictive operations. In healthcare, connected care, secure communications, and asset monitoring and tracking become high-value categories.

HOW THE GLOBAL PLATFORM SHIFT IS UNFOLDING

The platform shift is visible through practical deployments and commercial launches. One of the strongest global signals is the rise of network APIs for fraud and trust. GSMA Open Gateway began demonstrations at MWC 2023, and live deployments have followed. Over the last two years, the focus has been on high-demand APIs such as SIM swap and number verification—capabilities that directly address fraud, a board-level issue for banks and consumer platforms.

The platform shift is also visible in IoT, where telcos have moved beyond connectivity into software-driven device and lifecycle management. AT&T's Control Center provides a cloud-based IoT connectivity management platform that enables enterprises and developers to deploy, manage, and scale IoT devices worldwide. The platform supports near-real-time provisioning and monitoring, rule-based automation and alerts, API integration with other systems, and zero-touch provisioning, enabling rapid scaling with minimal manual intervention. It also incorporates AI/ML-powered anomaly detection and insights, adding intelligence beyond visibility.

This illustrates how telco platforms monetise connectivity through management, automation, analytics, and ecosystems rather than treating IoT as a set of SIM plans.

INDIA'S PLATFORM TELCO PROOF POINTS

India's shift towards platform telecom is becoming increasingly visible through examples across CPaaS, network exposure, multi-cloud networking, trust services, and AI-led platforms.

Airtel IQ provides a clear example of CPaaS as platformisation. Airtel IQ positions itself as an omnichannel cloud communications platform that

The strongest telcos will look less like infrastructure firms and more like software product companies—with API portfolios, roadmaps, and adoption metrics.



unifies customer engagement across voice, SMS, and WhatsApp. Airtel has also launched Airtel IQ Reach, a self-serve marketing communications platform for SMBs, and has publicly discussed integrating WhatsApp into its CPaaS offering through a collaboration with Meta. The strategic point is that CPaaS converts telco assets such as messaging, identity, and delivery quality into programmable enterprise services sold like software.

A second indicator is the commercialisation of network APIs. Nokia's partnership with Bharti Airtel aims to unlock 5G capabilities for developers and enterprises through network APIs using Nokia's Network as Code platform, with Airtel APIs offered on a subscription basis. This reflects telecom capabilities being packaged into products, distributed through a developer ecosystem, and monetised through subscription or usage.

Tata Communications IZO Multi Cloud Networking offers another proof point. Positioned as a unified multi-cloud network management and connectivity platform, it provides a single platform layer with automation and visibility. This is an example of telcos monetising cloud-adjacent platforms such as multi-cloud networking, on-

demand connectivity, and managed network functions rather than selling only links.

India's Open Gateway-linked anti-scam push further strengthens the platform narrative. GSMA's announcement around federated network services to help combat scams indicates that Indian operators see security and trust as platform opportunities, not merely regulatory obligations. In a country operating digital transactions at scale, trust services can emerge as meaningful revenue streams for telecoms.

Reliance Jio's platform posture is also aligned to network exposure and software layers. Jio describes network exposure using NEF/SCEF working with CAPIF to securely expose network capabilities. JioBrain is positioned as an end-to-end AI/ML platform for network optimisation, predictive maintenance, customer experience intelligence, and fraud detection.

On the enterprise IoT side, JioThings positions itself as an end-to-end AIoT organisation integrating connectivity, processing, and secure analytics. At an industry level, Jio Platforms has also announced plans with partners for an Open Telecom AI Platform aimed at

Network APIs turn telcos into enterprise enablers—offering fraud controls, verified identity, location signals, and QoS as on-demand software.

AI-driven solutions for operators, including open APIs and advanced AI techniques.

Across these examples, the pattern is consistent: telecom capabilities are being packaged as platforms and software services.

WHAT TELCOS MUST CHANGE TO WIN THE GAME

This shift is not only about deploying technology; it requires telcos to change operating models and build platform disciplines. A platform telco requires product thinking over project thinking. APIs and platforms are living products, not one-time deployments. They require roadmap discipline, versioning, documentation, developer support, and commercial packaging.

Developer relationships become strategic. If developers do not build on network APIs, the platform does not exist outside the operator's boundary. That is why initiatives like Open Gateway and CAMARA matter—they reduce fragmentation and improve developer adoption, allowing services to scale across operators and markets.

Modern OSS/BSS and open architectures are non-negotiable. Frameworks like TM Forum ODA matter because they enable faster integration and modular upgrades—critical for ecosystem scalability.

Security, privacy, and governance must be built-in. Network APIs touch high-risk domains such as identity, location, and device intelligence. Platform trust will depend on strong authentication and authorisation frameworks, monitoring, and compliance-by-design. CAPIF's emphasis on authorised API invocation aligns closely with this requirement.

Commercial models must evolve. Telcos will need pricing models that software buyers understand, including per-API-call pricing, subscription tiers, and revenue-sharing models. In high-demand verticals such as BFSI and marketplaces, operators can also package trust bundles. Over time, pricing will increasingly shift towards vertical outcome models linked to measurable results such as fraud reduction or onboarding success rates.

Clearly, the next chapter of telecom will be written in software. In the platform era, networks are no longer just engineered—they are programmed. The future value of telecom will come less from how much data a network carries and more from how intelligently that network can be exposed and consumed. Telecom monetisation is shifting from selling connectivity to selling capabilities, securely and on demand.

APIs are becoming the new spectrum: invisible to end users but foundational to digital business models. The most successful telcos will look less like infrastructure companies and more like software product organisations. The question is no longer whether telcos will become platforms, but how fast they can operationalise that shift.

Connectivity may be commoditised, but platforms are not. Telecom's competitive advantage is no longer just coverage; it is the ability to embed the network into enterprise workflows. Telecom's future will not be decided only by spectrum holdings or the speed of radio roll-outs. It will be defined by which operators behave like platform companies—with developer ecosystems, modular digital architectures, and programmable network capabilities that plug into India's rapidly digitising economy.

In the next 24–36 months, the most successful telcos will increasingly look like product organisations: building API portfolios, partnering with hyperscalers and ISVs, and selling repeatable software-led services across industries. Less adaptive players risk being trapped in low-margin connectivity. For India—where digital payments, commerce, identity, and public platforms operate at scale—the opportunity is even greater. If networks become programmable platforms, telecom can move from being invisible plumbing of the digital economy to becoming one of its most valuable software layers. 🧩

The author, a former Regional Director for IoT (India & ASEAN) at AT&T, is a Digital Tech Consultant.

feedbackvnd@cybermedia.co.in



Cloud-native workflows are shrinking enterprise latency

Event-driven cloud, microservices, and iPaaS orchestration are moving context with the asset—enabling real-time approvals, compliance, and execution.



BY DEEPANKAR DAS

In the world of cross-functional business operations, from marketing and advertising to supply chain management, the workflow has historically been a game of hot potato. A creative agency flings a video file at a brand manager; the manager flings a list of bulleted feedback back; legal flings a rejection notice. This

fragmented cycle is now being replaced by contextual workflows, where feedback, versions, and approvals live within the asset itself.

While the user sees a seamless interface, the real revolution is happening in the backend infrastructure,

The real shift is not UI polish—it is orchestration. Event triggers and microservices turn creative assets into data-rich, executable workflows.

In contextual collaboration, the file becomes the workflow layer: feedback, approvals, and compliance travel with the asset, not across inboxes.

where the 'Infrastructure' that allows a 4K video or a complex 3D design becomes a living, data-rich environment.

EVENT-DRIVEN ORCHESTRATION REPLACES POLLING

Traditional creative collaboration relied on 'polling', checking a folder to see if a new version had arrived. Modern infrastructure uses event-driven architecture.

In a realistic agency context, when an editor at a firm like Ogilvy or Dentsu uploads a new edit of a campaign video, an event is triggered at the infrastructure level.

This event not only sends a notification but can also trigger a microservice to automatically generate a low-res preview for mobile reviewers, notify the legal team's specific compliance dashboard, and lock the previous version to prevent accidental edits. The infrastructure ensures the context (the file + the feedback) moves automatically, rather than waiting for manual hand-offs.

MICROSERVICES MAKE WORKFLOWS SEAMLESS

The reason modern platforms feel snappier and more integrated is the use of microservices. Instead of one monolithic application, the platform is a web of specialised services.

For a marketing team at a brand like Zomato or Nykaa, this means the tool can provide contextual articulation. One microservice might handle the frame-accurate video playback, another manages the voice note feedback stream, and a third handles identity management to ensure only authorised stakeholders see pre-launch assets.

