

VOICE & DATA

Connecting the Digital World

CyberMedia

Private 5G: Forging the factory of tomorrow

As Industry 5.0 moves from pilots to plants, low-latency networks, physical AI, and robotics are reshaping work, safety, resilience, and industrial scale.



Satellite links **08**
to anchor
India's digital
next phase
by P J Nath
CEO – Nelco



Machine- **18**
to-machine
networks need
coherence
by Lt Gen Dr S P Kochhar
DG – COAI



India's **28**
digital rise
runs into an
energy wall
by T V Ramachandran
President – BIF





APEEJAY SCHOOL

Nerul, Navi Mumbai | Estd. in 1986 | CBSE Affiliated



Foundation For Lifelong Learning Starts Here

ADMISSIONS OPEN 2026-27

PRE – NURSERY TO IX & XI



+91-7303096829

www.apeejay.edu/nerul/



KEY HIGHLIGHTS



Value-based holistic education



Curriculum aligned with
NEP 2020



State-of-the-art infrastructure



Focus on experiential and
competency-based learning



Safe & secure campus



Awarded for 'Innovation in Curriculum' during the
2nd World Education Edtech Conclave 2023

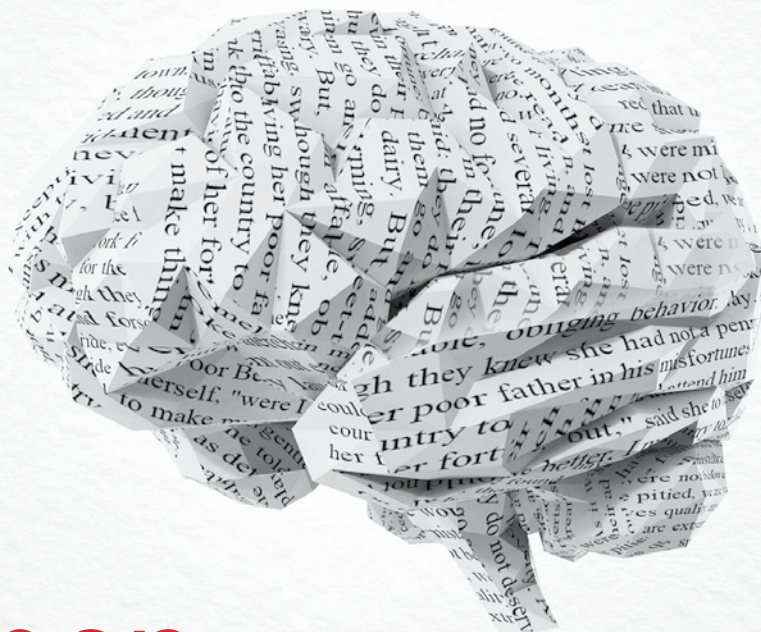
For more details, please contact us:

Apeejay School, Sector-15, Nerul, Navi Mumbai - 400706

Email: skool.nrl.by@apj.edu

Follow us on:





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
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

GM - EVENTS OPERATIONS & PROJECT: 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 RBANMS 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)

May 2026

[CONTENTS]

COVER STORY 22

Private 5G: Forging the factory of tomorrow



As Industry 5.0 moves from pilots to plants, low-latency networks, physical AI, and robotics are reshaping work, safety, resilience, and industrial scale.

INDUSTRY SPEAK

- 08** Satellite links to anchor India's digital next phase
- 11** Platform design liability challenges safe harbour norms
- 14** Wireless closes the gap with fibre-class connectivity
- 16** Payment networks brace for the next wave of digital fraud

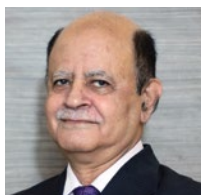
[TECHNOLOGY]

- 32** Smart meters need networks, not just more devices
- 35** Tactical 5G redraws the defence communication grid
- 38** Enterprise networks fail where trust layers fragment

[COMMENTARY]

- 64** Beyond BharatNet: Building resilient rural networks
- 67** CCTV shifts from surveillance to security risk
- 71** India's new online gaming rules end grey zones

TELECOM TALK



- 18** Machine-to-machine networks need coherence, not silos
- LT. GEN. DR. SP KOCHHAR**

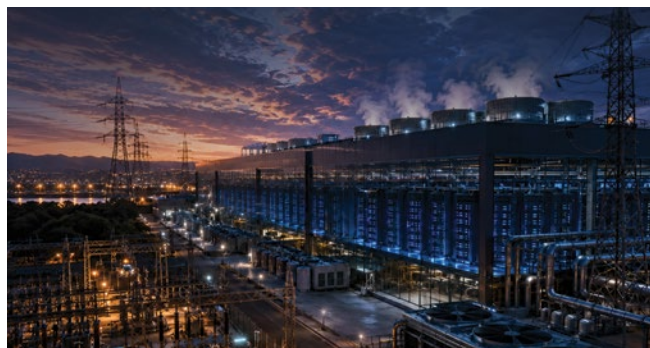
BROADBAND BYTES



- 28** India's digital rise runs into an energy wall
- TV RAMACHANDRAN**

FOCUS

- 42** Chasing AI supremacy through power-hungry server farms



ANALYSIS

- 48** The next telecom superpower may operate from orbit
- 54** India's quantum push needs telecom-scale networks
- 57** Fibre-ready buildings gain a new edge in property value
- 60** Chip reliability critical in the connected world

REGULARS

- 06** Voicemail
- 07** Opening Note
- 74** Postscript

[NEXT ISSUE]



APRIL 2026

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



FEEDBACK
From Online Readers

Share your views at vndedit@cybermedia.co.in

**NEXT
ISSUE**

DATA CENTRE & EDGE EXPANSION



For any query: ajaydh@cybermedia.co.in



SHUBHENDU PARTH [OPENING NOTE]

From launchpads to boardrooms, space finds scale

Skyroot Aerospace has become India's first space-tech unicorn. However, this is more than just a funding milestone. It is a signal that India's space sector has crossed an invisible but critical threshold. For decades, the country's space ambitions were shaped almost entirely by the government, guided by the Indian Space Research Organisation (ISRO) with discipline, scientific austerity, and quiet conviction. Today, that legacy is beginning to power a new era in which private enterprise is not merely supporting the ecosystem but helping define it.

The timing is significant. Skyroot's unicorn status comes just ahead of the expected launch of Vikram-1, India's first privately developed orbital rocket. That sequence matters because it demonstrates that investors are now backing not just ideas or prototypes, but execution capability. In India's deep-tech ecosystem, such transitions are rare. They demand patience, technical stamina, and the willingness to build what Henry David Thoreau may have called "castles in the air" and then place foundations beneath them.

India's space-tech story is no longer confined to prestige missions or scientific symbolism. It is increasingly about industrial capability, strategic infrastructure, and commercial competitiveness. Nearly 400 space-tech startups are now operating across launch systems, satellite manufacturing, earth observation, propulsion, communications, analytics, and downstream applications.

Companies such as Skyroot Aerospace, Agnikul Cosmos, Pixxel, and GalaxEye are beginning to create specialised capabilities that could eventually integrate into a larger national space manufacturing ecosystem.

This growth has not happened accidentally. Regulatory reforms such as the Indian Space Policy 2023 and the creation of IN-SPACe have fundamentally altered the operating environment. Access to ISRO infrastructure, liberalised foreign investment norms, and clearer authorisation frameworks have helped reduce uncertainty for private players. The government deserves credit for recognising that the future space economy cannot be built only through a closed institutional model.

Besides, another real opportunity is emerging in India's space sector, particularly in satellite communications. The emerging satcom battle could reshape the country's digital infrastructure landscape as dramatically as mobile telephony did two decades ago. Starlink, Eutelsat, OneWeb, and Jio Space Technology are all preparing for large-scale deployment in India. What appears today as a spectrum and licensing debate is, in reality, a battle over who will control the next layer of connectivity infrastructure.

The implications are profound. Satcom is no longer just about remote villages or maritime links. It is becoming central to aviation, defence communications, emergency response systems, IoT networks, financial inclusion, and future non-terrestrial 6G architectures. The convergence between terrestrial telecom and satellite broadband will create new alliances, new competitive tensions, and new policy challenges.

Yet, India must avoid reducing its space ambitions to a race for valuations alone. Unicorn status is important, but sustainable capability matters more. Launch systems, satellite constellations, propulsion technologies, chip ecosystems, secure communication layers, and the depth of sovereign manufacturing will determine whether India becomes merely a market for global players or a genuine space power.

Skyroot's rise suggests the country may finally be ready for the latter.

shubhendup@cybermedia.co.in

Satellite links to anchor India's digital next phase

AI, cloud, and edge expansion will require hybrid satellite-fibre networks that can keep India's digital infrastructure resilient nationwide at scale.



BY P J NATH

India's technology sector spent decades building global leadership in IT services. Today, attention is gradually shifting towards what the next phase of the country's technological evolution might look like. The country is transitioning from managing global code to owning the innovation-heavy, infrastructure-intensive systems that now define global digital leadership, including hyperscale cloud platforms, artificial intelligence, deep tech and semiconductor design.

The recent Boston Consulting Group and NASSCOM report, India Tech's Next Innings, brings this shift into focus. While India's technology sector has crossed the USD 300 billion mark, the real opportunity now lies in how effectively the country positions itself within the emerging USD 8.4 trillion global market centred on IP-led innovation and advanced digital infrastructure.

Yet, as we set our sights on this ambitious horizon, we must confront a foundational question that too

often remains in the background: What holds this ambition together?

The answer is connectivity, not as an afterthought, but as a strategic enabler. A technology ambition of this magnitude cannot sit on a fragile wire. Hyperscale cloud ecosystems, distributed data centres, real-time AI workloads, and mission-critical industrial systems demand networks that are resilient, redundant, and relentlessly reliable across India's vast and varied geography.

In India's case, that scale and diversity call for an architecture that combines terrestrial networks with satellite communication. And that is where satellite communication (satcom) moves from being a niche, supplementary option to a strategic pillar of India's digital future.

THE HIDDEN LAYER OF DIGITAL GROWTH

Every digital interaction today creates data. AI models consume compute at a scale unimaginable a decade ago.

As AI workloads, cloud expansion, and edge systems scale nationwide, resilient satellite-fibre connectivity will become the backbone of India's next digital infrastructure phase.

Enterprises are shifting their most sensitive workloads to the cloud, and governments are scaling digital public infrastructure that touches millions of citizens daily.

These forces are driving a sharp rise in demand for data centre capacity. India's data centre ecosystem is expanding rapidly, with hyperscale facilities emerging across established technology hubs and new industrial corridors. But the next phase of growth will not be about adding more server racks in a few cities. It will be about creating distributed data centre clusters—interconnected, high-availability networks that span the length and breadth of the country.

As these systems scale, the resilience of the networks linking them becomes just as critical as the computing power housed within the facilities. A data centre without robust, redundant connectivity is not a strategic asset; it is a stranded asset.

GEOGRAPHY SHAPES NETWORK STRATEGY

India's geography presents both opportunities and complexities for digital infrastructure. Coastal regions are emerging as attractive locations for hyperscale facilities due to their proximity to subsea cables, while industrial corridors, offshore assets, island territories, and remote zones are becoming increasingly data-intensive. Reaching this expanding ecosystem remains a challenge. And we have vast stretches of land where fibre deployment is slow, costly, and vulnerable to disruption.

For critical infrastructure that cannot afford downtime, even a brief connectivity gap can cascade into operational failure, financial loss, and erosion of trust. Dependence on a single layer of infrastructure in a country as diverse and dynamic as India is a risk we can no longer afford.

This is where satellite communication changes the calculus. A hybrid model that integrates fibre and multi-orbit satellite networks builds resilience through diversity.

EXTENDING CONNECTIVITY TO THE EDGE

Cloud infrastructure is no longer limited to large data centres in major cities. While hyperscale facilities remain central, more data is now being generated where economic activity happens, at the edge.



IN BRIEF

- India's next technology phase depends on resilient hybrid connectivity, not terrestrial networks alone.
- Distributed data centres need redundant satellite-fibre links to avoid becoming isolated infrastructure assets.
- Satcom can connect industrial corridors, offshore assets, and remote digital operations at scale.
- GEO and LEO satellite networks together can extend low-latency connectivity across difficult geographies.
- AI, cloud, and edge computing growth will increase demand for always-on, multi-layered network resilience.
- Policy, skilling, and industry collaboration will shape Satcom's role in India's digital infrastructure future.

Factories, ports, logistics hubs, and offshore energy sites are now run on sensors and automated systems that produce continuous streams of operational data. Much of this data requires real-time analysis to optimise efficiency, predict failures, and ensure safety. Yet many of these locations operate far from traditional network hubs, making reliable connectivity a persistent challenge.

Satellite communication bridges this gap. By complementing terrestrial networks, it ensures that distributed and remote operations are seamlessly connected to central cloud platforms. This allows India's

Satellite communication is shifting from a niche backup layer into a strategic infrastructure that can support distributed cloud, AI, industrial, and edge operations.

digital infrastructure to extend well beyond metropolitan clusters, turning the vision of a truly pan-India digital economy into a practical reality.

When a refinery in a remote coastal area, a logistics hub in a developing corridor, and a data centre in a major city can function as a single, integrated system, we unlock efficiencies and capabilities that were previously out of reach. That is the power of a hybrid connectivity architecture.

SUPPORTING INDIA'S TECHNOLOGY BETS

The BCG report calls for bold investments in areas that will shape India's next phase of technology leadership: hyperscale infrastructure, advanced computing, deep tech, and more. These ambitions require not just capital, but coordinated, resilient, and forward-looking infrastructure. Connectivity underpins this vision. Satellite networks enhance redundancy, secure distributed workloads, and ensure that India's data infrastructure can continue to scale without geographical constraints.

But realising this potential will require more than technology. It will require deep public-private collaboration, particularly as the space, telecom, and cloud industries converge. The lines between these sectors are blurring, and the policy frameworks that govern them must evolve to recognise the strategic importance of Satcom in strengthening national digital infrastructure.

BUILDING THE ECOSYSTEM FOR GROWTH

Infrastructure alone will not define our future, but the lack of it will certainly limit it. The road ahead requires a holistic ecosystem that brings together talent, regulation, and collaboration. Engineers and technologists with expertise in hybrid networks, satellite systems, and cloud architectures will be in increasing demand, making investments in skilling and education critical for building long-term capability.

Policy frameworks must also evolve to recognise that satellite communication is no longer a niche segment, but a strategic pillar of national digital infrastructure. This will require greater regulatory clarity, consistency, and a forward-looking approach to governance. Equally important is collaboration. No single entity can build this future alone; industry, government, and academia will

need to work together to develop solutions, establish standards, and share best practices.

Satellite communication sits at the intersection of these emerging priorities. As hybrid networks become the norm, the sector will require new capabilities, smarter analytics, and a broader understanding of Satcom's role in strengthening national digital infrastructure.