This modularity allows the backend to bridge disparate functions, such as linking a creative comment directly to a task in a project management system, without requiring the user to ever leave the visual workspace.

CLOUD-NATIVE ENGINES REMOVE REVIEW LATENCY

Collaborating on high-resolution assets like RAW images



IN BRIEF

- Contextual collaboration replaces hand-offs as feedback, versions and approvals live within the asset, removing email-thread friction and delay.
- Event-driven infrastructure replaces polling, auto-triggering previews, notifications, compliance workflows, and version locks when edits are uploaded.
- Microservices split functions—playback, feedback, identity, and tasks—creating seamless cross-team workflows without switching tools or contexts.
- Cloud-native engines anchor annotations as metadata tied to timecodes and pixels, enabling high-res asset review to be faster and more precise.
- DPDP Rules 2025 push for privacy-by-design: zero-trust access, audit trails, and erase-ready workflows must be built into collaboration stacks.
- iPaaS acts as the enterprise glue, syncing collaboration hubs with SAP/Oracle/Salesforce to avoid data drift and enable real-time action.

DPDP-era collaboration is regulated data processing. Privacy-by-design needs zero-trust identity, audit trails, and erase-ready cloud workflows.

or 4K social ads used to be a nightmare due to slow download speeds. The shift to cloud-native workflow engines and to object storage orchestration, such as AWS S3 with Lambda triggers, has changed the game.

The infrastructure now performs the heavy lifting in the cloud. When a reviewer leaves a pinpoint annotation on a specific frame of a video, the backend saves not only a text comment but also anchors that metadata to a specific time code and pixel coordinate in the cloud. This ensures that when the editor opens the project in their studio, the feedback is perfectly overlaid on their timeline.

DPDP SHIFTS SECURITY INTO WORKFLOWS

Security can no longer be a gate at the end; it must be shifted left into the collaboration workflow itself. With the notification of the DPDP Rules 2025, Indian infrastructure leaders will face a new mandate, Privacy-by-Design. Collaboration environments can no longer be just 'chat boxes', but they'd be data processing centres.

Modern infrastructure leverages Zero-Trust identity frameworks (like Azure AD). For an advertising agency handling sensitive pre-launch assets for a client, such as Airtel, the infrastructure ensures access is contextual. A freelancer might have access to a video file for exactly 48 hours, and the permission set is automatically revoked by the backend the moment the task is marked complete.

Also, secure messaging protocols now include automated audit trails. If a user exercises their 'right to erase' under the DPDP Act, the underlying cloud orchestration must be able to locate and purge that individual's data across all collaborative threads, attached files, and integrated apps simultaneously.

COLLABORATION MEETS REAL-TIME EXECUTION

When one broadens the scope and goes beyond creative workflows, contextual collaboration reshapes high-stakes business functions by bridging the gap between Communication and Core Operations.

For instance, HR Operations is switching from manual emails to a contextual workspace that triggers an automated provisioning flow. The moment a contract is signed in a tool like DocuSign, the backend automatically sets up access to enterprise systems, orders hardware, and creates the employee record.

If the supply chain is taken as an example, for a firm like Delhivery, if a shipment is delayed, the system (via IoT triggers) automatically updates the shared project timeline, notifies the customer-facing team, and triggers a rerouting task, enabling execution of a fix in real time.

iPaaS BECOMES THE GLUE FOR CIOs

For a diversified conglomerate like Reliance Industries or the Tata Group, the challenge isn't a lack of tools, but the fragmentation between them. Global systems like SAP or Oracle often struggle to speak to modern collaborative hubs or local favourites like Zoho and Freshworks.

This is where Integration Platform-as-a-Service (iPaaS) comes in. iPaaS acts as the central nervous system, providing a layer of contextual interoperability. Platforms like Workato and MuleSoft ensure that an action taken in a collaboration tool is instantly reflected in the system of record, such as SAP, Oracle, or Salesforce. This eliminates data drift, where the conversation moves faster than the database itself.

For the modern CIO, the shift toward contextual collaboration changes the 'Digital Estate' management strategy. It moves the CIO's office from a manager of systems to a Chief Architect of Trust, because the future of collaboration is not just about better communication but about an intelligent infrastructure that understands the context of the work and clears the path for the human mind to execute. 🧠

*The author is Co-Founder and CEO
of ButtonShift.*

feedbackvnd@cybermedia.co.in



PCQUEST JANUARY 2026 EDITION EMERGING TECHNOLOGIES THAT WILL RESHAPE 2026

ALSO READ MORE ON

- AI's power shift begins at the edge • 2025 PCs got brains, not just speed
 - Beyond specs: 2025 phones are engineered smart
 - The rise of Indian esports isn't luck; it's logistics
- Tech without borders: 2025's most empowering innovations
 - When every frame fights back, this is how AI survives
- The invisible intelligence powering healthcare and finance



Scan QR Code
& Subscribe now...

PCQUEST IS OFFERING
SPECIAL DISCOUNTS
FOR **NEW SUBSCRIBERS**
AND ITS READERS.
AVAIL THE OFFER NOW

Link: <https://bit.ly/3QvNQh8>

FOLLOW PCQUEST FOR THE REGULAR
UPDATES ON TECH AND TRENDS

 @pcquest  @pcquest  @pcquest

Leverage PCQuest platform & network. Write to:
Ajay Dhoundiyal | ajaydh@cybermedia.co.in | +91 99535 40318



For Subscription queries::

 subscriptions@cybermedia.co.in

 9289870545

The thinking network: Making every node count

AI agents and cloud-led orchestration will transform enterprise networks into intelligent systems that act, predict, and optimise before issues arise.



BY SAJAN PAUL

Enterprise networking in 2026 is set to evolve into intelligent, experience-driven platforms that enhance human capability through Artificial Intelligence (AI) and automation. Networks will move from reactive to predictive systems, with AIOps making real-time decisions and agentic AI orchestrating experiences across the full infrastructure stack.

One can also expect full-stack convergence transitioning from concept to standard practice, enabling unified intelligence that manages wired, wireless, and wide-area networks (WAN) as a seamless system. Perhaps most significantly, IT professionals will shift from troubleshooting to strategy, partnering with AI copilots to manage thousands of endpoints efficiently while focusing on innovation.

Here are four key predictions for how AI and cloud-led innovation will reshape enterprise networking into a proactive, self-optimising foundation for digital business.

#1

AIOps WILL OUTWEIGH WI-FI SPECIFICATIONS

In 2026, the way enterprises operate wireless networks will fundamentally change. AIOps will no longer be optional. While enhancements such as multi-link operation, wider channels, and deterministic latency continue to advance, their full potential will only be realised through AI's ability to make complex spectrum decisions far faster than human operators.

Continuous learning models will predict congestion, optimise radio frequency behaviour, and dynamically

AI-powered LANs will no longer react to problems—they will prevent them, redefining network experience as a proactive service.

reshape channel usage in real time. As a result, long-standing concerns around SSIDs, “best band” selection, and manual tuning will become outdated. Performance across wired and wireless environments will converge—not due to higher speeds—but because AI will manage user experience holistically, through an intent-based, integrated network fabric.

#2

AGENTIC AI WILL POWER PROACTIVE NETWORKS

The industry’s pursuit of self-driving networks will shift from early adoption to widespread deployment. The change will not lie in the idea itself, but in the maturity of agentic AI and cloud-based intelligence that can now act independently on behalf of IT teams.

Local area networks (LANs) will not just self-heal; they will proactively optimise user experiences. AI agents embedded in switches and access points will analyse behaviour patterns, anticipate service disruptions, and take corrective actions—often before any human notices a problem. For example, hardware replacements will be automatically initiated. AI will detect component degradation, validate the issue, create a support case, and dispatch a replacement—all without user or administrator intervention.

This transformation marks a shift from reactive maintenance to predictive service delivery, with AI ensuring business continuity at machine speed.

#3

FULL-STACK CONVERGENCE BECOMES STANDARD

By 2026, enterprise decision-making around infrastructure will pivot away from siloed solutions towards unified platforms. Organisations will increasingly demand one operational framework spanning wired, wireless, WAN, compute, and storage environments. AI-native automation and cloud-delivered orchestration will drive expectations for a single source of truth—a unified intelligence layer overseeing performance, experience, security, and lifecycle management from endpoint to cloud.

This trend will extend beyond networking. As platforms like OpsRamp unify observability and

operations across servers, storage, and applications, enterprises will expect the same cohesion in their connectivity layer. Competitive advantage will shift from individual component performance to the seamless integration and orchestration of full-stack systems, all governed by AI.

The winning architecture in 2026 will not be a collection of products—it will function as one intelligent organism. AI will unify, cloud will deliver, and enterprise buyers will select vendors based on their ability to deliver a coherent, end-to-end experience.

#4

AI WILL ELEVATE THE NETWORK WORKFORCE

The most profound workforce shift in enterprise networking will not be about automation replacing engineers—it will be about redefining their roles. Conversational AI copilots and agentic assistants will become embedded parts of IT teams, rendering traditional workflows such as dashboard-hopping and manual troubleshooting increasingly redundant.

With generative AI reaching new levels of accuracy and capability, AI will assume responsibility for first-line support—resolving policy conflicts, detecting anomalies, answering routine questions, and even initiating hardware replacements.

Future network engineers will not only configure systems but will also collaborate with AI to manage networks at scale. Precision will be achieved not through manual inputs, but through natural language interfaces where AI surfaces insights and executes actions. The most effective professionals will be those who understand how to guide AI—shaping prompts, validating intent, and orchestrating automation.

In 2026, the network engineer will evolve into a strategic operator, and AI will become the operational backbone of enterprise infrastructure. 🧠

*The author is the General Manager of HPE
Networking India.*

feedbackvnd@cybermedia.co.in



Security goes autonomous: AI agents, twins, AR wearables

Agentic AI, digital twins, and AR wearables are moving from pilots to operations, reshaping how Indian security teams detect, decide, and act.



BY ANDREW BURNETT

As India steps into 2026, several technology trends that once lived largely in research labs and conference keynotes are now becoming the daily reality of the security industry. What is new is not the idea of AI itself, but the emergence of Agentic AI—intelligent systems capable of taking autonomous actions across operational workflows.

Instead of asking what AI might do someday, security teams are now seeing what it can actually do in the field, under real constraints, real urgency, and real accountability.

Three technologies will particularly drive this shift in 2026: Agentic AI, Digital Twins, and Wearables with Augmented Reality (AR). Each represents an evolution not just in capability, but a step toward fully intelligent, interconnected, and immersive security ecosystems.

As India accelerates the adoption of smart city frameworks and digital surveillance infrastructure—through programmes such as the Smart Cities Mission and Digital India—these technologies are no longer futuristic concepts. They are becoming essential to

The security stack is becoming programmable: agents correlate feeds, trigger actions, and leave audit trails—without operators having to switch dashboards.

Digital twins are turning sites into testbeds, letting teams rehearse threats, validate SOPs, and optimise sensor placement before incidents occur.

the daily functioning of security operations across Indian enterprises, public infrastructure, and government systems.

AGENTIC AI: FROM HYPE-CYCLE TO OPERATIONAL WORKFLOWS

Agentic AI first gained attention for use cases such as code generation, but its practical impact in 2026 is expanding well beyond software development. The real shift is from capability demonstrations to task-focused agents embedded directly into operational flows. Rather than remaining a proof-of-concept novelty, agents are now being designed to orchestrate across systems: ingesting video feeds, correlating access logs, detecting deviations, and triggering follow-up actions—all without a human having to translate between disconnected interfaces and dashboards.

Indian policy and industry narratives reflect this momentum. The AI for Viksit Bharat study points to financial services organisations transforming front, middle, and back offices through machine learning and agentic AI. Similarly, the Ministry of Electronics & IT, in its vision for India's AI evolution, notes that AI-driven technologies, such as autonomous agents, are helping SMBs scale more efficiently, personalise experiences, and optimise operations.

While these are broad digital economy observations, the security function is quickly becoming one of the most immediate beneficiaries—because it deals with high-volume data, repeatable workflows, and time-bound decisions.

A practical example is the autonomous investigation agent. When an alarm is triggered, the agent does not simply flag it—it gathers the last 30 minutes of multimodal evidence (video, access events, sensor telemetry), correlates patterns, and proposes a mitigation action that the operator can approve. The value is twofold: speed, through a reduction in mean time to insight; and bandwidth, by allowing operators to focus on judgment and decisions rather than data collection. In other words, the agent compresses the operational cycle between detection and action.



IN BRIEF

- Agentic AI is shifting from demos to agents that run repeatable security workflows across video, access logs, and sensors.
- Autonomous investigation agents compress incident cycles by packaging evidence and proposing mitigation actions for approval.
- Digital twins are becoming operational tools for scenario testing, SOP design, and predictive maintenance of security devices.
- AI-driven twins enable privacy-aware planning by fusing multi-source data for real-time monitoring and predictive analytics.
- AR wearables are evolving from recorders to decision-support tools via context-aware prompts and natural language queries.
- The 2026 playbook is integration, simulation, and frontline augmentation—measured by response time, false positives, and confidence.

AR wearables bring hands-free intelligence to the frontline—summarising risk, replaying suspicious events, and answering patrol queries in seconds.

This push is also mirrored in global investment patterns. Industry projections suggest that Agentic AI could dominate IT budget expansion over the next five years, representing over 26% of worldwide IT spending and surpassing USD 1.3 trillion by 2029. What that signals is not simply enthusiasm—it indicates a decisive shift from experimentation to operationalisation at scale.

The actionable shift for organisations is therefore clear: stop asking, “What might agentic AI do?” and start identifying repeatable security workflows to automate—incident triage, patrol optimisation, evidence packaging, compliance reporting—and measure agent performance against those KPIs. The winners in 2026 will be the platforms that expose safe, auditable agent APIs and the vendors who integrate them into end-to-end operational playbooks rather than isolated, one-off features.

DIGITAL TWINS: FROM MODELS TO MISSION-CRITICAL DECISIONS

Digital twins, highly sophisticated virtual models synchronised with real-world systems, are also reaching a point of real practicality. The concept is not new. Manufacturing and logistics have long used digital twins to monitor assets, model environments, and plan operations. What is new for security is the granularity and the scale now possible, driven by sensor density, compute capacity, and AI-driven correlation.

The Indian policy lens has already begun to recognise this potential. The Ministry of Communications has described AI-driven digital twins as privacy-preserving systems that integrate real-time, cross-sectoral data to enable unified and dynamic planning. Beyond monitoring, the emphasis is on predictive analytics and scenario simulation—optimising resource allocation, supporting infrastructure resilience, and enabling collaborative planning across stakeholders. For security teams, this is significant because it shifts the function from reactive operations to structured, simulation-backed decision-making.

Globally, organisations such as NVIDIA have demonstrated digital twins for data centres, integrating

cameras, fire alarms, access control, and environmental sensors to create a unified, real-time view of operations. These are not static replicas. They are interactive environments where teams can safely test, optimise, and validate system behaviour.

The value goes far beyond visualisation: digital twins enable organisations to monitor, optimise, and actively manage the desired state of multiple subsystems in real time—preventing drift, identifying weak links, and accelerating action when anomalies emerge.

A well-built security twin can simulate high-impact scenarios before they become real incidents. Consider a virtual fire drill that models pedestrian flow if a corridor is blocked, or a simulation of lockdown strategies that maintains egress while containing a threat.

These are not academic exercises; they directly inform SOPs, design choices, sensor placement, and decisions on resilient communications or edge compute. For complex estates such as airports, ports, hospitals, large campuses, and multi-tenant high-rises, a unified twin can reduce configuration drift, accelerate forensic reconstruction, and support predictive maintenance for critical devices.

Over time, this capability could reshape the industry’s approach to risk and planning. With a unified, real-time view of complex environments, security teams can anticipate threats, optimise resource allocation, and continuously refine SOPs based on simulated outcomes rather than relying solely on historical events. The longer-term shift is profound: from incident response to predictive and preventative security strategies, with investments in training, infrastructure, and systems guided by “what-if” models grounded in operational data.

THE GAME-CHANGERS: WEARABLES AND AR IN ACTION

AR and wearables have had a turbulent history, but their resurgence in 2026 will look different—largely because AI changes what these devices are. AI transforms wearables from simple capture tools into intelligent

In 2026, the edge of advantage is not more cameras—it is faster decisions, fewer false alarms, and security workflows built like software.

companions. It elevates AR from a visual overlay into a real-time, context-aware guidance layer. Rather than passive devices that record what a guard sees, the next generation of wearables will increasingly see, listen, and interpret the environment—delivering timely, decision-relevant insights through voice, visual cues, or hybrid interfaces.

India's technology policy messaging reinforces this direction. The Ministry of Electronics and Information Technology has explicitly referenced India preparing for cutting-edge technologies, including 5G, AI, blockchain, AR/VR, machine learning, robotics, NLP, and other frontier domains. In the security industry, that preparation translates into frontline augmentation, remote support, and decision compression—especially in environments where response time and situational awareness determine outcomes.