HYBRID NETWORKS FOR THE NEXT PHASE

India's first phase of technology growth put us on the global map. It demonstrated our ability to deliver services at scale. What comes next—powered by ownership of platforms, intellectual property, and mission-critical hybrid infrastructure—will see us leading the world.

Data centres and hyperscale cloud platforms will anchor this transformation, but their success depends on resilient, scalable networks. Satellite communication is now poised to play a far greater role in this architecture—not as a single solution, but as a multi-modal, multi-orbit ecosystem.

The convergence of Geostationary (GEO) satellites, which provide wide coverage and persistent connectivity, with Low Earth Orbit (LEO) constellations, which deliver low latency and high throughput, creates a powerful continuum. Together, they enable a hybrid fabric that complements terrestrial infrastructure and extends seamless connectivity across even the most challenging geographies.

As we move toward a future defined by infrastructure ownership and deep tech innovation, our connectivity models must evolve beyond point solutions. A truly resilient digital backbone will be built on a multi-modal approach—integrating fibre, GEO, LEO, and emerging non-terrestrial networks into a cohesive, intelligent architecture.

This is not just an option; it is the foundation on which India will build a truly unshakeable digital ecosystem. In fact, the next innings is for India to define. Let the country build it on a foundation that can carry the weight of its ambition. 🌟

The author is the Managing Director and Chief Executive Officer of Nelco.
feedbackvnd@cybermedia.co.in



Platform design liability challenges safe harbour norms

US court verdicts and India's evolving laws may expand platform liability beyond hosted content, bringing algorithms and addictive design under scrutiny.



BY VIKRAM JEET SINGH & PRACHI RUNGTA

Algorithms designed to attract users can also attract liability.

Two landmark US court verdicts in March 2026 may signal a shift in the law relating to platform liability, though the legal position may have moved from “platforms are mere conduits” to one where “platforms are products, and their makers can be sued”.

For technology companies operating in India, the next critical question is whether the Indian legal framework supports similar claims and, if so, how they may present themselves.

US VERDICTS TEST SAFE HARBOUR RULES

Typically, Section 230 of the US Communications Decency Act, 1996, shields online intermediaries from

The debate is moving from content moderation to design accountability, especially when children's data, behaviour, and well-being intersect online in law.

Algorithms, autoplay, infinite scroll, and alerts are becoming legal questions, not merely design choices for stronger platform engagement and retention.

liability for third-party content. This provision has, so far, been effective in protecting major digital businesses from liability for content posted on their platforms. Equivalents of this intermediary safe harbour protection can be found in laws across the world, including Section 79 of India's Information Technology Act, 2000.

On 25 March 2026, in KGM v. Meta and YouTube, a Los Angeles jury found that a platform's addictive design caused harm to a young user and awarded USD 6 million in damages. The jury's verdict focused on the "addictive design" element of social media and online content platforms.

Meta and Google have indicated that they intend to appeal the decision. Interestingly, KGM did not challenge the user-generated content, but attacked the platforms' in-built architecture. By framing the matter as a product liability claim rather than a content-moderation issue, the plaintiffs successfully circumvented safe harbour.

A day earlier, on 24 March 2026, the New Mexico Attorney General secured a civil penalty of USD 375 million against Meta under the state's Unfair Practices Act. This was a state-led consumer protection action rather than a private tort action. That said, it rested on similar foundations: addictive design leading to harm, regardless of the content being carried.

GLOBAL REGULATORS TARGET DESIGN HARMS

The regulatory environment in many other countries is moving in a similar direction. In the United Kingdom, the Online Safety Act requires platforms to map out the "risk of harm" to children.

This mandate forces companies to assess not only the content users post, but also whether the platform's own design, such as algorithms that create addictive feedback loops, increases the likelihood of psychological or physical harm.

On 6 May 2026, the European Commission held TikTok's features, including infinite scroll, autoplay, push notifications, and personalised recommendations, to be in preliminary breach of the Digital Services Act.



IN BRIEF

- US courts suggest addictive platform design may bypass safe harbour by shifting claims away from user-generated content liability.
- India's DPDP Act could become a key trigger for claims involving children's data, behavioural monitoring, and targeted advertising.
- The Consumer Protection Act may offer two routes: deficient service claims and stricter product liability for defective design.
- Indian courts may need to decide whether algorithms and digital platforms can be treated as products under existing consumer law.
- Product liability could lower the burden on claimants by focusing on inherent design defects rather than proving negligence.
- Platform architecture is becoming a compliance and liability issue, extending scrutiny beyond the content hosted online.

Courts in India may have to decide whether digital architecture can be treated as a product capable of causing measurable legal harm to young online users.

INDIA'S REGULATORY RESPONSE TAKES SHAPE

In March 2026, Karnataka became the first Indian State to announce a ban on social media access for children under 16. Around the same time, the National Human Rights Commission issued notices to the Ministry of Electronics and Information Technology over alleged violations of the Digital Personal Data Protection (DPDP) Act, 2023.

Section 9 of the DPDP Act prohibits the processing of children's personal data in a manner likely to cause any "detrimental effect" on a child's well-being. It also specifically forbids behavioural monitoring and targeted advertising directed at children.

The commission noted the absence of systems to track children's data transfers and inadequate grievance redressal mechanisms as non-compliances.

FROM REGULATORY BREACH TO ACTIONABLE HARM

An Indian action in tort, similar to the one in the US, is one possibility. One possible argument is that platforms owe a duty of care to child users, that deploying addictive design features breaches that duty, and that such a breach causes harm.

Indian tort jurisprudence, however, is not as developed as that of the United States. A product design claim in India would likely depend on a prior finding of breach under the DPDP Act to support causation and withstand scrutiny. The Consumer Protection Act (CPA), 2019, offers a second avenue, with two distinct frameworks.

The first is the services framework. Under Section 85 of the Act, a service provider is held liable where the service was faulty or deficient, or where negligence or conscious withholding of information caused harm. This route requires a factual link between the platform's conduct and the specific harm suffered.

There also remains a threshold question of applicability. Section 2(42) of the Act expressly excludes services rendered "free of charge". Whether user data or user attention constitutes consideration sufficient to bring social media within this definition is still being tested under Indian law.

The second framework relates to product liability. The CPA's product liability framework is set out under Chapter VI, Sections 82 to 87. Section 84(1)(b) imposes strict liability on the manufacturer of a product with a design defect. In contrast, Section 84(2) makes clear that this liability attaches even where the manufacturer proves it was not negligent.

The product liability regime operates on a materially lower threshold than the services framework, which requires proof of deficiency or negligence.

If a platform's recommendation algorithm could be classified as a product, a claimant in India would not need to prove negligence at all. The claimant needs only to show that the inherent design was defective and caused harm. Whether this classification holds depends on how courts interpret the definition of "product".

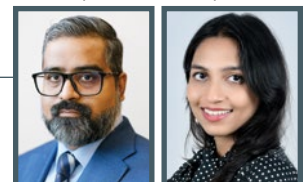
On a literal reading, Section 2(33) suggests that a product must be an article or goods in a tangible state, whether gaseous, liquid, or solid. However, the Act also relies on the broader definition of "goods" under Section 2(21) as "every kind of movable property". The Consumer Protection Act itself explicitly envisages "digital products" within its e-commerce provisions, although it stops short of defining them.

This creates an interpretive opening for Indian courts: should the definition of a product be read narrowly in terms of its physical state, or broadly to encompass digital platforms and assets?

Platform design, then, is itself becoming a liability and compliance issue, in addition to the content actually hosted on the platform.

In India, the question is mixed: whether a viable liability framework exists and whether the judiciary will recognise platforms as engineered products capable of causing actionable harm through defective design. 🧩

The authors, Singh (left) and Rungta, are Partner and Associate, respectively, at BTG Advaya. feedbackvnd@cybermedia.co.in



Wireless closes the gap with fibre-class connectivity

As digital operations spread across distributed locations, next-generation wireless is delivering agile, reliable fibre-class connectivity at scale.



BY VINOD BABU BOLLIKONDA

For many years, fibre has been the benchmark for high-quality connectivity. It has stood for speed, stability, and low latency, and for good reason. Enterprises, public institutions, and service providers have relied on fibre to support critical digital operations, cloud access, collaboration, and increasingly data-intensive workloads. But the connectivity landscape is evolving.

Today, next-generation wireless technology is narrowing the gap so effectively that organisations can now achieve fibre-class performance in places where laying fibre is slow, costly, or impractical.

This shift matters because connectivity is no longer just a technical layer. It is becoming a strategic enabler of business continuity, customer experience, and digital expansion. The ability to deliver reliable, high-performance access without depending entirely on

physical cabling is changing how networks are designed, deployed, and scaled.

FROM HEAVY TO LIGHT INFRASTRUCTURE

Historically, extending high-capacity connectivity has required significant physical infrastructure. Fibre deployments often involve trenching, permits, civil construction, and extended planning cycles. While this model remains essential for backbone networks, it can introduce delays when organisations need to connect distributed operations quickly across campuses, branch networks, logistics hubs, industrial environments, or emerging markets.

This is where infrastructure-light wireless architectures are gaining importance. By reducing dependence on physical buildout, they enable the extension of enterprise-grade connectivity with far greater speed and flexibility. For organisations operating

across campuses, branch networks, logistics hubs, industrial sites, or underserved regions, that flexibility is transformational.

The practical advantage is straightforward: networks can be launched faster, expanded more easily, and adapted to changing demand without waiting for the full fibre rollout cycle. In an environment where digital services are expected to be always available, that kind of agility is no longer a luxury. It is a competitive requirement.

The real significance of next-generation wireless lies not only in the speeds it can achieve, but in the range of business applications it enables. When wireless networks deliver consistent throughput, low latency, and stable performance, they can support enterprise-grade digital workloads.

This shift is already influencing multiple industries. In education, it supports connected classrooms and digital learning platforms. In healthcare, it enables telehealth services, remote diagnostics, and real-time access to clinical systems. In retail and logistics, reliable connectivity can support branch operations, supply chain visibility, and mobile workforce coordination.

Across public services and enterprise environments, it helps extend digital services to regions where fibre infrastructure remains limited or under development.

As a result, wireless connectivity becomes more than an access mechanism—it becomes a multiplier of digital capability. Organisations gain the flexibility to deploy services across more locations, operate more efficiently, and accelerate digital initiatives without the limitations of physical infrastructure timelines.

Ultimately, network performance is no longer judged solely by the presence of connectivity. It is measured by whether that connectivity can sustain mission-critical workloads under real operating conditions. Wireless technologies capable of delivering fibre-class performance significantly expand where and how organisations can operate digitally.

REDEFINING NETWORK DEPLOYMENT COSTS

Another important outcome of this transition is its impact on network economics. Historically, network expansion has been heavily influenced by infrastructure cost and construction timelines. Extensive physical buildouts often slow deployment and increase capital requirements.

Next-generation wireless introduces a more flexible approach to network design. Organisations can adopt hybrid architectures that combine wired and wireless connectivity, selecting the most appropriate technology based on geography, deployment timelines, and operational requirements.

Hybrid connectivity strategies also improve resilience. Networks that combine fibre and advanced wireless access can support redundancy and continuity planning more effectively, helping organisations maintain reliable services even when a single connectivity path is disrupted.

For decision-makers, the strategic question is no longer whether wireless should replace fibre entirely. Instead, the focus shifts to identifying where fibre remains essential, where wireless can extend coverage, and where wireless solutions can deliver comparable outcomes with greater deployment efficiency.

THE NEXT PHASE OF ENTERPRISE ACCESS

Connectivity is entering a more dynamic phase. As enterprises expand distributed operations, adopt cloud-native architectures, and support increasingly mobile workforces, the traditional assumption that high-performance connectivity must always rely on physical fibre is gradually evolving.

Next-generation wireless is not simply a substitute for fibre infrastructure. In many scenarios, it provides a more agile way to deliver comparable levels of reliability and performance while reducing dependence on extensive physical buildout.

The future of enterprise networking will likely be hybrid by design. Fibre will continue to anchor high-capacity backbone networks, while wireless technologies will rapidly extend connectivity across distributed environments.

In that sense, the real transformation is not that the fibre is disappearing. It is that fibre-class performance is no longer confined to fibre-only deployments. This shift opens the door to a broader, more flexible approach to digital connectivity and enterprise transformation. 🌐

*The author is the Group CEO of Blue Cloud
Softtech Solutions.*

feedbackvnd@cybermedia.co.in



Payment networks brace for the next wave of digital fraud

As digital payments and machine-led transactions scale rapidly, India's real-time payment ecosystem faces increasing pressure to detect fraud in real time.



BY ARBAAZ JAMAL

India's digital payments story is defined by scale, speed and global leadership, not just adoption. UPI has taken the lead in this and has emerged as the world's largest real-time payments system. Media reports indicate that in January 2026, UPI processed 21.7 billion transactions worth Rs 28.33 lakh crore. UPI emerged as the world's largest real-time retail payment

system, accounting for 81% of retail digital payments in FY 2024-25, according to India's Ministry of Finance.

The payment ecosystem is becoming more complex as it has evolved from mobile-first payments to machine-led transactions powered by Internet of Things (IoT) devices, wearables and connected systems. With this

India's payment ecosystem is moving beyond smartphones into wearables, vehicles, and IoT systems, significantly expanding fraud risks.

As transactions become increasingly invisible and automated, fraud detection must operate continuously across devices and payment networks.

rapid expansion, the real question is whether India's payment infrastructure is equally prepared for the next wave of transaction fraud.

FRAUD RISKS RISE WITH PAYMENT SCALE

India's payments ecosystem is now operating at unprecedented scale, bringing new challenges. According to government data, in just the first 10 months of 2025, India recorded around 24 lakh digital fraud cases, resulting in losses of over Rs 4,200 crore. As transaction volume surges, so does the fraud surface, shifting from card-based risks to real-time threats. These threats are increasingly driven by phishing, social engineering and app-based manipulation, breaching systems while exploiting behaviour, speed and trust within the ecosystem.

The next phase of digital payments will be increasingly invisible and embedded into everyday experiences. This shift is already visible in India through the rise of recurring mandates such as UPI AutoPay, smart mobility solutions, and connected consumer devices. Payments will not be restricted to smartphones; they will be integrated into cars, wearables, connected cars, smart appliances & enterprise solutions to enable automatic transactions with little or no human intervention.

This shift will ensure convenience but also increase the risk landscape, as many IoT devices operate on inconsistent, often weaker security frameworks, with limited encryption standards and infrequent software upgrades. As machine-to-machine payments grow, securing the device layer will become critical, as fraud may no longer rely on deceiving users but on exploiting compromised devices.

INSTANT PAYMENTS CREATE INSTANT RISKS

India's strong real-time payment infrastructure is fast becoming a critical point of vulnerability. Instant settlements offer convenience but at the cost of real-time threats. In a system built for speed, there is very little time left to intervene, detect, or reverse a fraudulent transaction once it has been executed.

Moreover, human behaviour remains the most exploited weak link, even as technology becomes more

sophisticated. Fraudsters leverage urgency, fear and trust and manipulate users into authorising transactions. In many cases, the user makes the wrong decision, even when the system works as designed.