The market trajectory is also clear. Globally, the AR sector is projected to surge from USD 35.8 billion in 2024 to USD 233.3 billion by 2030, at a CAGR of around 37%. Notably, software and services account for most AR revenue, signalling that enterprises are looking beyond hardware novelty and adopting AR for operational use cases such as training, simulation, remote assistance, and real-time decision support.

What makes this category especially powerful for security is natural language interaction. A guard can ask, "When was this area last patrolled?" and receive a concise, evidence-backed response. They can request the system to replay the last suspicious approach and tag it for review, or ask for a summarised risk context before entering a zone. In effect, wearables shift from passive recorders to active decision-support tools, improving situational awareness while keeping hands and attention free.

While mass deployment may still be a few years away, the direction is unmistakable. The future of security work will be increasingly wearable—through smart glasses, headsets, and wrist-mounted devices—and powered by conversational systems that deliver real-time decision

support, particularly in large public infrastructure and high-risk industrial settings.

FROM PROMISE TO PRACTICE: THE 2026 SECURITY PLAYBOOK

Across these trends, one theme is consistent: AI is the enabling layer that makes previously hyped technologies operationally useful. Agentic AI turns workflows into autonomous sequences rather than manual checklists. Digital twins convert environments into testable systems rather than static floor plans. AR wearables convert frontline personnel into connected decision nodes rather than isolated eyes and ears.

For CISOs, facility heads, and operations leaders, the playbook for 2026 is both simple and strategic. Prioritise integration via open, auditable APIs. Expand simulation capabilities through twins that map directly to SOPs. Pilot wearable augmentation that compresses time-to-decision and improves situational awareness. Most importantly, measure success not through novelty, but through operational KPIs: response time, false-positive reduction, investigation time, workload reduction, and decision confidence.

In simple terms, India's security landscape is evolving quickly, and Agentic AI, digital twins, and AR wearables are moving from early trials into real-world systems. With national programmes accelerating modernisation, security leaders are prioritising AI for faster, more consistent responses; digital twins for better planning and predictive operations; and wearables for stronger execution on the ground.

After years of excitement and experimentation, the industry is entering a more serious era—one where emerging technologies no longer feel like prototypes, but like operational partners. In 2026, the shift is unmistakable: security innovation is no longer about what is possible—it is about what is deployable, measurable, and trusted. 🧩

The author is the Interim Chief Technology Officer of Milestone Systems.

feedbackvnd@cybermedia.co.in



Digital infrastructure shifts from scale to trust

AI-scale compute, multi-agent automation, domain LLMs, and sovereign cloud shifts are redefining digital infrastructure—with trust and risk at the core.



BY NARINDER KUMAR

In a world defined by accelerating disruption, escalating expectations, and shifting geopolitical and economic realities, technology is once again writing the playbook for business success. The trends shaping the enterprise landscape signal a clear transition—from experimentation to responsibility, from scale to trust, and from isolated innovation to integrated execution.

At the centre of this shift is digital infrastructure. Compute, cloud, networks, and cyber resilience are no longer background enablers—they are becoming board-level determinants of competitiveness. In an AI-powered and deeply interconnected economy, success will depend on how well leaders balance speed with governance, intelligence with accountability, and automation with human oversight.

The technologies on this horizon are not “nice-to-have” initiatives. They are strategic infrastructure imperatives—engines of value creation, risk mitigation, and competitive differentiation. Leaders who understand and act on these trends now will not only navigate uncertainty but reshape the future contours of their industries.

AI INFRASTRUCTURE: REDEFINING ENTERPRISE COMPUTE

In 2026, the demands of AI will outpace traditional computing models. AI workloads are becoming so large, diverse, and mission-critical that leaders have now started to think of AI like electricity, a strategic grid they rely on. AI supercomputing platforms, systems that integrate CPUs, GPUs, AI ASICs, and specialised architectures, will unlock next-generation analytics, simulation, and machine learning workloads.

Digital infrastructure is being rewritten: AI compute, cloud sovereignty, and security platforms will decide who scales with confidence.

For leaders, this shift is already visible across industries where compute intensity directly translates to competitive advantage. In banking and capital markets, it supports near-real-time risk modelling, fraud detection, and stress testing at unprecedented scale. Manufacturing and energy companies are using these platforms to run digital twins of factories, grids, and supply chains, optimising performance before physical changes are made.

These supercomputing platforms are not just about speed; they will continue to redefine what is computationally possible in domains such as drug discovery, climate modelling, financial risk analysis, and personalised AI services.

AI-NATIVE PLATFORMS: RESHAPING SOFTWARE DELIVERY

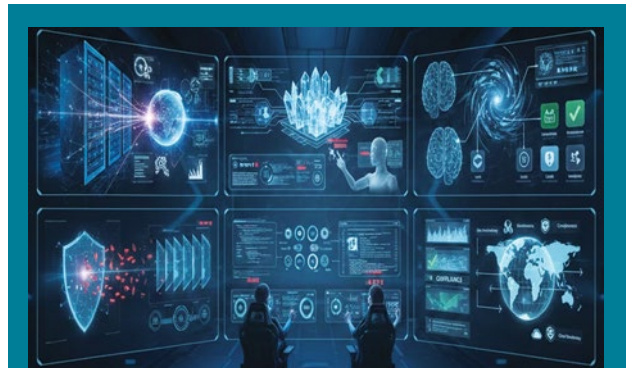
AI is not just augmenting workflows. It is progressively building them. AI-native development platforms embed generative AI into the software lifecycle from design and testing to observability, enabling faster, more flexible delivery with smaller, highly productive teams.

For leaders, this trend will continue to be more than a productivity play. It democratises innovation, allowing domain experts and cross-functional teams to build solutions without traditional engineering bottlenecks.

Industries with complex digital backbones are already seeing tangible impact. Retail and consumer brands are using AI-native platforms to rapidly launch personalised experiences across channels. Telecom and media organisations are accelerating feature releases while reducing regression risks through AI-driven testing and observability.

MULTI-AGENT AI: ORCHESTRATING AUTONOMOUS WORK

The era of isolated AI tools is ending. In 2026, multi-agent systems (MAS), which are collections of AI agents that interact, cooperate, and coordinate toward complex goals, will become critical. These systems will increasingly function as orchestration layers, transforming how work is automated, how decisions are made, and how processes adapt in real time. Successful leaders will treat



IN BRIEF

- AI supercomputing is turning compute into core digital infrastructure for real-time risk, simulation, and industrial-scale analytics.
- AI-native platforms will compress software cycles, embedding testing and observability to deliver faster releases with fewer defects.
- Multi-agent AI will orchestrate workflows across systems, enabling autonomous execution while keeping humans in control of exceptions.
- Domain LLMs will improve accuracy and compliance, making regulated AI deployments viable in BFSI, healthcare, legal, and industry.
- AI security platforms will become essential to counter prompt injection, data leakage, model misuse, and rogue autonomous agents.
- Geopatriation will reshape cloud decisions as sovereignty, resilience, and compliance redefine where enterprise workloads should run.

these systems not just as add-ons, but as orchestration engines powering autonomous workflows, dynamic optimisation, and new forms of human-AI collaboration.

Multi-agent systems are particularly relevant in environments where decisions must be coordinated across systems and timeframes. In logistics and supply chain, agents can continuously rebalance inventory, routes, and demand forecasts. Insurance firms are

Cloud strategy is now a geopolitical subject—workloads will shift closer to home as enterprises prioritise sovereignty and continuity.

beginning to explore agent networks that assess claims, validate documentation, and flag anomalies while escalating only high-risk cases to humans.

DOMAIN LLMs: ENABLING COMPLIANCE-GRADE ACCURACY

The rush to navigate a general language model's lifecycle has taught two clear lessons: scale is powerful, but domain accuracy and compliance are what ultimately win customer trust.

Domain-specific language models (DSLMS)—trained and governed on sector-specific datasets—can deliver the precision, auditability, and regulatory alignment that enterprises need, particularly in highly regulated industries such as finance, healthcare, and legal services.

In effect, AI models that are trained and fine-tuned on industry-, function-, and workflow-specific data offer higher accuracy, stronger compliance, and lower operational risk. As a result, these specialised LLMs are becoming essential for sectors including healthcare, legal, finance, and industrial operations.

Banks and financial institutions are already using such models to interpret regulatory text, assess exposure, and generate compliant customer communication, while healthcare providers are applying them to clinical documentation, coding, and decision support—areas where accuracy and clarity are non-negotiable.

Leaders and enterprises that build, curate, and govern these domain-centric models will be better positioned to unlock tangible business value rather than merely novelty.

AI SECURITY PLATFORMS: REINFORCING DIGITAL TRUST

As AI becomes more pervasive, cyber risk becomes more existential. Encryption at rest and in transit is no longer enough. Confidential computing—cryptographically protecting data while it is being processed—will become essential for secure collaboration, cross-party analytics, and regulated AI deployments.

AI security platforms are emerging as the unified backbone for securing both third-party and custom

AI applications against risks like data leakage, prompt injection, and rogue agents.

GEOPATRIATION: DRIVING SOVEREIGN CLOUD STRATEGY

Cloud adoption was once synonymous with globalisation. Now, geopolitical risk is prompting organisations to rethink where and how data and workloads reside. Geopatriation—moving workloads to sovereign, regional, or in-country infrastructure—will be a strategic imperative for compliance, trust, and resilience. This is not deglobalisation, but selective localisation to reduce risk and increase control.

To stay at the top of this, leaders would need to audit where critical data resides, map sovereignty risks, and build a regional platform strategy that can meet compliance and market needs.

2026: REWARDING LEADERS WHO EXECUTE WITH TRUST

The common thread across these trends is not technology for its own sake, but the strategic leverage it enables. As AI and digital connectivity touch every function, the real winners will be enterprises and leaders who align technology with business value, build secure, ethical, and scalable systems, embed resilience into operations and services, and enable human-AI collaboration rather than replacement.

What feels different in the coming year is the pace of acceleration. Innovation cycles have compressed dramatically, pushing once-emerging technologies into the mainstream far sooner than expected. As a result, leaders no longer have the luxury of waiting.

2026 will not reward the fastest adopters, but the most deliberate ones—those who align technology, trust, and execution at scale. Those who act now will not merely adapt to change; they will shape markets, standards, and competitive advantage for the decade ahead. 🌟

*The author is the Co-Founder and CEO of
To The New.*

feedbackvnd@cybermedia.co.in



The new enterprise core: cloud, cyber, and connectivity

In 2026, MSMEs will unify cloud platforms, cyber resilience, and high-availability connectivity with AI automation to stay agile and always-on.



BY VISHAL RALLY

The digital momentum built over the last few years has laid the foundation for a more agile, resilient, and future-ready enterprise landscape in 2026. Across India's B2B technology ecosystem, particularly among MSMEs, digital transformation has moved from aspirational to operational necessity. Strong public digital infrastructure, expanding cloud-edge ecosystems, and increasing AI adoption have together driven sustained year-on-year digital growth.

More importantly, enterprises are no longer adopting technology in silos. Cloud, cybersecurity, connectivity, and customer engagement platforms have evolved from support functions into core pillars of business continuity, experience, and enterprise agility. The milestones achieved in 2025 are now shaping how organisations design their digital frameworks for the years ahead.

One of the defining shifts has been the move from scale-driven adoption to agility-led execution. Businesses

are prioritising transformative technology adoption to respond faster to market volatility, regulatory shifts, and changing customer expectations.

AI-led automation, secure cloud platforms, private networks, and cyber resilience are now viewed as foundational capabilities rather than discretionary IT investments. Together, they are enabling organisations to operate with greater predictability, responsiveness, and confidence.

CLOUD: THE ENTERPRISE RESILIENCE BACKBONE

Once viewed primarily as a cost optimisation tool, cloud has evolved into a core enabler of innovation and operational resilience. By leveraging geo-redundant architectures, automated backups, and real-time data replication across distributed data centres, cloud platforms significantly strengthen business continuity. They minimise downtime, protect data integrity, and enable rapid recovery from system

The enterprise core is being rebuilt—cloud, cyber, and connectivity now work as one stack to deliver resilience, agility, and continuity.

failures or local disruptions while reducing reliance on physical infrastructure.

With a pay-as-you-go model, the cloud provides unprecedented flexibility and scalability. This enables firms to dynamically adjust their computing resources, scaling up or down in response to market fluctuations or real-time demand, without incurring major capital investments. This flexibility ensures new products and services enjoy faster time-to-market, better collaboration among hybrid or remote teams, and easier access to AI, ML, and other advanced technologies for data-driven decision-making.

A retail manufacturer, for example, adopted a cloud-first approach to manage seasonal demand swings. By scaling infrastructure dynamically during peak cycles and optimising costs during lean periods, the business improved time-to-market while maintaining operational stability.

UCaaS: POWERING DISTRIBUTED WORKFORCES

As hybrid work models stabilised, enterprises increasingly turned to Unified Communications as a Service (UCaaS) to streamline collaboration. By consolidating voice, video, messaging, and email into a single cloud-based platform, UCaaS reduced complexity while improving productivity. For growing organisations, UCaaS replaced legacy on-premises systems with flexible, secure communication tools accessible from anywhere. Seamless integration with productivity platforms enabled richer collaboration, faster decision-making, and lower infrastructure overheads, freeing up capital for core business priorities.

A mid-sized educational institution, for instance, adopted a cloud-based contact centre platform to streamline student onboarding and faculty interactions across voice, chat, email, and digital channels. By unifying all touchpoints into a single interface, the institution improved response times, ensured continuity across interactions, and delivered a more personalised experience, enhancing student satisfaction while reducing administrative effort.

CYBERSECURITY: FROM DEFENCE TO RESILIENCE

From a vanilla perimeter defence, cybersecurity has



IN BRIEF

- Digital transformation is now operational: MSMEs treat cloud, cybersecurity, and connectivity as core business capabilities rather than IT add-ons.
- Cloud has evolved into a resilience backbone using geo-redundancy, replication, and automated recovery to minimise downtime and data loss.
- UCaaS is simplifying hybrid work by unifying voice, video, and messaging in a secure cloud layer, improving speed and productivity.
- Cybersecurity is shifting from perimeter defence to resilience-first models built on zero trust, continuous monitoring, and identity controls.
- Connectivity is now strategic: diversified fibre-wireless links, failover, and routing intelligence protect uptime, revenue, and customer trust.
- Omnichannel CX platforms integrate touchpoints with analytics, helping firms deliver personalised service without legacy complexity or cost.

shifted to a more cohesive, proactive model that promotes cyber resilience. Stringent cybersecurity firewalls are now indispensable for business continuity. Enterprises are increasingly adopting zero-trust frameworks, continuous monitoring, and identity-driven access controls to anticipate and contain threat vectors.

Connectivity has moved from utility to strategy, with uptime, failover, and routing intelligence now directly shaping revenue and trust.

For MSMEs, managed cybersecurity solutions have become critical for maintaining uptime, protecting customer data, and meeting compliance expectations. Embedding security across the development lifecycle has also enabled faster innovation without compromising trust, an essential capability as digital ecosystems become increasingly complex.

CONNECTIVITY: THE STRATEGIC GROWTH LAYER

Reliable connectivity has emerged as the invisible backbone of enterprise agility. Organisations are increasingly adopting diversified network architectures combining fibre, wireless, and next-generation connectivity to eliminate single points of downtime. Automated failover and intelligent routing ensure uninterrupted access to cloud applications, even during local outages. This is particularly critical for sectors such as logistics, payments, and customer support, where downtime directly impacts revenue and customer trust.

Businesses can push for rapid expansion into untapped markets with secure, high-speed, on-demand connectivity that supports global and distributed operations. Moreover, this low-latency access, so essential for real-time collaboration and cloud applications, boosts productivity and enables greater responsiveness to consumer demands, irrespective of geographic location.

CX: OMNICHANNEL ENGAGEMENT AT SCALE

There has been a critical shift toward omnichannel engagement as a strategic differentiator. Customers now expect seamless interactions across voice, chat, email, social media, and digital platforms without fragmentation or loss of context. Cloud-based contact centre and customer experience platforms are enabling businesses to unify these touchpoints into a single, intelligent engagement layer.

By integrating AI-driven insights and analytics, enterprises can deliver consistent, personalised experiences across channels, improving responsiveness, satisfaction, and long-term loyalty. For MSMEs, this has unlocked enterprise-grade customer engagement capabilities without the complexity or cost of traditional systems.

SD-WAN: THE MSME NETWORK EQUALISER

Digital transformation has significantly levelled the playing field for MSMEs. Technologies such as SD-WAN have enabled smaller enterprises to achieve network agility, performance optimisation, and cost efficiency capabilities that were once limited to large organisations.