This risk increases as payments become more automated with less human intervention. To navigate this roadblock carefully, it is more critical to ensure that convenience does not come at the cost of awareness. Users should have clear visibility, real-time alerts, and intuitive user controls. There should also be adequate and sustained digital literacy among users.

Acknowledging these challenges, the Reserve Bank of India (RBI) has proposed a one-hour "cooling-off" period for high-value transactions above Rs 10,000 involving new beneficiaries. This will ensure the perfect balance between speed and security, without disrupting the very efficiency that defines digital payments in India.

TRUST WILL DEFINE PAYMENT RESILIENCE

India's payment infrastructure is one of the most advanced globally and is defined by seamless integration. The next phase will test its resilience, not just its capacity, as transactions shift from user-initiated actions to device-led interactions. The risk will become more distributed and less visible, and security can no longer be confined to endpoints or post-transaction checks.

Regulatory steps, like the RBI's proposed cooling-off period, will reflect a necessary shift towards stronger safeguards, but the bigger challenge will be to ensure that security keeps pace with innovation. Security must move from being a checkpoint to becoming an always-on layer within the transaction flow.

India's payment ecosystem has mastered scale and speed, but the real test will be its ability to stay ahead of threats while preserving its strength and simplicity that made it successful. In a system where money moves instantly, trust cannot be an afterthought. Trust must be built into every transaction. 🧩

The author is the Director and Chief Operating Officer of InstiFi.

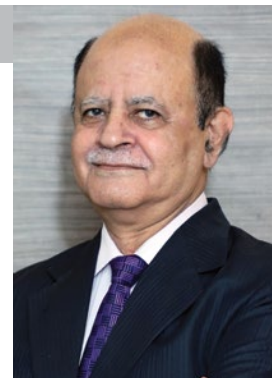
feedbackvnd@cybermedia.co.in



LT. GEN. DR. SP KOCHHAR

MACHINE-TO-MACHINE NETWORKS NEED COHERENCE, NOT SILOS

As connected systems scale across industries, the future of M2M communication in India will depend on secure, interoperable and telecom-led frameworks.



India's digital transformation is entering a decisive, far more complex phase—one in which connectivity is no longer limited to people but extends seamlessly to machines, systems and entire industries. Machine-to-Machine (M2M) communication lies at the core of this transition, enabling a wide range of use cases, from smart meters and connected vehicles to industrial automation, logistics optimisation, and critical public infrastructure.

The scale of this opportunity is immense. M2M is not merely an extension of telecom—it is a foundational layer for the next generation of digital and industrial ecosystems. However, alongside this opportunity lies a significant policy risk. If the framework governing M2M

evolves in a fragmented and inconsistent manner, it could undermine the very benefits it seeks to unlock.

At the centre of the current debate is a fundamental question: should enterprises be granted direct access to spectrum for captive M2M and private network deployments, or should these services continue to be enabled through licensed telecom networks? The answer will not only influence the trajectory of the telecom sector but will also shape the architecture of India's broader digital economy.

M2M AS CRITICAL INFRASTRUCTURE

M2M communication today is deeply embedded in critical sectors such as energy, transportation, manufacturing

“

As industries become machine-connected, fragmented communication frameworks could introduce long-term security and scalability risks.



The debate over enterprise spectrum access will influence how securely and efficiently India's digital infrastructure evolves.

and public infrastructure. These are not standalone applications; they are interconnected, data-driven and often mission-critical systems.

Their reliability directly impacts operational efficiency, safety and economic continuity. In such an environment, connectivity cannot be treated as a commodity—it must be secure, resilient and interoperable by design.

Telecom networks already provide this foundation. Built through sustained investments over decades and governed by stringent regulatory frameworks, these networks ensure security, traceability and service reliability at scale.

They are engineered to support high-density device ecosystems, continuous data exchange, and real-time responsiveness—capabilities essential for M2M deployments. Importantly, they operate within a unified framework that ensures consistency across geographies and use cases.

RISKS OF PARALLEL NETWORK MODELS

Allowing direct spectrum allocation to enterprises outside this framework risks weakening these strengths in several ways.

To begin with, it introduces fragmentation into the communication ecosystem. The emergence of multiple parallel networks, each operating with different standards, protocols and oversight mechanisms, will inevitably create silos.

Interoperability will become more complex, costs will rise due to infrastructure duplication, and scalability will be constrained. There is also a tangible risk of interference and inefficient spectrum use in a fragmented environment. For a country like India, where large-scale, unified systems have driven success, such fragmentation would be a step backwards.

Equally critical is the issue of security. M2M systems are increasingly part of the national critical infrastructure. Licensed telecom networks operate under well-defined service obligations, including monitoring, lawful interception and cybersecurity frameworks.



IN BRIEF

- M2M connectivity is becoming the backbone for utilities, transport, manufacturing, and critical public infrastructure.
- Fragmented enterprise spectrum models could create interoperability gaps and inefficient spectrum utilisation nationwide.
- Telecom-led frameworks already provide scalable security, traceability, and resilience for machine communication systems.
- Parallel connectivity ecosystems may weaken the incentives for telecom investment, critical to long-term digital infrastructure growth.
- 5G features, such as network slicing, can support enterprise M2M deployments within existing telecom frameworks.
- India's future 6G ecosystem will require a unified, interoperable, and secure communication infrastructure at scale.

Extending connectivity outside this regulated environment, without equivalent safeguards, introduces vulnerabilities that are difficult to mitigate. In a digital economy, weaknesses in communication systems can quickly translate into systemic risks, affecting not just individual enterprises but entire sectors.

The question of spectrum efficiency also warrants careful consideration. Spectrum is a finite and valuable national resource. Telecom operators can utilise it efficiently through shared infrastructure, network optimisation, and

Telecom-led M2M frameworks can deliver customised enterprise connectivity without weakening interoperability or resilience.

coordinated planning. Fragmenting this resource across isolated enterprise networks risks underutilisation and duplication. Such an approach is neither economically efficient nor strategically sound, particularly at a time when demand for spectrum continues to grow. The most significant concern, however, is the distortion of the regulatory landscape. Telecom operators operate under a comprehensive framework of obligations, including licence fees, spectrum usage charges and strict compliance requirements.

Allowing enterprises to access spectrum directly, without comparable obligations, creates an uneven playing field. This asymmetry not only disrupts market dynamics but also risks disincentivising continued investment in telecom infrastructure—investment that remains essential for national connectivity and digital growth.

BUILDING A UNIFIED M2M FRAMEWORK

It is important to clarify that this position is not intended to constrain enterprise innovation. On the contrary, India must actively encourage the adoption of advanced technologies such as industrial IoT, smart manufacturing and Captive Non-Public Networks (CNPNS). However, the path to achieving this lies in leveraging and strengthening the existing telecom framework, rather than bypassing it.

Advancements in technology, particularly with the evolution of 5G, reinforce this approach. With capabilities such as ultra-reliable low-latency communications and massive device connectivity, telecom networks are inherently designed to support diverse and demanding M2M use cases. There is no structural limitation that necessitates the creation of parallel frameworks.

Telecom-led models already offer the flexibility enterprises require. Through network slicing, dedicated enterprise solutions and managed Captive Non-Public Networks, operators can deliver customised connectivity tailored to specific operational needs. These solutions combine performance, security, and scalability, enabling enterprises to focus on innovation without managing the complexities of connectivity infrastructure.

Looking ahead, the implications of today's policy choices become even more significant. As India prepares

for 6G and next-generation digital systems, the need for unified, interoperable and secure communication frameworks will only intensify. Fragmentation at this stage will make future integration far more complex and costly, potentially limiting India's ability to compete globally in emerging technology domains.

What India requires is not multiple parallel pathways, but a coherent and scalable framework—one that balances innovation with security, flexibility with standardisation and growth with long-term sustainability. Such a framework must recognise telecom networks as the backbone of digital infrastructure while enabling enterprises to build innovative solutions on this foundation.

The M2M debate, therefore, is about far more than connectivity models. It is about defining the structure of India's digital ecosystem. It is about ensuring that the growth of connected systems does not come at the cost of security, efficiency or resilience.

A fragmented approach may offer short-term flexibility, but it comes with long-term costs—reduced interoperability, increased complexity and heightened security risks. A telecom-led approach, on the other hand, provides a proven foundation that is secure, scalable and future-ready.

India's digital success has been built on coherence, integration and the ability to operate at scale. These principles must continue to guide policy decisions as the country moves into the next phase of its digital journey.

The choice before us is clear. We can either create parallel silos that fragment the ecosystem, or we can build on a unified framework that strengthens it.

For a nation that has demonstrated the power of scale and integration, staying the course of coherence is not just preferable—it is imperative. 🌟

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

[illegible]

**A cultural movement about edited intelligence
in an age of infinite information**

A constant stream of unobserved update
overwhelms Judgement.

Editing and curating Information converts it
into insight.

READ LESS. KNOW MORE.

"An Initiative by Association of Indian Magazines"

PRIVATE 5G: FORGING THE FACTORY OF TOMORROW



As Industry 5.0 moves from pilots to plants, low-latency networks, physical AI, and robotics are reshaping work, safety, resilience, and industrial scale.

BY PRATIMA HARIGUNANI

We have all heard of the steam engine. Something we cannot imagine the Industrial Revolution without. But what about James Nasmyth's steam hammer? Maybe not so much. And yet, it was quite pivotal in ironing out many challenges with heavy industrial metalwork and forging large components – something the Industrial Revolution would have really slowed down without.

Private 5G and its adjacent connectivity fibres and technological advancements are no less than those of the heavyweights. It is hard to forge yesteryear legacy environments with futuristic factories without this hammer. And the beauty is that this hammer is as much about the precision it carries as it is about the strength it wields.

Let us take a quick walk around this new force.

At BALCO, the smelter complex of Vedanta Aluminium in Chhattisgarh, one can already see human-machine

collaboration, physical AI, and large scale robotics, including humanoid systems such as ALAISA, to augment decision making in real time. The humanoid here functions as an on-the-ground, AI-led interface that supports structured learning, real-time query resolution, and contextual guidance on SOPs and critical safety protocols directly at the point of operation.

Take the case of UAV manufacturing environments. They often revolve around mission-specific platforms, design iterations and specialised assembly processes, which means the production ecosystem typically combines engineering-led integration and testing rather than highly automated mass-production lines, explains Karan Shah, Chief Financial Officer, Jyoti Global Plast.

"Technologies such as AI-driven machine vision and connected inspection systems can, therefore, play an important role in areas such as airframe inspection, payload integration validation and system diagnostics during ground and flight testing," Shah underscores the value of connectedness.

The factory floor is becoming a coordinated system where connectivity, compute, sensors, robots, and human judgement must move in sync at an industrial scale.



“Robotics can reduce human exposure in high-risk industrial zones while workers provide context, adaptability, and strategic judgement on the shop floor.”

ASHISH GOEL

Chief Digital & Information Officer, Vedanta Aluminium



IN BRIEF

- Private 5G is emerging as the network layer that enables robotics, sensors, AGVs, and AI systems to operate reliably in industrial environments.
- Industry 5.0 is moving beyond smart factories to human-machine collaboration, physical AI, resilience, and sustainability at scale.
- Factory automation now depends on edge networks, low latency, sensor data, and predictable performance across industrial campuses.
- Physical AI is expanding beyond humanoids to cobots, rovers, mobile robots, inspection systems, and autonomous vehicles at scale.
- India's readiness is uneven, with gains in safety automation but gaps in skills, standards, cybersecurity, regulation, and talent.
- Legacy IT-OT fragmentation, human acceptance, and liability questions remain barriers to responsible adoption in modern factories.

In aluminium smelting, robotics are particularly impactful in high-temperature zones, material-handling areas, and continuous inspection areas, where minimising human exposure is critical, explains Ashish Goel, Chief Digital and Information Officer of Vedanta Aluminium.

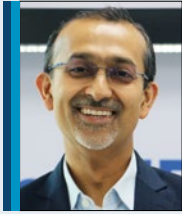
“At the same time, the broader operating environment continues to benefit from a collaborative model, where robotics brings precision, consistency, and data-driven insights, while human expertise adds contextual understanding, adaptability, and strategic decision-making.”

From the humanoid (strapped with sophisticated cameras, microphones and sensors) that was tested successfully at BMW Group Plant Spartanburg in South Carolina, US, in a real production environment in 2024 (it could handle precision and dynamic manipulations, complex gripping and two-handed coordination) to Audi that is consistently rolling out AI in production and logistics- we have taken a huge hop from Industry 4.0 to 5.0.

If Industry 4.0 was all about smart data, real-time monitoring, AI, cloud, Internet of Things (IoT), robotics, and digital twins, Industry 5.0 is all about Collaborative robots, human-AI collaboration, and human-augmentation tools.

Industry 4.0 was a good start, spurring efficiency, automation, faster manufacturing, and digital connectivity, but Industry 5.0 takes it all to another level with human augmentation, human-centricity, sustainability, and system resilience. It is thus a growing space, rising from USD 71.74 billion in 2024 to USD 96.33 billion in 2025, according to ResearchandMarkets.

Industry 5.0 is no longer just a vision of the future. It is already being tested and expanded upon through small and big changes across the world. As seen in the MIT Technology Review Insights Survey-EY Data analysis, 2026, which explores the value of Industry 5.0 transformations, most industrial investments target efficiency. The 250 industry leaders in this survey shared



“Private 5G gives industrial sites predictable performance for robotics fleets, machine vision, smooth handovers, and real-time monitoring at scale daily.”

KUNAL BAJAJ

CEO & Co-Founder, CloudExtel

potential improvements in agility (49%), resilience (48%), profitability (58%), and even sustainability (71%).

In vehicle assembly areas at Audi's German plants, worker guidance on the production line, for instance, comes from the Cloud. And at the body shop for the A5 and A6 series in Neckarsulm, Germany, an Edge Cloud is used in a highly automated production environment for large-scale series production, while Virtual programmable logic controllers are replacing local hardware controllers on the production lines.

At these factories, industrial devices, including around 100 robots, work together with millisecond precision, according to the company's recent announcements. The pilot phase for two use cases is also in progress at its Neckarsulm paint shop: aimed at dosage optimisation in pretreatment and anomaly detection in cathodic dip coating (CDC).

The Volkswagen Group's first AI-supported weld splatter detection system is expected to go into series production at six plants in Ingolstadt. Consider how, at Audi's Neckarsulm site, a splatter detection system detects weld splatter on the underbody of a car and marks it with light, and, due to a recent upgrade, a robot arm has taken over grinding them down, a job once physically demanding.

A lot of this magic lies in the boring but important parts of Edge networking, low-latency connectivity, sensor data, and, hence, in Private 5G.

PRIVATE 5G AT WORK ON FACTORY FLOORS

As Industry 5.0 gets real with integration, scalability and production-ready deployments, it finds a lot of help from Private 5G, for sure.

“Private 5G is now becoming a core enabler for Industry 4.0, especially in environments where reliability and real-time responsiveness are non-negotiable. In manufacturing plants, ports, and logistics hubs, it allows



WHY 5G MATTERS

- **Network role:** Links robots, AGVs, sensors, machines, edge systems, and AI platforms
- **Core value:** Enables low latency, reliability, predictable performance, and dense device support
- **Industrial use:** Supports machine vision, telemetry, inspection, diagnostics, robotics, and safety
- **Strategic impact:** Enables human-machine collaboration and physical AI at scale
- **Readiness gap:** IT-OT integration, cybersecurity, skills, standards, and regulation remain barriers

robotics, autonomous guided vehicles, and IoT-based control systems to communicate seamlessly with very low latency,” says Kunal Bajaj, CEO and Co-Founder, CloudExtel.

This is particularly important for collaborative automation, where humans and machines must work side by side in a safe, synchronised manner.

Private 5G networks are increasingly being explored as an enabling layer for advanced industrial and aerospace environments where autonomous systems,



“AI-led vision and connected inspection can support UAV airframe checks, payload validation, diagnostics, and telemetry-driven testing at scale globally.”

KARAN SHAH

Chief Financial Officer, Jyoti Global Plast

robotics, AI-driven inspection systems and dense sensor networks must operate with high reliability and low latency, shares Shah.

“In the UAV sector, such connectivity can help support real-time telemetry exchange, remote diagnostics and faster integration between aerial platforms, ground control systems and analytics infrastructure,” he explains.

Bernd Otto Hormann, CEO of MHP India, highlights that the real shift is not just about connectivity but about integrating complex shopfloor environments into a unified, scalable architecture. Robots, AGVs, sensors, and AI systems need to operate as a coordinated system, not as isolated technologies. Private 5G enables this level of orchestration.

With over 6,500 small cells and 12,500 km of fibre deployed, including 27 railway stations, we are already supporting high-density, high-performance connectivity environments, Bajaj informs.

“In large indoor facilities and industrial campuses, this translates into consistent coverage, smooth handovers, and minimal interference, all of which are essential for robotics fleets and AI-driven machine vision systems carrying out real-time inspections and monitoring. The real value of Private 5G lies in delivering predictable performance at scale, and that is where shared, well-designed infrastructure becomes critical,” he adds.

PHYSICAL AI MOVES TO THE FACTORY FLOOR

As factories evolve towards a new future, AI will stop being strictly digital. Its contours will get physical and phygital soon.

Humanoid robots are only one expression of a much broader physical AI landscape, unravels Forrester’s Top 10 Emerging Technologies report. While humanoids attract attention, the research shows that many of the most valuable deployments of physical AI occur in non humanoid form factors that are cheaper, more durable,

and better suited to specific tasks, the report points out. The same AI advances that enable humanoids are improving mobile robots, cobots, autonomous vehicles, and inspection systems at scale, it adds.

The Forrester report delineates that, unlike traditional automation, which relies on scripted behaviour in controlled environments, physical AI systems integrate world models, real world sensor data, and reasoning engines to adapt safely when conditions change.

This allows robots and autonomous systems to operate beyond tightly constrained settings, from factory floors to public roads and industrial sites. There is a shift from AI that supports digital decision making to AI that directly affects the physical environment. This transition has profound implications for safety, regulation, workforce design, and capital investment.

As Goel captures from his own deployment experience, “Digital AI (predictive maintenance, data analytics, and process optimisation) operates primarily in the background as the brain of our operations, and it has already delivered immense value. Physical AI is the next phase of evolution. This is where AI is embedded directly into machines, rovers, and robotics to act as the body.”

He further adds that the recent deployment of a humanoid robot at BALCO perfectly reflects this transition, bringing contextual intelligence and interactive capabilities directly into the physical operational environment.

“There is no question that humanoid robots are impressive, but they are not the most important part of the story. The real shift is the growing capability of physical AI – systems that can perceive what is happening around them, reason about next steps, and safely act in the real world. Those capabilities benefit humanoids, but they matter far more for the many other forms of physical automation that are cheaper, more durable, and already delivering practical value at scale,” says Paul Miller, VP and Principal Analyst, Forrester.

Private 5G's real value lies not in wireless access alone, but in the predictability it delivers for AI-led inspection, automation, handovers, and monitoring.

The first AI-controlled robots are taking over ergonomically strenuous tasks, and chatbots are providing additional relief, as Gerd Walker, Member of the Board of Management for Production and Logistics at Audi, also stated when the company announced plans to scale up AI and robotics this January. The automaker had, as it framed, put Edge Cloud 4 Production (EC4P) into operation across its production environment- deepening fully networked factory automation and widespread use of AI in production.

MISSING LINKS IN INDUSTRY 5.0 READINESS

Is the manufacturing vertical really ready for all that technology and 5G has to offer?

There is strong readiness in areas such as safety driven automation, predictive maintenance, and process standardisation, where robotics and automation are already delivering measurable gains in accident prevention, uptime, and operational consistency, Goel observes. "These use cases are well understood and increasingly accepted on the shop floor, supported by ongoing investments in digital infrastructure and targeted upskilling."

At the same time, several gaps need to be addressed for large scale, responsible adoption, Goel cautions. "Standardised human-robot interaction protocols are still evolving, and insurance, regulatory, and liability frameworks have not fully kept pace with rapid technological advancement. Human acceptance, while improving, continues to require deliberate change management; robots need to be consistently positioned and experienced as reliable enablers of safety and productivity, not as threats or novelty deployments."

A critical lesson, he points out, is that successful digital transformation is driven as much by people as it is by technology. "Early engagement with shop-floor teams, addressing their apprehensions, and focusing on continuous capability building are absolutely critical for rapid adoption."

Hormann reminds us that complexity should not be underestimated. "Legacy environments, fragmented IT and OT landscapes, and diverse protocols continue

to create integration challenges. Cybersecurity and capability building are also critical considerations."

As highlighted in the MIT Insights 2026, most organisations are not realising the full value potential of Industry 5.0 due to factors such as culture, skills, and collaboration barriers, as well as tactical and misaligned technology investments.

As for India, Oliver Wyman Forum's 2025 Industry 5.0 Index (an analysis of 92 countries globally) ranks 52, with 58 in Talent, 61 in sustainability, and 45 in resilience.

Nonetheless, the revolution has begun, and a new spark welding yesterday with tomorrow is already visible. Goel is optimistic about what is coming. "We see the future of manufacturing as intelligent, autonomous, and human centric. At Vedanta Aluminium, digital transformation is a core strategic lever to build resilient, efficient, and sustainable manufacturing systems. Our focus is on solving real industrial challenges through intelligent manufacturing ecosystems that improve safety, reliability, and decision making at scale."

So is Shah. "At Jyoti Global Plast, current applications of such technologies are primarily focused on verifying precision manufacturing parameters and ensuring quality consistency in critical components used in UAV systems. Over time, similar technologies could also support automated inspection of lightweight drone structures, verification of payload integration and telemetry-driven testing environments as UAV platforms become increasingly sophisticated."

The key, for us, is to approach this transformation with clear priorities, adds Hormann. "Focus on high-impact use cases, drive standardisation across interfaces and data models, and build architectures that can scale over time."

Soon, we will see more and more examples of humans and robots working seamlessly, leveraging new connectivity and technology breakthroughs. The Nasmyth is clearly busy. Shaping the 'next' industrial revolution. 🌟

pratimah@cybermedia.co.in

TV RAMACHANDRAN

INDIA'S DIGITAL RISE RUNS INTO AN ENERGY WALL

AI workloads, data centres, and broadband growth are pushing India toward a defining challenge: power resilience and nationwide digital expansion.



Unarguably, quality living in modern times demands heavy data usage, as the internet and data-intensive apps are woven into almost every aspect of our day-to-day work, socialising and entertainment. Hence, India's digital transformation is one of the most remarkable stories of our time.

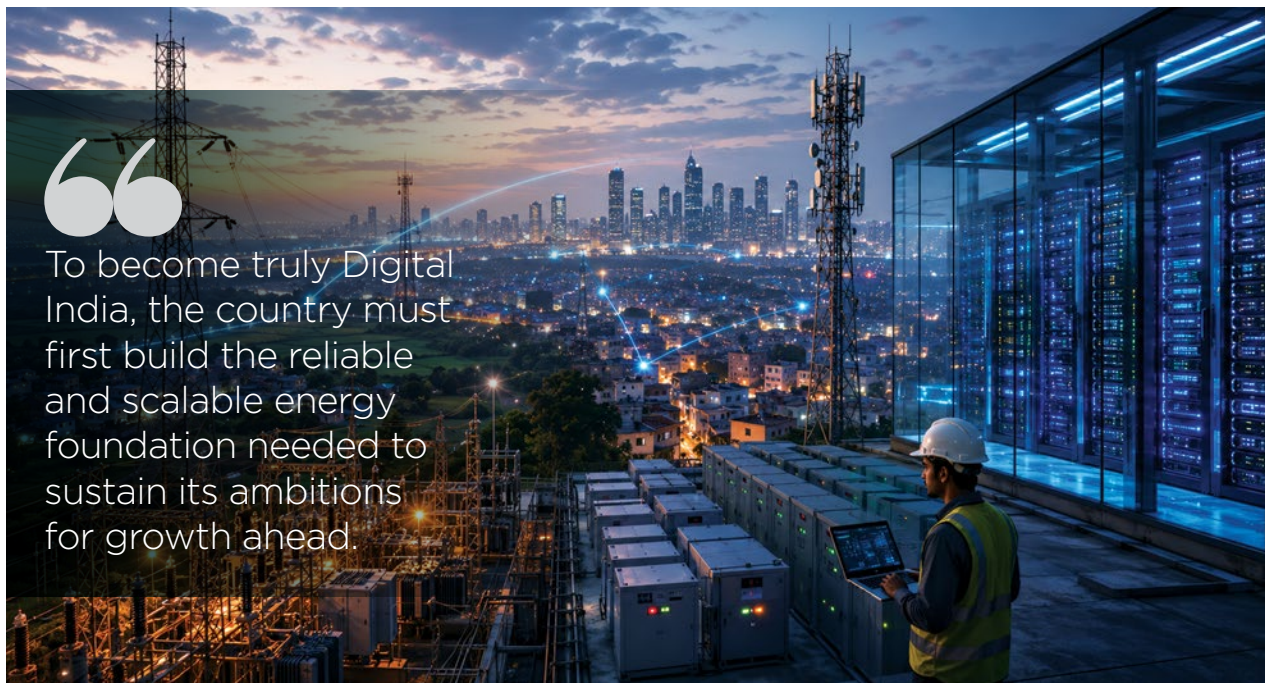
From digital payments to online education, from e-governance to e-commerce, the country has adopted technology at a prodigious scale. However, somewhat overlooked is the significant sustainability price to be paid for it - the high energy costs, and this is probably because India is at the lower end in the global scale of per capita energy consumption.

There is a temptation in some quarters, especially among environmentalists, to portray India's low per capita energy consumption as a "green" advantage—a sign of an advanced, low-carbon, frugal society. This is a dangerous delusion.

India, home to nearly one-fifth of humanity, currently consumes less than one-tenth of global energy. Our per capita energy consumption is one-third of the global average, one-tenth of the USA's and one-fourth of China's. This low consumption level, unfortunately, reflects both a harsh developmental reality and a future challenge. As digital adoption deepens, particularly as AI permeates every facet of our lives and economic activity expands, energy demand is set to rise sharply.

“

To become truly Digital India, the country must first build the reliable and scalable energy foundation needed to sustain its ambitions for growth ahead.



India's ambitions in AI, cloud, and digital infrastructure may ultimately depend on how rapidly it expands reliable, affordable power nationwide.

The digital ecosystem is becoming a significant contributor to this demand. Mushrooming mobile towers and data centres, which power everything from streaming services to cloud applications, require vast amounts of electricity. Sharpening the per capita increase in energy requirement is inevitable.

For India, the challenge is not just to meet this rising demand, but to do so sustainably. This requires a fundamental rethink of how digital infrastructure is built. We are having to strike the right balance in bridging the rather deep chasm between India's digital dreams and its power deficit.

We have to grant that in today's grand theatre of global geopolitics, energy consumption is the most honest indicator of a nation's metabolic rate. While services and high-finance manoeuvres can massage GDP figures, energy—the physical capacity to do work—reveals the raw truth of a country's industrial depth, domestic comfort, and technological sophistication. For India, a nation currently intoxicated by dreams of becoming a "Digital Superpower" and an "AI-First Economy," the energy data presents a sobering, almost chilling, reality.

As of 2024-25, India's per capita electricity consumption stands at approximately 1,460 kWh. To the uninitiated, this might seem like a respectable climb from the dark days of the early 2000s. However, when placed on the global scales alongside the titans India aspires to emulate, the disparity is not just a gap—it is quite startling.

An American citizen consumes nearly 9 times as much electricity as an Indian. Even China, which shared a similar developmental trajectory with India for decades, now consumes nearly five times as much electricity per person. Perhaps most telling is Brazil—a fellow BRICS member with a significant tropical footprint—whose citizens still utilise more than double the energy of their Indian counterparts.

In a developing economy, low energy consumption is not a merit; it is a constraint. It is actually a proxy for thousands of small-scale industries that cannot automate due to "peak-load" shedding, and for a rural population that still likely uses biomass for cooking, leading to severe indoor air pollution and other problems.

In the context of India's "Viksit Bharat 2047" (Developed India) vision, our current energy position needs urgent improvement. Energy is the "master resource. Without a massive surge in the availability of cheap, reliable power, the transition from a developing to a developed nation is physically impossible. You cannot run a first-world economy on a third-world energy level.

THE DIGITAL AMBITION VS THE PHYSICAL CONSTRAINT

The most pressing concern lies in the collision between India's digital roadmap and its energy reality. India is currently undergoing a "Data Centre Frenzy." With 'unique internet penetration' crossing 55% in 2025—predominantly through mobile—monthly data usage has reached 32 GB per user. However, this is just the tip of the iceberg, since the really intensive data-critical apps would need heavy fixed broadband penetration and usage and, as already seen in the USA and Europe, per fixed-line monthly data consumption would soon exceed 500 GB. This is already being experienced on the limited fibre-based fixed broadband in India. This is bound to scale up fast.

Moreover, Artificial Intelligence is not just software; it is a power-thirsty. Training a single large language model can consume more electricity than a small Indian town uses in a year. If India intends to build its own sovereign AI stacks, it will need a massive, dedicated power surplus that does not exist yet.

The cooling crisis: Unlike the USA or Germany, India's data centres must operate in ambient temperatures often exceeding 40°C. The energy required to keep these "digital brains" from melting is a significant overhead that nations with cooler climes do not face.

The reliability gap: Digital economies require "five-nines" reliability (99.999% uptime). Our current grid, while improving, still struggles with quality and stability. For a global tech hub, a millisecond flicker in the power supply could mean a catastrophic failure.