By simplifying network management and improving application performance across locations, SD-WAN has reduced reliance on expensive hardware and manual intervention. MSMEs can now scale faster, operate more securely, and remain flexible in increasingly competitive markets. For example, a fast-growing mid-size cosmetic healthcare company with multiple experience centres adopted SD-WAN to centralise network control and automate routine tasks. The result was faster issue resolution, reduced downtime, and greater focus on strategic initiatives rather than day-to-day firefighting.

AI: ENABLING THE FUTURE-READY ENTERPRISE

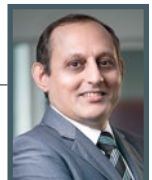
Another defining milestone has been the rise of more efficient, context-aware AI systems. Enterprises are increasingly deploying intelligent models that combine analytics, automation, and contextual intelligence to enable adaptive decision-making and personalised engagement. These capabilities are reshaping how businesses operate by enabling smarter planning, better resource utilisation, and deeper customer engagement across sectors ranging from retail and manufacturing to education and urban infrastructure.

As organisations move into 2026, success will depend on how effectively they integrate cloud, cybersecurity, connectivity, communications, and intelligent automation into a cohesive digital framework.

For B2B technology providers and MSMEs alike, the focus must shift from isolated deployments to an ecosystem approach that enables resilience, scalability, and continuous innovation. The enterprises that will lead in 2026 are the ones building their digital core today with clarity, capability, and confidence. 🌟

The author is the President and Chief Revenue Officer of Tata Teleservices.

feedbackvnd@cybermedia.co.in



TO STAY AHEAD OF THE CURVE IN TELECOM READ VOICE&DATA

**Celebrating
Dataquest
40 years:
Avail Special
discount
on V&D.**



**Digital
subscription
also available on
Magzter, Zinio,
Readwhere,
& Readly**



Book Digital Subscription Now!

Yes! I want to subscribe to Voice&Data



Scan QR Code
& Subscribe now...

Subscribe to Digital Edition @ ₹735/-

Period	Issues	Print Subscription Rate		Digital Subscription Rate
		New	Renewal	
☐ 1 year	12	₹1,140/-	₹1,050/-	₹735/-
☐ 2 years	24	₹2,190/-	₹2,020/-	₹1,470/-
☐ 3 years	36	₹3,285/-	₹3,020/-	₹2,205/-

or **Subscribe online:** subscriptions.cybermedia.co.in/voicendata

Please tick your subscription choice above, fill the form below in CAPITAL LETTERS and mail it to us at subscriptions@cybermedia.co.in

☐ I want to avail premium service of receiving your copy by courier. Tick which ever is applicable.

☐ ₹ 600/- 1 year ☐ ₹ 1200/- 2 years ☐ ₹1800/- 3 years

Name [•]: Mr/ Ms _____ Date of Birth:

Organisation: _____ Designation: _____

Delivery Address: _____

City: _____ State: _____ Postal Code:

Mob [•]: Tel: Email [•]: _____

GST No. [•]: PAN No. [•]:

☐ I am paying ₹ by DD/Cheque No.: Dated:

Payable at (specify bank and city) _____

OR

☐ Please Remit for ₹ Through RTGS/NEFT to our A/C details given below:

Bank Name: ICICI Bank Limited, A/c no. 017705000132, Branch & IFS Code: Gurgaon, ICIC0000177

[•] Essential fields

Signature _____ Date: Subscription No. (for renewal) _____

Order form can be mailed with payment (cheque/DD) to:

Cyber Media (India) Ltd, Cyber House, B-35, Sector-32, Gurgaon-122003

Contact: Alok Saxena, Tel: 0124-4237517 (Extn-347), 91+9953150474, Email: aloksa@cybermedia.co.in

For Subscription queries:

9289870545

Terms & Conditions: _____

• This offer is valid for a limited period. • Rates and offer valid only in India. • NEFT/UTR No., Email & Mobile number mandatory. • Please allow 4-6 weeks for delivery of your first copy of the magazine by post. • Send crossed Cheques in favour of Cyber Media (India) Ltd. • Please write your name and address on the reverse side of the cheque or DD. All outstation cheques should be payable at par. • Cyber Media (India) Ltd. will not be responsible for postal delays, transit losses or mutilation of subscription form. • Cyber Media (India) Ltd. reserves the right to terminate or extend this offer or any part thereof. The decision to accept or reject any or all forms received is at the absolute discretion of the publishing company without assigning any reason. • Please include pin code for prompt delivery of your copy. • In case payment is through credit card, date of birth must be mentioned. • All disputes shall be subjected to Delhi jurisdiction only.

Creating sustainable, scalable, secure data centre stacks

As India's digital load surges, data centres must go beyond uptime—cut energy costs, scale on demand, and embed zero-trust security.



BY SURESH BACHWANI

In India's rapidly evolving digital economy, the data centre has moved from being a back-end IT utility to the strategic core of enterprise operations. From real-time digital payments and telecom networks to manufacturing automation and government platforms, every critical service now depends on resilient, high-performing infrastructure.

Yet, as data volumes rise and regulatory expectations tighten, the data centre of the future must deliver more than capacity and uptime. It must operate responsibly, adapt at speed, and protect trust by design. In this context, three pillars define the modern data centre stack: sustainability, scalability, and security. Enterprises that embed these principles are not only improving operational efficiency but also strengthening resilience, regulatory readiness, and long-term competitiveness.

SUSTAINABILITY: FROM ESG MANDATE TO OPERATIONAL ADVANTAGE

Sustainability has become a boardroom priority for Indian

enterprises. With India's data centre capacity crossing 1,600 MW in 2024, energy efficiency and environmental impact are now central to infrastructure decisions. Industry estimates suggest that 40–50% of a data centre's operating costs are driven by power and cooling, making sustainability a financial concern as much as an environmental one.

A large Indian banking enterprise offers a relevant example. Faced with rising energy costs and internal ESG targets, the bank modernised its legacy data centre by consolidating workloads onto a hyperconverged, virtualised platform. The move reduced its physical server footprint, improved power usage effectiveness (PUE), and simplified energy monitoring across sites. Beyond cost savings, the transformation also enabled more structured ESG reporting, a demand increasingly expected by regulators and global investors.

Telecom operators managing high-density, latency-sensitive workloads are also adopting energy-efficient

hardware, intelligent cooling, and workload optimisation to balance growth with sustainability. For these organisations, sustainable IT operations are no longer aspirational; they are essential to protecting margins at scale.

Circular IT practices are gaining traction across Indian enterprises as well. Extending asset lifecycles, reusing refurbished components where viable, and ensuring compliant e-waste disposal are helping organisations reduce environmental impact while controlling capital expenditure. In many cases, these initiatives are now linked directly to corporate sustainability disclosures.

SCALABILITY: ARCHITECTING FOR INDIA'S NON-LINEAR GROWTH

India's digital demand curve is anything but predictable. Seasonal transaction spikes in BFSI, sudden capacity surges in telecom, and rapid adoption of AI and analytics across industries require infrastructure that can expand and contract without disruption.

A mid-sized Indian telecom provider illustrates this shift well. As subscriber data usage surged, the organisation moved away from a traditional three-tier architecture to a hybrid model combining on-premises hyperconverged infrastructure with public cloud resources. This enabled the telco to scale compute and storage dynamically, while keeping latency-sensitive workloads closer to the edge. The result was faster service roll-out, improved customer experience, and closer alignment between infrastructure spend and business demand.

This approach reflects a broader market direction. India's public cloud services market is projected to grow from USD 12.75 billion in 2024 to USD 25.5 billion by 2028, driven by enterprises seeking flexibility without sacrificing control. Hybrid architectures, containerisation, and software-defined infrastructure are increasingly becoming default design choices for organisations that need both agility and predictability.

Scalability, in this sense, is no longer about provisioning excess capacity. It is about architectural readiness: the ability to respond quickly to new business models, regulatory changes, and emerging technologies without repeatedly re-engineering the core.

SECURITY: TRUST AS THE FOUNDATION OF DIGITAL GROWTH

As digital adoption accelerates, security remains the

most critical and non-negotiable pillar of the data centre stack. Indian enterprises operate in an environment of heightened cyber risk, stricter compliance mandates, and increased scrutiny from customers and regulators.

Industry projections suggest India's cybersecurity market will grow from USD 6.87 billion in 2024 to over USD 20 billion by 2030, underscoring the scale of the challenge. High-profile breaches across sectors have reinforced the need for proactive security models rather than reactive controls.