THE PATH FORWARD: A RADICAL EXPANSION

The Indian government's Draft National Electricity Policy 2026 recognises this existential threat. It sets an

A mobile-first internet model helped India scale connectivity quickly, but fibre and Wi-Fi may prove far more sustainable for future demand across modern networks.

ambitious target of 2,000 kWh per capita by 2030 and 4,000 kWh per capita by 2047.

Is this achievable? The evidence suggests we are moving in the right direction, but the path is steeply uphill. India added a historic 34.6 GW of non-fossil fuel capacity in FY2025-2026 alone. As of late 2025, over 50% of our installed capacity comes from non-fossil sources. This is a global gold standard for energy transition.

However, “installed capacity” is not the same as “generation.” Solar does not work at night, and wind is seasonal. To support a 24/7 digital economy, India must solve the storage puzzle. We need massive investments in Battery Energy Storage Systems (BESS) and Pumped Hydro, alongside a pragmatic realisation that “baseload” power from nuclear and high-efficiency coal cannot be abandoned prematurely.

Today, India’s internet usage is overwhelmingly mobile-driven. While this has enabled rapid access, it is not the most efficient way to deliver high volumes of data. Mobile networks are energy-intensive, particularly when scaled for dense usage and high data consumption. Fibre-based broadband, on the other hand, offers a more sustainable alternative. It can deliver significantly higher capacities with lower energy consumption. When paired with Wi-Fi for local access, it offers a significantly more energy-efficient and cost-effective connectivity model.

This is particularly relevant for India, where indoor data usage dominates. Wi-Fi-based access reduces the need for high-power mobile transmissions, improving both energy efficiency and user experience.

India’s ambition to become a global hub for data centres and digital services depends on reliable, efficient, and sustainable infrastructure. Energy costs are a major component of data centre operations. By adopting energy-efficient connectivity models and integrating renewable energy sources, India can enhance its attractiveness as a destination for digital investments. Such an approach would also align with India’s broader sustainability commitments.

Reducing the energy intensity of the digital economy can contribute to climate goals while supporting economic growth. Policy support will be critical in enabling this transition. Expanding fibre infrastructure, particularly in underserved areas, must remain a priority. Public Wi-Fi initiatives, such as PM-WANI, can play a key role in extending connectivity while maintaining efficiency.

The recent de-licensing of 500 MHz of spectrum for Wi-Fi in the 6 GHz band, which facilitates low- and very-low-power use cases, should further enhance capacity and performance while conserving energy sustainably. At the same time, industry must invest in energy-efficient technologies, from advanced cooling systems in data centres to optimised network equipment.

India now stands at a crossroads. It can either follow traditional, suboptimal and energy-intensive models of digital growth, or it can chart a more sustainable path that leverages efficiency as a core principle. The choices made today will determine not just the pace of digital expansion but also its long-term viability.

India’s low energy consumption per capita is the final frontier of development. While we celebrate our digital apps and our fintech prowess, we must remember that every byte of data is ultimately a stream of electrons.

To be “Digital India,” we must first be “Powered India.” We should try to reach the middle energy bracket occupied by China and Brazil as soon as possible. If we fail to bridge this gap to the middle, our digital ambitions will remain just that—dreams deferred by a flickering light bulb. The “India Story” of the next two decades might then not be written in code; it could be written in the power of our grid.

India’s digital future must not become an energy burden. Instead, it could become a model of how growth and sustainability can go hand in hand. 🌞

The author is Hon. FIET (London) and the President of BIF.

(Views are personal.)

Research inputs by Neha Hathiari.

feedbackvnd@cybermedia.co.in

DATAQUEST 40th
THE BUSINESS OF INNOVATION SINCE 1982DIGITAL
LEADERSHIP
CONCLAVEFROM DIGITAL
TRANSFORMATION
TO AI-LED ENTERPRISE
REINVENTION

June 2026, New Delhi

For over four decades, Dataquest has tracked the defining shifts of India's technology landscape. Today, as AI begins to reshape the enterprise more fundamentally than any previous wave of transformation, leadership priorities are being rewritten. The Dataquest Digital Leadership Conclave & 33rd ICT Business Awards 2025 is designed as a focused gathering of CIOs, digital leaders, policymakers, and industry voices. As India's technology landscape enters a new phase marked by AI, data-led decision-making, modern infrastructure, resilience, and governance, the awards seek to honour those who are not just responding to change but defining it.

Follow us: [X](#) [in](#) [f](#) @dataquestindia #ictawards #dqconclve26

33rd ICT Business Awards

KEY CONFERENCE HIGHLIGHTS

- A focused, half-day CXO engagement designed for meaningful, high-quality discussions.
- Editorial-led discussions on AI, data, and enterprise transformation
- Participation from CIOs, digital leaders, and policymakers
- Integrated ICT Awards recognising industry leadership
- High-quality networking with senior decision-makers
- Balanced format: keynote, panel, fireside, and awards
- 150+ Attendees
- Dataquest ICT Business Awards
- Digital Leader Awards for CIO's
- 5000+ CXO's to get influenced

WHO SHOULD ATTEND

- CIOs, CTOs, CDOs
- Digital & transformation leaders
- CISOs & data leaders
- GCC heads & enterprise architects
- Policymakers & ecosystem stakeholders

Audience Nature: Senior decision-makers from leading enterprises and government-linked organisations.

HALL OF FAME

IT PERSON OF THE YEAR

2024



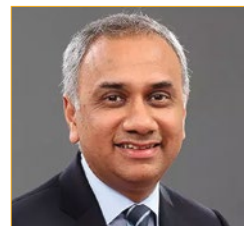
ASHWINI VAISHNAV

2023



RAJEEV CHANDRASEKHAR

2022



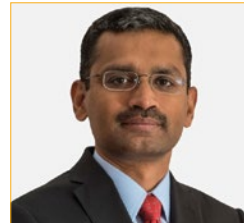
SALIL PAREKH

2021



AJAY SAWHNEY

2020



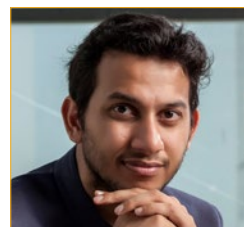
RAJESH GOPINATHAN

2019



PRAKASH KUMAR

2018



RITESH AGARWAL

2017



BHAVISH AGGARWAL

2016



VIJAY SEKHAR SHARMA

2015



RAHUL SHARMA

For sponsorships, contact our team.

Anita Swamy (South) Sr. Manager - Business Solutions & Sales | anitas@cybermedia.co.in | +91-9880304171

Sudhir Arora (North & East) Sr. Manager - Business Solutions & Sales | sudhirarora@cybermedia.co.in | +91-9811625351

Ajay Dhoundiyal (North) Sr. Manager - Marketing Alliances & Business Solutions | ajaydh@cybermedia.co.in | +91-9953540318

Smart meters need networks, not just more devices

India's smart meter expansion will succeed only if resilient, scalable connectivity networks sustain reliable, nationwide data exchange across utilities.



BY TEPPA HEMIA

India's ambitious smart metering programme is often framed as a numbers game: millions of meters to be deployed, timelines to be met, and losses to be reduced. Yet, beneath the scale of procurement and installation lies a more fundamental determinant of success: connectivity.

Without a robust, scalable and cost-efficient communication layer, even the most advanced smart meters risk becoming underutilised endpoints rather than active enablers of grid intelligence.

At its core, smart metering is a data infrastructure project. The value of a smart meter lies in its ability to reliably transmit data over long periods, often in challenging environments. This shifts the focus from devices to networks, from what is installed on the wall to how it communicates across the system.

CONNECTIVITY AS THE GRID BACKBONE

India's electricity distribution landscape presents a uniquely demanding environment for connectivity. High population density in urban areas, dispersed

Utilities are discovering that weak communication layers can undermine even the most advanced smart meter deployments at scale.

As smart metering expands nationwide, connectivity resilience is emerging as the defining factor behind grid intelligence outcomes.

rural geographies and variable infrastructure quality create a wide spectrum of deployment conditions. In such a context, network reliability is a prerequisite for operational viability.

Frequent data gaps, latency issues or network downtime directly impact billing accuracy, outage management and demand response capabilities. For utilities operating on thin margins, these inefficiencies can quickly erode the expected benefits of smart metering investments.

The challenge, therefore, is not just to connect meters, but to ensure consistent, resilient communication at scale. This requires a careful evaluation of connectivity technologies, each with distinct trade-offs.

LPWAN AND CELLULAR TRADE-OFFS

Low Power Wide Area Network (LPWAN) technologies have gained traction due to their ability to support large numbers of devices with relatively low energy consumption. Their architecture is well-suited to sparse deployments and can offer cost advantages, particularly when operating in license-free or shared-spectrum environments.

However, LPWAN performance is highly dependent on network design and infrastructure build-up. Coverage gaps, interference and limited downlink capacity can affect reliability if not carefully managed. In large-scale deployments, network planning and density become critical to maintaining performance.

Cellular technologies, on the other hand, offer established infrastructure and managed quality of service. With the evolution of IoT-specific standards, cellular networks are increasingly positioned as a viable option for smart metering. Yet, they come with their own considerations, most notably high recurring connectivity costs and dependency on telecom operators' network evolution and priorities. Cellular technologies' reach to places where the meters are located remains a problem, too.

The emergence of new approaches reflects an ongoing effort to bridge these gaps. Among them, NR+, a mesh-based standard purpose-built for large-scale IoT,



IN BRIEF

- Smart metering is fundamentally a connectivity and data infrastructure challenge, not merely a device deployment exercise.
- Network reliability directly affects billing accuracy, outage response, and demand-side management across utilities.
- LPWAN and cellular models each bring trade-offs in scalability, cost, coverage, and long-term operability.
- Connectivity technologies must remain viable for 10–15 years without frequent upgrades or network redesigns.
- Interoperability and open ecosystems will shape the long-term flexibility and economics of smart meter rollouts.
- India's large-scale deployments show that network architecture choices determine operational efficiency at scale.

is gaining traction. As the foundation of Wirepas' mesh connectivity, it already connects more than ten million smart electricity meters in India.

NR+ aims to combine the scalability of cellular ecosystems with the flexibility and cost structure required for massive IoT deployments. Still, its success will depend on ecosystem maturity and alignment across

India's rollout highlights how interoperability, spectrum strategy, and network design now shape the economics of utility modernisation.

stakeholders, which Wirepas has addressed through its investments in the Wirepas Certified Platform and its collaboration with a growing number of HES and meter manufacturers in India.

SCALABILITY ACROSS METER LIFECYCLES

One of the defining characteristics of smart metering infrastructure is its lifespan. Meters are expected to operate for 10 to 15 years, often with limited physical access for upgrades or maintenance. Connectivity solutions must therefore be designed with long-term stability in mind.

This raises critical questions: Will the chosen technology remain supported throughout the deployment lifecycle? Can it scale from pilot phases to nationwide rollouts without significant redesign? How resilient is it to changes in spectrum regulation or network congestion?

India's experience has already highlighted the risks of underestimating these factors. Early deployments in some regions have encountered challenges with network performance and interoperability, prompting a re-evaluation of connectivity strategies.

Technologies operating in globally harmonised, license-exempt bands, such as NR+, offer an alternative model that balances predictable performance with deployment flexibility.

POLICY AND ECOSYSTEM ALIGNMENT

Connectivity decisions do not exist in isolation. Regulatory frameworks, spectrum policies and the broader telecom ecosystem shape them. In India, the alignment between utilities, telecom operators and policymakers plays a pivotal role in determining outcomes.

Spectrum availability, in particular, remains a key factor. Licensed spectrum can offer greater reliability and predictability, but at a higher cost. License-exempt options provide flexibility and lower barriers to entry, but may introduce performance variability. Striking the right balance requires a nuanced understanding of both technical and economic trade-offs.

Equally important is the need for interoperability and open ecosystems. As deployments scale, the

ability to integrate devices, networks and platforms from multiple vendors becomes essential. Proprietary approaches may offer short-term advantages but can limit flexibility and increase long-term costs. Standards-based approaches such as NR+ are designed with this interoperability in mind, enabling multi-vendor ecosystems to develop without compromising network cohesion.

CONNECTIVITY LESSONS FROM SCALE

India's smart metering rollout is already among the largest of its kind globally and offers valuable insights for other markets. Perhaps the most important lesson is that connectivity cannot be treated as an afterthought. It must be considered a foundational layer, on par with the meters themselves.

Successful deployments have demonstrated the importance of holistic planning, aligning device capabilities, network architecture and operational processes from the outset. They also highlight the value of adaptability, as utilities refine their approaches based on real-world performance.

Large-scale deployments in India, such as those based on NR+, illustrate how network design choices directly influence long-term performance and operational efficiency.

As India continues to expand its smart metering programme, the focus is likely to shift from deployment speed to system effectiveness. This will bring connectivity choices into sharper focus.

The next phase of growth will depend not only on how many meters are installed, but on how well they communicate consistently, efficiently and at scale. Increasingly, this is bringing attention to connectivity models that are resilient by design, such as distributed mesh architectures like NR+. The right connectivity layer is the foundation on which the entire initiative's success rests. 🧩

*The author is the Founder and CEO of Wirepas.
feedbackvnd@cybermedia.co.in*



Tactical 5G redraws the defence communication grid

Built for moving troops and contested theatres, the 5G-enabled defence network must deliver encrypted, high-speed links with layered redundancy at scale.



BY DR SIDHARTH SHUKLA

Defence communication is built for a different operating environment from civilian telecommunications. While commercial networks are designed around coverage, capacity, user density, and service continuity for public use, defence networks are shaped by mission-critical needs, mobility, security, redundancy, and operational command requirements.

In this setting, 5G can support tactical defence communications, but only when it is deployed as a dedicated, customised, secure, and defence-controlled network rather than as an extension of a public or hybrid cellular system.

DEFENCE NETWORKS FOR MISSION CONTINUITY

The nature of defence communication makes it distinct from civilian communication systems. It has to be critical

in function, fail-safe in design, and supported by multiple layers of redundancy across both platform and spectrum. It must also be swift, secure, and capable of providing real-time, high-bandwidth communication to troops who are constantly on the move.

The purpose of this communication architecture is not limited to connecting users. It must link troops deployed in forward areas with decision makers at headquarters located in depth. This makes defence communication both tactical and strategic. It has to support battlefield movement and command-level planning across a theatre of operations.

Defence communication can broadly be viewed through two verticals. The first is strategic communication, which forms the core of the defence communication architecture. It is primarily static and covers a large theatre of operations with multiple strategic nodes.

Tactical 5G can give forward troops secure voice and data links while enabling rear headquarters to send timely directions during live battlefield operations.

These nodes are interconnected through reliable, high-bandwidth, heterogeneous communication links. The architecture uses a mix of optical fibre, microwave UHF point-to-point radios, and high-capacity satellite links for terrains that are difficult to reach.

The second vertical is tactical communication, which is designed for limited operational areas during battle. Unlike strategic communication, tactical communication is mobile and dynamic. It must align with the different phases of a tactical battle.