Many BFSI and healthcare organisations are adopting zero-trust architectures, continuous monitoring, and integrated backup and disaster recovery as part of core infrastructure design. In one such case, a healthcare enterprise handling sensitive patient data implemented identity-centric access controls, network segmentation, and immutable backups. This reduced exposure to ransomware threats while supporting compliance with data protection norms.

Security must now be embedded across every layer: identity, network, workload, and data. A resilient data centre assumes incidents will occur and is engineered to detect, contain, and recover from them with minimal business disruption.

THE DATA CENTRE AS A STRATEGIC BUSINESS ENABLER

The role of the data centre in India is being fundamentally redefined. No longer a static facility, it is becoming a dynamic platform that supports growth, governance, and innovation simultaneously. The future-ready data centre stack is shaped by three essentials: sustainability aligned with energy-efficiency goals and ESG commitments; scalability that supports unpredictable growth and digital acceleration; and security built on zero-trust principles and continuous resilience.

For Indian enterprises, the question is no longer whether to modernise their data centres, but how strategically they do it. Organisations that invest early in sustainable, scalable, and secure architectures will be better positioned to manage risk, meet regulatory expectations, and support long-term digital growth. Ultimately, the modern data centre is no longer simply supporting the business; it is enabling it. 🌟

*The author is the Chief Technology Officer
at Orient Technologies.*

feedbackvnd@cybermedia.co.in



From threats to trust: How AI secures digital growth

As cyber threats evolve, AI is helping Indian D2C and B2C businesses turn digital vulnerabilities into resilience, trust, and sustained growth.



BY NITIN SHAH & MERRIL CHERIAN

As India's digital economy accelerates, Direct-to-Consumer (D2C) and Business-to-Consumer (B2C) organisations face growing cyber threats. With increasing online transactions, customer data collection, and omnichannel engagement, cyber resilience—the ability to anticipate, withstand, recover, and adapt to cyber incidents—has become a strategic imperative. Artificial Intelligence (AI) is emerging as a powerful enabler in this domain.

AI-driven solutions can significantly strengthen cyber resilience by enabling faster detection, contextual threat analysis, and adaptive response mechanisms. As cyberattacks grow in volume and sophistication, AI provides the scale and speed needed to manage threats that exceed human monitoring capabilities.

From anticipating breaches to orchestrating swift recovery, AI empowers organisations to make security operations smarter, leaner, and more responsive.

Predictive threat intelligence: Machine learning models analyse historical attack patterns and global threat feeds to predict emerging risks, enabling proactive defence. These models evolve as new attack vectors emerge, ensuring resilience against future threats.

Automated detection and response: AI-powered Security Information and Event Management (SIEM) systems can detect anomalies in real time, reducing response times from hours to seconds.

Behavioural analytics: AI can monitor user and system behaviour to identify deviations indicative of

Adaptive security powered by AI enables real-time response to cyber threats while aligning with compliance and business risk priorities.

insider threats or account takeovers, critical for sectors handling sensitive consumer data.

Adaptive security posture: AI enables a dynamic, intelligence-driven approach to cybersecurity in which defences continuously evolve based on real-time threat intelligence, risk assessments, and business context. Unlike static security models, adaptive security anticipates changes in the threat landscape and adjusts controls accordingly, a critical factor for achieving cyber resilience.

Enhanced recovery capabilities: AI significantly improves organisational recovery from IT system disruptions. AI systems implemented by organisations have demonstrated their efficacy in reducing downtime through automated problem detection and resolution.

Furthermore, AI can facilitate automated backups and restore processes, ensuring minimal data loss and service interruption. Organisations that have integrated AI into their recovery strategies report enhanced resilience and faster recovery times, thereby maintaining operational continuity and safeguarding critical assets.

For D2C and B2C businesses, these capabilities translate into safeguarding customer trust, minimising downtime, and ensuring compliance with data protection regulations, such as India's Digital Personal Data Protection Act.

CYBER RESILIENCE DRIVING AI ADOPTION

Interestingly, cyber resilience does not just benefit from AI—it also accelerates AI adoption. Organisations hesitant to deploy AI often cite concerns about data security and operational risks.

A robust cyber resilience framework mitigates these fears by demonstrating the organisation's ability to manage and contain cyber risks, thereby enabling safer experimentation and deployment of AI systems. Confidence in resilience encourages stakeholders to support AI initiatives, knowing that disruptions can be managed effectively.

Securing AI models and data pipelines: Protecting training data and algorithms from tampering builds

confidence in AI integrity. Implementing encryption, access controls, and integrity checks helps prevent unauthorised manipulation of training datasets or algorithms. By safeguarding these components against tampering, organisations ensure trustworthy outputs, maintain compliance, and build confidence in AI-driven decisions, reinforcing resilience and reliability across digital ecosystems.

Ensuring business continuity: Resilient systems reduce the perceived risk of disruptions in AI-driven automation during cyber incidents. By leveraging predictive analytics, organisations can anticipate potential failures and proactively address vulnerabilities. Using machine learning and AI tools, historical and real-time data can be analysed to identify patterns and anomalies, enabling faster diagnosis and issue resolution.

Regulatory alignment: Demonstrating resilience helps organisations meet compliance standards, making AI deployments smoother and less risky.

As trust in digital infrastructure grows, businesses are more willing to integrate AI into customer experience, personalisation, and supply chain optimisation—key differentiators in competitive D2C and B2C markets.

For Indian organisations, the synergy between AI and cyber resilience is not optional—it is foundational. Investments in AI-powered cybersecurity tools, coupled with a resilience-first mindset, will define the winners in an era where consumer trust is paramount.

By embedding AI into security strategies today, businesses can future-proof themselves against tomorrow's threats while unlocking the full potential of digital transformation. 🧩

Shah (left) is Partner – Digital Trust and Head – Cyber Security, Resilience and Privacy GRC, and Cherian is Partner – Digital Trust and National Leader – Cyber Resilience at KPMG in India.
feedbackvnd@cybermedia.co.in



5G FWA growth drives a modest wireless subscriber uptick

TRAI's November 2025 data shows wireless growth led by Jio and Airtel, as 5G FWA expands and Vi and MTNL continue to lose users.



BY AYUSHI SINGH

The Telecom Subscription Data, recently released by the Telecom Regulatory Authority of India (TRAI), indicates that telecom service providers Bharti Airtel, Bharat Sanchar Nigam Limited (BSNL), and Reliance Jio added wireless subscribers in November 2025, while Vodafone Idea (Vi) and state-run MTNL reported net losses.

The total number of wireless subscribers, including mobile and Fixed Wireless Access (FWA), stood at 1,187.48 million at the end of November 2025, up from 1,184.62 million in October. This represents a month-on-month growth of 0.24%. The number of wireless mobile

subscribers also increased by 0.17%, rising from 1,171.87 million to 1,173.88 million over the same period.

TRAI noted that tele-density as of 30 November 2025 was calculated using population projections from the Report of the Technical Group on Population Projections for India and States 2011–36, published in July 2020. Data for earlier months was based on projections from the same report released in November 2019.

5G FWA RISE AND UBR MOMENTUM

The number of wireless 5G Fixed Wireless Access (FWA) subscribers rose from 9.91 million at the end of October

With active users at nearly 93% of the base, the market's next phase will be shaped by capacity, service quality, and FWA economics.

2025 to 10.41 million by the end of November. Of these, 5.32 million were in urban areas and 5.09 million in rural areas. Urban users accounted for 51.11% of the total 5G FWA subscribers, while rural users made up 48.89%.

As of November 2025, Reliance Jio reported 7,646,142 5G FWA subscribers, reflecting a net addition of 250,274 during the month. Bharti Airtel reported 2,765,883 subscribers, up 251,095 from the previous quarter. Reliance Jio also recorded 3,187,263 Ultra Broadband Radio (UBR) FWA subscribers, a monthly increase of 351,757, representing a 12.41% growth rate.

TRAI stated that Reliance Jio Infocomm Limited began disclosing its UBR FWA subscriber base in August 2025. By the end of November, total UBR FWA subscriptions stood at 3.19 million, including 2.26 million urban and 0.93 million rural connections. Urban subscribers accounted for 70.95% of the total, while rural subscribers made up 29.05%.

SUBSCRIBER ADDITIONS AND CHURN TRENDS

During November 2025, Reliance Jio added 1.39 million wireless subscribers, Bharti Airtel added 1.22 million, and BSNL recorded net additions of 0.42 million. In contrast, Vodafone Idea lost 1.01 million subscribers, while MTNL reported a decline of 7,530 subscribers.

TRAI noted that all licensed service areas (LSAs), except Himachal Pradesh, Jammu & Kashmir, Assam, and Haryana, recorded growth in wireless mobile subscribers during the month.