This layer primarily consists of vehicle-based communication systems using switching equipment and PBXs for tactical users. Tactical nodes are ultra-mobile and connected via high-capacity point-to-point microwave links, forming a tactical grid of wireless nodes.

As a redundancy layer, HF and VHF tactical radio networks are also used to form a dynamic radio grid. This supports swift, secure communication during tactical operations, where mobility, changing terrain, and troop movements require systems that can adapt continuously.

5G FOR TACTICAL DEFENCE NETWORKS

Within this tactical environment, 5G fits well when it is deployed as part of a defence-owned tactical communication grid. The gNodeBs, or 5G base stations, can be mounted on defence communication vehicles. This allows the network to move with the formation and be deployed during both defensive and offensive operations.

These 5G-capable defence communication vehicles can connect to the last communication node of the strategic defence network near the country's borders. From there, they can create a grid of 5G communication vehicles to provide a robust, fail-safe, and redundant 5G network. As troops move into enemy territory, the grid can advance with them by adding new 5G defence communication vehicles in a caterpillar or leap-frog pattern.

In such a configuration, 5G can provide the forward-edge soldier with secure, high-speed data

and voice services over an established tactical 5G defence communication grid. This can enable real-time information to flow from forward troops to higher headquarters in the rear. It can also allow troops to receive clear directions from rear headquarters in time to act during battle.

For this to work, 5G radio access network and core capabilities must be customised for defence communication vehicles. Radio-frequency planning and design also need to be optimised to ensure effective, wide-scale 5G connectivity across the tactical battlefield. The server infrastructure must be installed within the defence communication setup and secured using high-level protocols and supporting systems.

The soldier's handset is also part of this architecture. The 5G handset issued to each soldier should be military-hardened and include encryption capabilities not only at Layer 3 and above, but also at Layers 1 and 2. This level of encryption is required to protect data from the enemy at its location.

WHAT MAKES A DEDICATED 5G GRID WORK

A 5G defence communication grid cannot be treated as a standard telecom deployment. Its hardware, devices, radio access network, and core must be manufactured in India and customised for defence requirements under the guidance and supervision of the Defence Ministry and affiliated establishments.

The handset also needs to be manufactured by an Indian OEM. It must comply with military ruggedness standards and be customised for Layer 1 and Layer 2 encryption. This requirement reflects the physical and security demands of tactical operations, where ordinary commercial devices are not designed to operate.

Spectrum allocation is another requirement. The defence communication network should use a spectrum that is separate from the commonly used frequencies of civil mobile network operators. This separation is required to reduce the risk of interference. The spectrum should be allocated in the sub-1 GHz band to improve range on the tactical battlefield.

The battlefield value of 5G lies in mobility, redundancy, encryption, and control, not merely faster data speeds or wider coverage across contested theatres.

The network should also have satellite gateway capabilities at multiple locations within the country to provide geo-redundancy. In addition, the 5G defence network should support non-terrestrial networks. Satellite connectivity should be available on handsets, while the radio access network and core should also support NTN capabilities.

Operations and maintenance must remain under defence control. The radio access network, core, network operations centre, security operations centre, and servers should be maintained and operated principally by trained defence personnel. This requirement is linked to the network's confidentiality and critical nature.

WHY PUBLIC OR HYBRID NETWORKS FALL SHORT

The tactical 5G defence communication grid cannot be achieved by using the existing pan-India civil networks of mobile network operators. One reason is that civil cellular infrastructure stops 50 km short of the country's borders under the regulatory policy in force. This makes such networks unsuitable for tactical defensive and offensive operations near the border or deep inside enemy territory.

Civil cellular infrastructure also includes network elements and devices that are mostly of foreign origin. In a dynamic geopolitical environment, such equipment could be sabotaged by the host country of the OEM during hostilities.

A network slice within a broader civil cellular network also does not meet the requirement for isolating the defence network from civil networks. The issue is not only about bandwidth or service separation. The defence communication network requires a level of isolation suited to mission-critical and confidential military communication.

There are operational concerns as well. Civil employees of mobile network operators manage the network operations centres and relevant servers. This arrangement cannot handle highly confidential defence data. Civil handsets also do not meet military ruggedness requirements and cannot comply with the high encryption levels required for defence use.

The network operations centres and servers of civil cellular infrastructure are connected to the Internet, which exposes them to cyberattacks and sabotage of the defence communication grid. The fibre-optic infrastructure of civil cellular networks is also laid and maintained by third parties, creating further vulnerabilities. Since the spectrum allocated to civil mobile operators uses commonly deployed bands and frequencies worldwide, it is also prone to interference by an enemy during offensive and defensive operations.

5G'S ROLE IN LAYERED DEFENCE ARCHITECTURE

Defence communication networks are not based on a single technology or protocol. Their planning and capability are layered by design. Tactical defence networks will continue to operate across HF, VHF, UHF, and military or citizen bands. These will be supported by tactical radio nets, mobile satellite links, MPLS and TDM-based tactical communication grids, digital troposcatter point-to-point links, and Army-owned optical fibre networks.

This layered approach ensures that when one technology operating in a particular frequency band fails, the soldier at the forward edge of battle has another pre-configured tactical communication grid available for real-time communication. The aim is to maintain a fail-safe, mission-critical, and reliable tactical communication grid.

In this architecture, 5G has a defined role. It can strengthen tactical battlefield communication when it is deployed as a defence-owned, defence-operated, secure, and mobile network. It falls short when treated as an extension of civil cellular infrastructure or as a public network slice. The difference lies in ownership, isolation, encryption, ruggedness, spectrum, redundancy, and operational control. 🧩

The author is an expert in defence communication strategies. He is an Army veteran with 24 years of experience designing, planning, and operating tactical and strategic defence communication networks for the Indian Army in difficult terrains in counter-insurgency and high-altitude warfare scenarios.

feedbackvnd@cybermedia.co.in



Enterprise networks fail where trust layers fragment

Hybrid enterprise access is exposing coordination gaps between identity, endpoint, and network controls across modern infrastructures.



BY VIJENDER YADAV

Enterprise security today is built in layers. Organisations invest in identity and access management, endpoint management, and network security controls, assuming that stronger layers will naturally create stronger protection. In practice, that assumption often breaks down. Breaches do not always happen because a control is missing. They happen because controls operate without enough shared context.

Each of these layers has matured significantly, with capabilities such as multi-factor authentication, endpoint detection and response (EDR), and software-defined perimeters becoming more common.

Yet breaches continue to occur in environments well equipped with these controls. The problem is often not

the absence of tools, but the absence of coordination. Security fails less often within individual layers than in the spaces between them, particularly when context is lost during an access decision.

These gaps are difficult to detect because each system may still be functioning as intended. Identity systems authenticate users, endpoint tools validate device posture, and network controls establish access paths. The weakness arises when these decisions are made separately, without a shared, real-time understanding of risk.

IDENTITY WITHOUT FULL DEVICE CONTEXT

Modern IAM systems have become adept at validating user identity through mechanisms such as adaptive authentication and risk-based access policies. However,

Enterprise breaches increasingly exploit the gaps between identity, endpoint, and network controls rather than failures within individual security tools.

these systems are still largely user-centric. They focus on validating credentials and, in some cases, behavioural signals, but they do not always incorporate strong device binding or continuous device posture into the access decision.

A user may pass MFA and satisfy conditional access requirements, but still be operating from an unmanaged or compromised endpoint. If device trust is not tightly linked to identity through signals such as device compliance, OS integrity, or EDR telemetry, authentication becomes only a partial indicator of risk.

In hybrid work environments, where users frequently access enterprise resources from personal or partially managed devices, this gap becomes more pronounced. Identity assurance without device context creates a false sense of security.

ENDPOINT RISK WITHOUT ENFORCEMENT

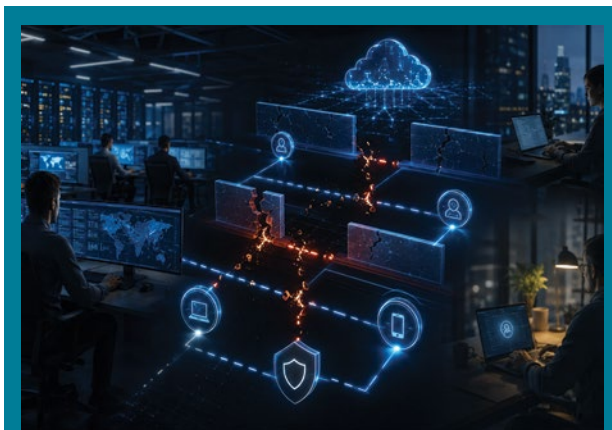
Endpoint management and EDR/XDR platforms provide deep visibility into device health. They assess compliance based on patch levels, encryption status, application controls, and threat-detection signals. These checks are often used in pre-access validation, particularly within conditional access frameworks. The problem emerges after access has already been granted.

In many environments, device compliance is assessed at login, but not continuously enforced throughout the session. If a device falls out of compliance due to a missed patch, configuration drift, or active malware, the endpoint tool may detect the change, but the access control system may not act on it in real time.

This creates a disconnect between detection and enforcement. The endpoint may generate high-risk signals, but unless those signals are tied directly to session controls, access remains unaffected. The result is a static trust decision operating in a dynamic threat environment.

NETWORK TRUST STILL EXTENDS TOO FAR

Network access has traditionally been governed by perimeter-based models, where trust is extended based on location. While technologies like VPNs have



WHAT ORGANISATIONS MUST EXAMINE?

- How quickly endpoint risk signals reach session controls
- Whether identity, endpoint, and network policies are actually enforced together
- Which business-critical applications would benefit first from continuous access evaluation

evolved, the underlying assumption often remains the same. Once inside the network, the user is trusted to a certain degree.

This approach is increasingly misaligned with modern access patterns. In distributed environments, users connect from different locations and devices, making the idea of a trusted network boundary far less meaningful. VPN-based access, in many cases, still provides broad network-level visibility without applying granular, identity-aware controls at the application layer.

Zero Trust Network Access (ZTNA) attempts to address this by shifting from network-centric to identity-centric access. But identity-aware access alone is not enough if endpoint posture and session context are not being continuously evaluated. Without that, even a more modern access model can fall short.

Security platforms may exchange telemetry effectively, yet fragmented enforcement still creates exploitable trust gaps across enterprise access sessions.

POLICIES FRAGMENT ACROSS TRUST LAYERS

A critical but underappreciated challenge is policy fragmentation. Enterprises often define security policies across multiple systems. IAM platforms enforce authentication and authorisation rules, endpoint tools define compliance baselines, and network solutions control access pathways.

While these policies may appear aligned conceptually, they are enforced independently. That is where inconsistency enters the picture. A device marked non-compliant by an endpoint tool may not immediately trigger session termination. A rise in identity risk may not reach network-level controls quickly enough to change access.

This fragmentation is not necessarily a failure of policy design. It is a failure of orchestration. Without a unified enforcement layer, policies remain static rules applied within separate systems rather than dynamic controls governing the full access lifecycle.

INTEGRATION WITHOUT UNIFIED CONTROL

To address these issues, many organisations have integrated their security stack through APIs and event-driven architectures. While that improves interoperability, it does not fully resolve the problem. Most integrations remain asynchronous. They rely on event triggers, polling intervals, or synchronisation processes that introduce latency.

Even small delays between a change in risk posture and a corresponding access decision can create exploitable windows. The issue is not simply whether systems exchange data, but whether they can act on that data fast enough and in a coordinated way.

More importantly, integration often focuses on signal sharing rather than decision-making. Systems exchange information, but continue to make access decisions independently. What is still missing in many environments is a centralised, context-aware control plane that can aggregate risk signals and enforce decisions consistently in real time.

ACCESS MUST BECOME CONTEXT-AWARE

Addressing these gaps requires a shift from point-in-time access control to continuous access evaluation.

Access decisions cannot remain limited to the moment of authentication. They have to extend across the full duration of a session.

A stronger access model should combine identity signals, device posture, network context, and behavioural analytics into a unified decision engine. That engine should be able to reassess risk continuously and adjust the session in real time, whether by triggering step-up authentication, restricting access, or terminating the session altogether.

This requires tighter coupling between policy engines, telemetry sources, and enforcement points. It also requires rethinking sessions as dynamic entities that can be modified or revoked based on evolving risk, rather than static constructs established at login.

RETHINKING TRUST FOR HYBRID ACCESS

As enterprises continue to scale across cloud environments, remote workforces, and third-party ecosystems, the complexity of access management will only increase. The traditional layered security model still matters, but it is no longer sufficient without coordination between layers.

The focus must shift to building a unified access fabric in which identity, endpoint, and network signals are continuously correlated and enforced. This is not about replacing existing systems, but about ensuring they operate with shared context and aligned decision-making.

Enterprise access rarely breaks because security teams lack controls. It breaks because controls operate without awareness of one another. Attackers exploit those seams, moving across systems that were never designed to act as a single unit.

Closing these gaps requires more than incremental tuning. It requires a shift toward context-driven, continuously enforced access. Until that happens, the invisible gaps between network, identity, and endpoint layers will remain one of the most persistent weaknesses in enterprise security. 🧩

*The author is the Co-founder and Chief Executive Officer of Accops.
feedbackvnd@cybermedia.co.in*



25th TELECOM LEADERSHIP FORUM

EMPOWERING LEADERS IN TELECOMMUNICATIONS

FROM CONNECTIVITY TO COGNITIVE INFRASTRUCTURE

03 July 2026, New Delhi

[X](#) [in](#) [f](#) @voicendata_ <https://tlfindia.in> #tlfindia #tlfawards2026

Voice&Data, India's leading and largest telecom media is organising its 25th edition Telecom Leadership Forum, a full day conference in Delhi. We are celebrating 31+ years of "Connecting the Digital world" the synergy between telecom and enterprises Voice&Data will recognise & felicitate the leading visionaries, industry experts & personalities, that made the Indian telecom ecosystem, to new era for the world, leading by example. Their actions & leaderships acumen has impacted the enterprises, Indian growth wagon, end consumers & society at large.

TELECOM LEADERSHIP AWARDS



TELECOM
PERSON OF
THE YEAR



LIFETIME
ACHIEVEMENT
AWARD



PATHBREAKER
OF THE YEAR

KEY HIGHLIGHTS

- Full Day Conference
- 10+ Sessions
- Keynotes & Panels
- 200+ Tech Decision Makers
- 5,000+ CXOs
- 24th TLF Jury Awards
- 20+ Category Awards
- Live Networking
- Speakers Lounge
- Experience Zone
- Live Social Feeds
- Live Polls and Feedback

For speakership and partnership opportunities, reach out to
Ajay Dhoundiyal | Sr. Manager
ajaydh@cybermedia.co.in | +91 99535 40318

HALL OF FAME

TELECOM PERSON OF THE YEAR

2024



SUNIL VACHANI

2023



K. RAJARAMAN

2022



TATA CONSULTANCY SERVICES,
C-DOT, BSNL, TEJAS NETWORKS

2021



ANSHU PRAKASH

2020



MANOJ MODI

2019



R S SHARMA

2018



ARUNA SUNDARARAJAN

2017



MUKESH AMBANI

2016



GOPAL VITTAL

2015



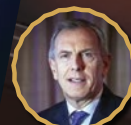
DR RAHUL KHULLAR

2014



HIMANSHU KAPANIA

2013



MARTEN PIETERS

Chasing AI supremacy through power-hungry server farms

As AI adoption accelerates globally, data centres are emerging as strategic assets, shaped by power access, cooling demands, and energy security.



BY AYUSHI SINGH

We speak about the cloud as though it exists somewhere weightless and invisible. Artificial intelligence is often discussed in terms of algorithms, software models and digital transformation. Yet behind every AI query, streamed film, online payment and cloud application lies a vast physical infrastructure that has quietly become one of the world's most strategic industries: the data centre.

These facilities are the industrial backbone of the internet economy. Every digital interaction is routed

through enormous halls of servers that operate around the clock in carefully controlled environments. What feels instantaneous to users is sustained by infrastructure engineered to handle enormous computational loads, absorb failures in real time and deliver uninterrupted uptime at a global scale.

For years, data centres operated largely in the background of the digital economy. Now, the explosive rise of AI is pulling them into the centre of global debates around energy, sustainability, industrial policy and national sovereignty.

AI infrastructure is transforming data centres from invisible back-end facilities into strategic industries competing globally for power and water resources.



“The next phase of AI infrastructure growth will depend on reliable low-carbon power, operational resilience, and energy efficiency at hyperscale globally.”

ASHISH ARORA

Chief Executive Officer, Nxtra by Airtel

According to the International Energy Agency (IEA), global data centre electricity consumption reached approximately 415 terawatt-hours (TWh) in 2024, around 1.5% of global electricity demand, and could rise to nearly 945 TWh by 2030 as AI adoption accelerates. AI-focused facilities are becoming so energy-intensive that the IEA compares some of them to heavy industrial operations such as aluminium smelters.

The implications stretch far beyond technology. Electricity grids, water resources, renewable energy access, geopolitical stability and climate targets are all becoming critical variables in the future of digital infrastructure.

DIGITAL GROWTH MEETS PHYSICAL LIMITS

The pressure is most visible in the race to secure power and water. Deepak Virwani, a workforce management consultant, says infrastructure constraints are increasingly becoming a defining challenge for the sector. “It is increasingly difficult, and in some regions, it is already a limiting factor for growth,” he says.

Modern hyperscale data centres can consume as much electricity as small towns, often requiring tens to hundreds of megawatts of continuous power. According to Virwani, the issue is not simply obtaining access to power, but securing a reliable and uninterrupted supply, something many grids, particularly in rapidly urbanising economies, struggle to provide consistently at scale.

Water availability has emerged as another major pressure point. Traditional cooling systems rely heavily on evaporative cooling, requiring substantial water use each year.

“In water-stressed regions, this creates a direct conflict between infrastructure expansion and local sustainability priorities,” Virwani says. “This has already led to tighter scrutiny and, in some cases, restrictions on new developments in certain geographies.”



IN BRIEF

- AI-driven data centres are rapidly increasing electricity demand, cooling pressures, and infrastructure complexity worldwide.
- Power availability is becoming a critical constraint for hyperscale and AI-focused data centre expansion globally.
- Renewable energy integration is moving from a sustainability strategy to a core infrastructure planning requirement.
- Data sovereignty rules and geopolitical risks are reshaping where future digital infrastructure gets deployed.
- AI workloads are driving major shifts toward liquid cooling and ultra-high-density data centre architectures.
- Future data centre competitiveness will depend on energy resilience, operational efficiency, and low-carbon power access.



“Data centre expansion and sustainability can no longer operate separately as AI workloads sharply increase global energy consumption levels worldwide.”

ANIL NAMA

Chief Information Officer, CtrlS Datacenters

The challenge is intensifying because AI workloads are fundamentally different from traditional cloud computing. AI training clusters powered by high-performance GPUs generate significantly greater heat and require far denser computing environments.

Virwani describes this as a growing “structural tension”, where the strongest demand growth is occurring precisely in regions facing mounting infrastructure constraints.

To manage these pressures, operators are increasingly investing in renewable energy procurement, advanced cooling systems and more selective infrastructure deployment strategies.

“Expansion is increasingly gated by energy ecosystems and resource sustainability, not just capital and demand,” he says.

POWER SHAPES DIGITAL INFRASTRUCTURE

As AI adoption accelerates globally, access to energy is becoming one of the most important competitive differentiators in the data centre industry. Anil Nama, Chief Information Officer at CtrlS Datacenters, says balancing rapid capacity expansion with sustainability has become central to long-term infrastructure planning.

“Balancing capacity expansion with sustainability is a key challenge for the data centre industry, especially as AI and hyperscale workloads drive rising power demand,” Nama says.

According to Nama, the industry is increasingly integrating renewable energy directly into infrastructure expansion strategies rather than treating sustainability as a parallel objective. “The focus now is on securing power from reliable, scalable renewable sources,” he says. “The industry is moving toward integrating renewables into expansion plans using captive generation, long-term

agreements, and energy partnerships to ensure cost predictability and sustainability.”

CtrlS, for example, is expanding its renewable energy integration through its GreenVolt solar initiative and a partnership with NTPC Green Energy to develop more than 2 GW of renewable energy capacity for its facilities.

“At CtrlS, we are taking a similar approach by embedding renewable energy into our infrastructure strategy,” Nama says. “For example, our GreenVolt solar initiative already powers a substantial part of our Mumbai campus. We are expanding our renewable capacity through large partnerships, including a collaboration with NTPC Green Energy to develop over 2 GW of renewable power for our data centres.”

He says the industry is now moving towards a model in which sustainability and scale are no longer separate goals.

“This reflects a broader industry trend in which expansion and sustainability are integrated, ensuring growth remains scalable and aligned with future sustainability goals,” Nama says.

Globally, the shift is already reshaping infrastructure economics. The IEA estimates that electricity generation dedicated to data centres could exceed 1,000 TWh by 2030, with renewable sources expected to meet nearly half of the additional demand growth.

Yet even in mature digital infrastructure markets, energy availability is becoming increasingly constrained. In several parts of Europe, delays in grid expansion and power shortages are already slowing new data centre deployment despite continued demand. “Energy availability is emerging as a hard constraint,” Virwani says. “Even when demand and regulatory conditions are favourable, lack of power can halt or defer projects.”



“AI infrastructure growth is increasingly constrained not by capital alone, but by reliable power access and long-term resource sustainability worldwide.”

DEEPAK VIRWANI

Workforce Management Consultant

INTERNET INFRASTRUCTURE SHIFTS GEOGRAPHICALLY

The AI boom is not only changing how data centres operate but also reshaping where they are built. Historically, location decisions were driven by connectivity, land availability and proximity to end users. Today, data sovereignty laws, geopolitical tensions and energy security are increasingly influencing infrastructure strategy. “Data centre location decisions are now more strategic, driven by data sovereignty, geopolitics, and energy availability,” Nama says.

Governments across the world are tightening localisation requirements for sensitive and critical data. Regulations such as Europe’s GDPR and India’s emerging data localisation frameworks are pushing global cloud providers to expand infrastructure footprints within national borders. Virwani says this is moving the industry away from centralised efficiency towards what he calls “distributed resilience”. “Infrastructure that was once viewed as neutral is now evaluated against factors such as political stability, trade restrictions and conflict exposure,” he says.

Ashish Arora, Chief Executive Officer of Nxtra by Airtel, says data centre planning has evolved far beyond technical considerations. “Data centre location is no longer a technical decision alone but is an intersection of regulation, geopolitics, and energy transition decisions,” he highlights, adding that decisions are shifting from simply capacity to where a facility can ensure compliance, resilience, and green infrastructure at scale.

According to Arora, energy availability is rapidly becoming the defining constraint for the next generation of AI infrastructure. “The next wave of AI and cloud growth will be constrained not by demand, but by access to reliable, low-carbon power,” he says. “That is why we are investing ahead of the curve in firm, round-the-clock renewable energy through long-term partnerships

and collaborations with key industry experts to secure scalable green power for our facilities.”

He adds that sustainability commitments are increasingly shaping customer expectations as global enterprises look to align infrastructure deployment with broader ESG goals.

“Coupled with our net-zero by 2031 commitment and green-by-design approach, this gives our customers confidence that their growth in India is aligned with their global ESG and decarbonisation goals,” Arora says.

India, in particular, is emerging as a strategically important market due to policy support, rising digital demand, and expanding renewable energy ecosystems. “From a data sovereignty perspective, India is already moving towards a more localisation-driven regime, especially for critical and sensitive workloads,” Arora points out.

“We see this as a structural tailwind for India’s data centre ecosystem, because it creates a strong case for building capacity closer to the end user, backed by domestic networks and cloud connectivity,” he adds.

Nama believes the global infrastructure map is shifting from being “network-centric to energy- and sovereignty-centric”.

The transition reflects a broader shift in how governments and corporations view digital infrastructure, not simply as commercial real estate but as critical national infrastructure.

AI IS REDESIGNING DATA CENTRES

The rise of AI is also fundamentally changing the architecture of data centres themselves. Traditional enterprise data centres were built around predictable computing workloads and relatively low rack densities.

AI infrastructure expansion is forcing governments and operators to rethink digital growth through the combined lens of energy security and resilience.

AI clusters are rapidly overturning those assumptions. The IEA estimates that the power density of AI servers increased elevenfold between 2020 and 2025 and could rise another fourfold by 2027.

Virwani says this is forcing “a fundamental redesign of data centre architecture”. “These systems increase rack power densities substantially, often several times higher than traditional enterprise workloads,” he explains. As a result, cooling systems are becoming a defining element of infrastructure design.

He further highlights that liquid cooling, including direct-to-chip and immersion cooling, is moving from niche to mainstream adoption. Adds Arora: “The industry is shifting towards AI-optimised environments where cooling, power delivery and high-speed interconnects are central architectural priorities rather than supporting systems.”

He further explains how AI is fundamentally changing the physics and economics of data centres. “We are moving from traditional, air-cooled, general-purpose halls to highly dense, AI-optimised infrastructure where power, cooling, and interconnect become the core design variables, not afterthoughts.” According to Arora, the transition is already redefining infrastructure design standards across hyperscale facilities. “Traditional cooling is already at its limits for large AI and ML clusters,” he says. “New hyperscale builds are therefore being engineered to support very high rack densities and power delivery that can comfortably support AI workload scale.”

He also points to the emergence of AI-driven infrastructure management systems that optimise thermal efficiency and energy utilisation in real time. “We see much deeper integration between power, cooling, and digital systems, where AI and telemetry drive real-time optimisation of PUE, thermal performance, and uptime,” Arora says.

Nama says rack densities that once averaged 5-10 kW are now increasing to 40-100 kW in AI-focused

environments: “This leads to liquid cooling, modular architectures, and integrated compute-cooling systems.” Also, from an investment perspective, the economics of digital infrastructure are also changing rapidly.

“AI infrastructure requires substantial capital, with hyperscalers and enterprises boosting long-term capex to secure scalable compute,” Nama says. “At the same time, there is a move toward flexible models such as phased campus builds, GPU-as-a-service, and hybrid ownership to optimise utilisation and manage AI hardware’s evolving lifecycle.”

Arora believes future competitiveness will depend less on sheer scale and more on operational efficiency and infrastructure resilience. “Returns will increasingly be driven by the ability to deliver ultra-high density reliably, secure round-the-clock low-carbon power, and run facilities with AI-driven operational intelligence,” he says.

THE INTERNET FACES RESOURCE PRESSURES

For much of the internet era, data centres remained largely invisible despite underpinning almost every aspect of modern digital life. That invisibility is rapidly disappearing.

As AI drives unprecedented demand for compute power, the physical systems supporting the digital economy are becoming inseparable from broader debates over sustainability, industrial competitiveness, energy security, and national resilience.

The future of AI may depend not only on breakthroughs in algorithms and chips, but on whether nations and infrastructure providers can secure enough electricity, cooling capacity and sustainable resources to support the next phase of digital growth.

What users experience as seamless intelligence is, underneath, an enormous industrial system competing for power, water, land and geopolitical advantage at a scale the internet economy has never faced before. 🌐

ayushis@cybermedia.co.in

DATAQUEST MAY 2026 EDITION: MAKE IN INDIA: HOW FAR HAVE WE COME?

ALSO READ MORE ON

- AWS Summit 2026: India's AI Story Moves Closer To Production
- Why India's AI Future Needs Both Sovereign Control And Heritage Depth?
- Sify's Sharad Agarwal On Why India's Data Centre Story Is Now A 10 GW Baseline
 - Where AI is Already Executing Work in Aerospace
- Are You Talented Enough?: Seven skills to stay relevant in the AI era.
 - Made-in-India Chips: 'Wedge'ing the Semicon Door Open
- Made-for-India – not exactly Made-in-India – and here's why - Jackie Lee



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

The next telecom superpower may operate from orbit

Backed by Starlink and xAI, SpaceX's proposed USD-2-trillion IPO is betting that the future of telecom and AI infrastructure will operate from orbit.



BY JAIDEEP GHOSH

In April 2026, SpaceX confidentially filed a draft IPO registration with the US Securities and Exchange Commission (SEC), targeting a June 2026 listing at a valuation of USD 2 trillion and seeking to raise approximately USD 75 billion. This will be the world's largest-ever IPO—surpassing Saudi Aramco's USD 29 billion record debut in 2019—and will place

SpaceX among the ten largest global companies by market capitalisation.

At USD 2 trillion, SpaceX will be valued above Meta, Berkshire Hathaway, and Musk's own Tesla. It is also the first of an anticipated trio of 2026 mega-IPOs, preceding the expected listings of OpenAI and Anthropic.

SpaceX is repositioning itself from a rocket launch company into a telecom, AI, and orbital infrastructure powerhouse serving global markets worldwide at scale.

Starlink's rapid scale is transforming low-earth orbit from a niche satellite service into a mainstream communications infrastructure for global connectivity.

THE SPACEX IPO FACT SHEET

Key Metric	Proposed SpaceX IPO Details (June 2026)
Target Valuation	USD 2.0 trillion
Capital to be Raised	~USD 75 billion
Listing Venue	NASDAQ
Expected Float	~3.3% to 5%
Lead Underwriters	Morgan Stanley, Goldman Sachs, JPMorgan Chase, Citigroup, BofA
Strategic Acquisitions	xAI (Merged February 2026). Cursor, a code editing start-up (Announced intent in April 2026)

At nearly 125x its estimated 2025 revenue of ~USD 16 billion, this valuation demands an explanation. Two strategic milestones provide the narrative foundation: Starlink's crossing of 10 million subscribers across 150+ markets, and the USD 250 billion merger with xAI in February 2026.

These have repositioned SpaceX from a capital-intensive launch provider into a global telecom and AI infrastructure platform—what Musk is marketing as an “Orbital Intelligence” play.