WIRELESS MARKET SHARE IN NOVEMBER

The TRAI report also indicates that as of 30 November 2025, private access service providers accounted for 92.06% of total wireless subscribers, while public-sector operators BSNL and MTNL together held a 7.94% market share.

Reliance Jio led the market with a 41.41% share and 486.09 million wireless subscribers, followed by Bharti Airtel at 33.64% with 394.88 million subscribers. Vodafone Idea held 17.01% with 199.71 million users, BSNL accounted for 7.92% with 92.96 million

subscribers, and MTNL held a marginal 0.02% share with 0.24 million users.

In terms of wireless broadband subscribers (including mobile and fixed wireless), Reliance Jio reported 496.92 million users as of November 30, 2025, followed by Bharti Airtel with 304.21 million, Vodafone Idea with 127.74 million, and BSNL with 29.4 million.

ACTIVE USERS AND VLR INDICATORS

On the peak Visitor Location Register (VLR) date in November 2025, 1,090.91 million of the 1,173.88 million wireless mobile subscribers were active. TRAI said active users accounted for approximately 92.93% of the total wireless subscriber base.

During the month, Airtel recorded a peak VLR of 98.81%, Reliance Jio had 98.15%, Vodafone Idea had 84.59%, BSNL had 58.47%, and MTNL had 144.76%. TRAI clarified that VLR data forms the basis for estimating active wireless subscribers.

Overall, the November 2025 data points to a steady recovery and consolidation in India's wireless market, led primarily by Reliance Jio and Bharti Airtel. The net subscriber additions, coupled with rising Fixed Wireless Access (FWA) adoption, indicate growing demand for data-centric and home broadband alternatives, particularly 5G-based services.

Jio's strong momentum across both 5G FWA and UBR highlights its strategy of leveraging advanced networks to deepen broadband penetration, while Airtel's gains reflect continued competitiveness in urban and premium segments. In contrast, ongoing subscriber losses for Vodafone Idea and MTNL underline persistent financial and network challenges.

The high proportion of active users and the expanding role of FWA also suggest that future growth will be driven less by basic connectivity and more by quality, capacity, and integrated mobile, broadband offerings across urban and rural India. 🌐

ayushis@cybermedia.co.in

India plans vehicle-to-vehicle communication by 2026

With V2V tech, cars may soon 'talk' to each other, sharing warnings to avoid crashes—part of a national push for road safety.



The Ministry of Road Transport and Highways plans to make vehicle-to-vehicle (V2V) communication mandatory in India by the end of 2026, Union Minister Nitin Gadkari has announced after a two-day meeting with state transport ministers and officials from 28 states and Union Territories.

The proposed system, aimed at reducing road collisions, will require all vehicles to be equipped with on-

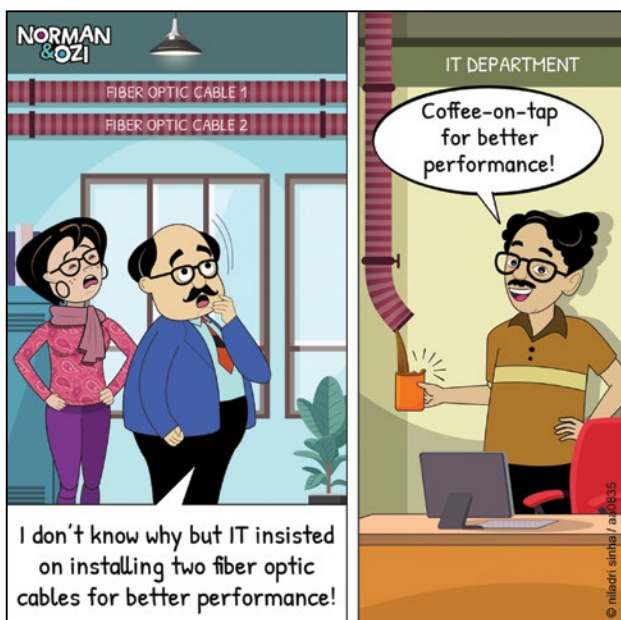
board units (OBUs) that wirelessly transmit location, speed, braking, and direction data to nearby vehicles. The alerts are designed to warn drivers about potential hazards before they are visible—including sudden braking, stationary vehicles, and traffic in blind spots.

Gadkari said the Department of Telecommunications has agreed in principle to allocate 30 MHz spectrum in the 5.875–5.905 GHz band to support the V2V system. A joint task force with the DoT has been set up to oversee implementation.

Initially, the mandate will apply to new vehicles, with retrofitting of older vehicles, particularly buses and trucks, expected in later phases. The cost of OBUs is estimated between Rs 5,000 and Rs 7,000 per vehicle. Technical standards are under development with automakers, Road Transport Secretary V Umashankar said.

The initiative is part of India's broader goal to halve road fatalities by 2030. India recorded over five lakh road accidents in 2023, resulting in more than 1.7 lakh deaths.

However, challenges remain. Experts point to the high costs, lack of global standardisation, and the tight timeline. While many countries have allocated spectrum for V2V, large-scale deployment remains limited.



YOUR CUSTOMERS ARE EVOLVING. LET YOUR BRAND LEAD WHERE IT MATTERS MOST. CYBERMEDIA'S INTEGRATED GO-TO-MARKET ENGINE PROVIDES INFLUENCE, VISIBILITY, AND HIGH-INTENT LEADS ACROSS INDIA'S MOST TRUSTED TECH MEDIA PLATFORMS.

LEAD THE CONVERSATION USING CYBERMEDIA'S 360° GTM STRATEGY. UNMATCHED REACH ACROSS OUR FLAGSHIP BRANDS



DATAQUEST
Enterprise &
Tech Leadership



PCQUEST
CIOs, Tech
Influencers & SMBs



VOICE&DATA
Telco & Digital
Infra Leaders



DQCHANNELS
ICT Partners &
Channel Decision Makers

OUR BESPOKE B2B MARKETING PROGRAMS BUILD, ENGAGE AND SCALE COMMUNITIES

Account-Based CXO Connects & C-Level Roundtables | Content-Led Thought Leadership Campaigns | Audience Segmentation Across IT & Business Decision Makers | Print, Digital, Event, Podcast & Research Integration | Measurable ROI & Lead-Nurturing Programs

High-Impact Verticals We Specialize In: Cloud & Multi-Cloud Solutions | Cybersecurity & Risk Management | Data, AI & Advanced Analytics | Enterprise IT Infrastructure & SaaS | Telecom, 5G & Network | SMBs & Mid-Market Technology Buyers | Transformation | Sustainability & Green IT | Channel Ecosystem: VARs, MSPs, Distributors, Sis | SMBs & Mid-Market Technology Buyers

DELIVER INFLUENCE AND OUTCOMES WITH CYBERMEDIA

42+ Years of Tech Publishing Legacy | Deep CXO Access & Vertical Intelligence | Custom Campaigns with Content + Conversion Focus | Trusted by Top Global & Indian IT Brands

LET'S BUILD SMART, VERTICAL-LED CAMPAIGNS THAT TURN YOUR BRAND MESSAGE INTO MEASURABLE BUSINESS IMPACT.

www.dqindia.com | www.pcquest.com | www.voice&data.com | www.dqchannels.com



Apeejay Institute of Management & Engineering Technical Campus, Jalandhar | Estd. in 1997

Affiliated to I.K Gujral Punjab Technical University (IKG-PTU), Kapurthala
Approved by AICTE, MOE | NAAC Accredited



REGISTRATIONS OPEN 2026

Build a successful career with **AIMETC**

PROGRAMMES OFFERED



MANAGEMENT

- MBA (2 years)
- BBA (3 years)
- B.Com (H) (3 years)



COMPUTER APPLICATION

- MCA (2 years)
- BCA (3 Years/2 Years*) (*for lateral entry)



ENGINEERING & TECHNOLOGY

- 4 years/3 years*** (*for lateral entry)
- B.Tech. - Computer Science & Engineering (CSE)
- B.Tech. - CSE (Artificial Intelligence & Machine Learning)
- B.Tech. - CSE (Internet of Things & Cyber Security including Block Chain Technology)

SOME OF OUR KEY RECRUITERS



Disclaimer: We offer only placement assistance. Placements may vary with industry requirements, market sentiment and student merit.

Scan for website



For more details, please contact us:

Apeejay Institute of Management & Engineering Technical Campus, Rama Mandi,
Hoshiarpur Road, Jalandhar -144007
Email: aim.jln@apj.edu | Phone: +91-9569-181-181