THE IPO ARCHITECTURE

The SEC registration reveals a dual-class share structure designed to preserve Musk's voting control. Unusually, 30% of the offering is reportedly allocated to retail investors—a deliberate extension of the “founder brand” ecosystem Musk has cultivated, intended to attract long-term Tesla shareholders.

The financial trajectory is instructive. From a private valuation of USD 46 billion in 2020, SpaceX reached USD 800 billion by early 2025. The xAI merger in February 2026 reset the baseline to USD 1.25 trillion. The leap to the USD 2 trillion IPO target in four months reflects market conviction in the Space-AI narrative.

VALUE DRIVER 1: STARLINK — THE GLOBAL LEO BACKBONE

Starlink is the primary engine of value. With over 10,000 satellites in orbit—roughly two-thirds of all active satellites globally—SpaceX has built an unmatched satellite communications network.

As of February 2026, the service crossed 10 million subscribers and generated ~USD 11.4 billion in revenue in 2025, a 50% year-over-year increase. More significantly, Starlink achieved an EBITDA margin of 63%, well above the 30-40% margins typical of global mobile operators.

STARLINK FINANCIAL PERFORMANCE

Starlink Growth Metrics	2024 Actuals	2025 Actuals	2026 Projections
Global Subscribers	~4.5 million	9+ million	16.8 – 25 million
Revenue	~USD 7.6 billion	USD 11.4 billion	USD 18.7 – USD 20 billion
EBITDA Margin	50%	63%	Projected 70%+
Satellites in Orbit	~6,500	~10,000	~14,000+

The integration of xAI signals a future where orbital communication networks also become distributed intelligence and compute infrastructure platforms globally.

The launch of “Starlink Mobile” (formerly Direct-to-Cell) at MWC 2026 marks a critical inflexion. By connecting unmodified smartphones directly to its constellation, Starlink is eliminating cellular dead zones globally. The transition from last-resort rural connectivity to first-choice global LEO backbone—directly challenging terrestrial telecom incumbents—is now largely complete.

VALUE DRIVER 2: THE XAI MERGER – THE INTELLIGENCE LAYER

The USD 250 billion merger with xAI provides the AI intelligence layer atop Starlink’s connectivity infrastructure. Integration of xAI’s Grok model enables proprietary Starlink telemetry to drive real-time AI training, creating a self-reinforcing data flywheel.

For investors, this transforms SpaceX from a communications utility into backbone infrastructure for next-generation AI-driven industries—spanning autonomous defence applications to real-time global financial analytics.

VALUE DRIVER 3: ORBITAL COMPUTE – THE SPACE DATA CENTRE

Earth-bound AI data centre development faces

structural constraints: power, land, and cooling. SpaceX’s response is relocating heavy compute workloads to orbit. In January 2026, the company filed with the FCC for a constellation of up to one million solar-powered satellites engineered to function as orbital data centres.

The commercial viability of this “compute-in-orbit” model hinges on Starship achieving the launch cost reductions needed to make it economically competitive with terrestrial infrastructure.

VALUE DRIVER 4: VERTICAL INTEGRATION

Unlike traditional aerospace firms dependent on complex subcontractor webs, SpaceX manufactures its engines, hulls, satellites, and user terminals in-house. This confers cost advantages and deployment speed that terrestrial operators cannot replicate, creating durable technical and economic moats that underpin the long-term valuation case.

THE VALUATION PARADOX: A NEW ASSET CLASS

The arithmetic is stark. At ~125x 2025 revenue, SpaceX’s proposed multiple dwarfs Tesla (~16.5x), Palantir (~43x), and high-growth SaaS firms at 15-20x. Traditional telcos rarely exceed 6-15x EV/EBITDA.

VALUATION MULTIPLE COMPARATIVE			
Company	Market Cap (Approx. April 2026)	2025 Revenue	EV/Sales Multiple
NVIDIA	USD 4.61 trillion	USD 187.1 billion	~24.6x
Alphabet	USD 3.92 trillion	USD 402.8 billion	~9.7x
Apple	USD 4.03 trillion	USD 435.6 billion	~9.3x
Microsoft	USD 3.07 trillion	USD 305.5 billion	~10.1x
SpaceX (IPO Target)	USD 2.00 trillion	USD 16.0 billion	~125.0x
Tesla	USD 1.56 trillion	USD 94.8 billion	~16.5x
Meta Platforms	USD 1.71 trillion	USD 201.0 billion	~8.5x
Berkshire Hathaway	USD 1.07 trillion	USD 372.1 billion	~2.9x

The proposed IPO could accelerate a structural shift in telcos as communications infrastructure increasingly expands beyond terrestrial networks worldwide at scale.

Sustaining a USD 2 trillion valuation requires investors to accept that SpaceX is not an aerospace company or a telco but a new asset class—"Space-AI"—part telecom carrier, part data centre provider, part defence infrastructure play—positioned to capture a dominant share of a projected USD 10 trillion space economy.

The valuation premium is effectively the market's "Imagination Premium": the delta between a conventional DCF value and what investors will pay for "Brand-Musk" and the prospect of orbital intelligence becoming the backbone of the global economy.

THE JIO PARALLEL

A useful parallel exists between SpaceX's ambitions and Reliance Jio's upcoming IPO, targeting ~USD 170 billion for Jio Platforms Ltd. Ambani, like Musk, is selling a narrative of integrated intelligence: "Jio-Brain" AI-ready data centres, Nvidia GH200 superchip partnerships, and a media monopoly via Jio-Star.

The structural difference is context. Jio's monthly ARPU of USD 2-3 is a fraction of Starlink's USD 100+ in Western markets. The Indian model must solve for affordability before achieving mass rural penetration—a constraint that meaningfully caps the addressable premium.

THE MUSK IMAGINATION PREMIUM

The premium Musk commands is grounded in an exceptional track record: rocket reusability achieved ahead of all forecasts, a 50%+ share of global launches, and the world's largest satellite constellation built within a decade.

Musk has a proven track record of value creation. For example, Tesla's market cap exceeds the combined market caps of Toyota, GM, and Ford. This execution history has kept institutional investors, including Alphabet and Fidelity, significantly invested in SpaceX. Narrative alone does not sustain a USD 2 trillion valuation; execution credibility adds to it.

THE OVERALL RISK ASSESSMENT

The primary risk is technical. If Starship V3 fails to achieve commercialisation targets, the economic

logic of orbital data centres—and the entire Space-AI narrative—unravels.

Regulatory headwinds add complexity: national security concerns over undisclosed foreign investments have prompted calls for increased oversight, potentially complicating the IPO roadshow. Geopolitically, SpaceX's centrality in military communications (most visibly in Ukraine) has drawn scrutiny over Musk's personal diplomacy alongside the company's dependence on U.S. government contracts.

Most consequentially, there is Key Man risk. The USD 2 trillion valuation is inextricably tied to Elon Musk. Any distraction from Tesla, X, or the Mars programme—let alone an exit—could rapidly erode the Vision Premium that accounts for the bulk of this valuation.

For the communications industry, the strategic implication is clear: the network edge is no longer at the cell tower or the fibre cabinet—it is in orbit. If the June 2026 IPO succeeds at the USD 2 trillion level, it will reshape the global technology landscape, elevating what may become a "Space-AI 3"—SpaceX, NVIDIA, and Amazon, alongside the existing Magnificent 7.

SpaceX's transition from rocket company to infrastructure utility to orbital intelligence platform—positioning itself as the operating system for the planet—represents the most ambitious corporate pivot in corporate history.

Whether it resolves as bold foresight or a speculative bubble will be determined over the next decade of execution. What is already evident, however, is this: in today's communications economy, narrative is more valuable than spectrum. Musk has weaponised both, and global capital has already bought into the USD 2 trillion dream. 🚀

The author is the Group President, FyneHand Group, a boutique advisory and human capital firm. He is a former Big 4 Partner and writes on strategy, technology, and macroeconomics.

(Views are personal.).

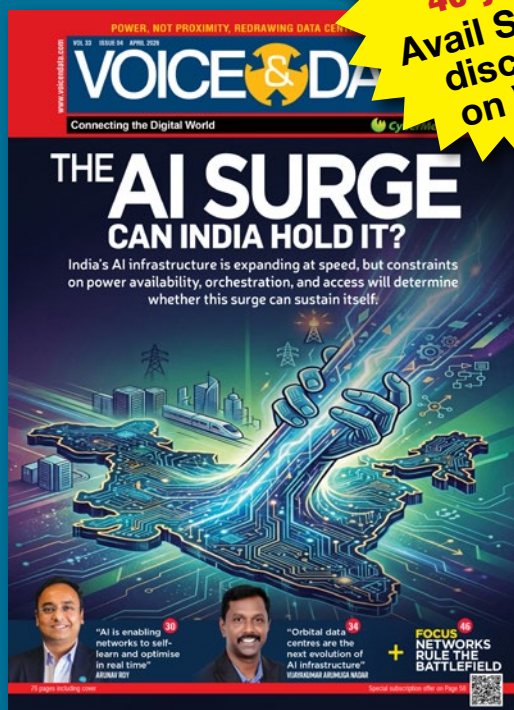
feedbackvnd@cybermedia.co.in



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.

India's quantum push needs telecom-scale networks

India's quantum ambitions will depend on telecom integration, regulatory clarity, and scalable frameworks for secure communications.



BY GAURAV SAHAY

India's ambition to build a national quantum communication network sits at the crossroads of technological sovereignty and geopolitical positioning. Unlike conventional telecommunications infrastructure, quantum communication redefines the very architecture of secure data exchange by embedding security into the transmission itself.

This shift is not merely technological but structural; it demands a reconfiguration of policy frameworks, telecom infrastructure, industrial participation, and international strategy. India's current trajectory, led by its National Quantum Mission (NQM), provides a foundational

blueprint. Still, the path to a fully operational, scalable, and globally competitive quantum communication network is layered with legal, regulatory, and infrastructural complexities.

At the core of India's push lies a comprehensive quantum ecosystem. The mission explicitly targets satellite-based secure quantum communication over 2,000 kilometres, intercity QKD networks, and multi-node quantum networks integrated with quantum memories.

This is not a purely academic initiative. It is structured as a national capability program with dual-use implications

Quantum communication is becoming a geopolitical battleground where alliances, interoperability, and trusted standards will define influence in the quantum era.

across defence, finance, and critical infrastructure. The recent demonstration of a 1,000-kilometre indigenous quantum communication network signals that India is transitioning from laboratory-scale experimentation to field-deployable infrastructure.

This shift is critical because quantum communication networks are not incremental upgrades to existing telecom systems; they require fundamentally different architectures.

QUANTUM NETWORKS BEYOND RESEARCH

From a policy standpoint, enabling quantum communication in India requires a multi-layered regulatory architecture that does not yet fully exist. At present, quantum technologies fall within a fragmented governance framework spanning the DST, DoT, DRDO and sectoral regulators.

While the NQM provides strategic direction, it does not yet translate into a comprehensive legal regime governing deployment and spectrum use, particularly for free-space optical links, cross-border quantum data flows, or liability frameworks for quantum-secure infrastructure. The absence of a dedicated or integrated regulatory code creates ambiguity, especially in areas such as the licensing of QKD networks, the certification of quantum devices, and compliance with national security directives.

Given that quantum communication inherently implicates encryption policy, it will inevitably intersect with India's evolving stance on encryption regulation, lawful interception, and data localisation. The legal tension here is structural.

While the state retains a legitimate interest in law enforcement and national security, reconciling these competing imperatives will require a calibrated statutory framework that balances cryptographic autonomy with sovereign oversight.

REGULATING QUANTUM COMMUNICATION

Equally central is the question of infrastructure

integration. Quantum communication cannot exist as a standalone network. It must be layered on top of existing telecom backbones. India's fibre-optic infrastructure, built and operated by public and private telecom players, must serve as the substrate for QKD systems.

Since quantum signals degrade over distance and cannot be amplified using conventional repeaters, this necessitates segmented networks connected by trusted nodes, which creates both engineering and legal challenges. From a legal perspective, it raises questions of network ownership, liability allocation across nodes, and standards for trust certification of intermediate nodes.

Besides, telecom operators will need to evolve from mere carriers of data to custodians of quantum-secure infrastructure, which will require amendments to licensing frameworks.

INTEGRATING QUANTUM WITH TELECOM

A public-private partnership (PPP) will be indispensable in this transition. The success of India's early quantum communication milestones has already demonstrated the role of the startup ecosystem.

The mission's expansion to support multiple deep tech startups reflects a deliberate policy choice to decentralise innovation and avoid over-reliance on state-led R&D. However, scaling from pilot deployments to nationwide infrastructure will require structured PPP models akin to those used in India's telecom and digital public infrastructure (DPI) ecosystems.

This includes viability gap funding, long-term procurement commitments from government agencies, and co-development frameworks with telecom operators. Legally, PPP contracts in this domain will need to address highly specialised risks, including technology obsolescence, cryptographic failure, export control restrictions, and intellectual property ownership in jointly developed quantum technologies.

Also, standardisation and contracts will need to evolve rapidly to accommodate these unique risk vectors.

India's quantum communication ambitions are moving beyond laboratory pilots toward telecom-scale infrastructure for secure national connectivity systems nationwide.

Another critical dimension is the integration of quantum communication with India's broader digital and telecom strategy, particularly 5G and the emerging 6G ecosystem. Quantum networks are not expected to replace classical networks but to operate as a secure overlay for sensitive communications.

This necessitates interoperability standards between quantum and classical networks, including post-quantum cryptographic protocols that can function within existing internet architectures. India's telecom R&D institutions, including C-DOT, have already been positioned as key nodes in the quantum communication ecosystem, signalling an intent to embed quantum capabilities within the national telecom infrastructure.

The legal implication here is the need for harmonised standards to ensure that quantum communication systems can interoperate across jurisdictions, particularly in cross-border data flows and international communication networks.

INDIA IN THE GLOBAL QUANTUM ORDER

On the global stage, quantum communication is rapidly becoming a domain of strategic competition, with countries such as China, the USA, and the EU investing heavily in quantum networks and satellite-based QKD systems. India's progress, particularly the rapid deployment of a 1,000-kilometre network, positions it as an emerging player in this domain.

However, global positioning will depend not merely on technological capability but on India's ability to shape international standards and alliances. Quantum communication networks will likely evolve into a federated global system, where interoperability, trust frameworks, and mutual recognition of security standards become critical.

India must therefore engage with international standard-setting bodies, pursue bilateral technology partnerships, and build strategic alliances to ensure its quantum ecosystem is not isolated. At the same time, export controls and technology transfer restrictions,

particularly in dual-use technologies, will shape India's engagement.

The challenges, however, remain substantial. Technologically, the absence of mature quantum repeaters limits the scalability of terrestrial networks, while satellite-based systems introduce high costs and operational complexities.

Economically, deploying quantum infrastructure at scale is costly, with uncertain commercial returns in the early stages. Legally, the absence of a comprehensive regulatory framework creates uncertainty for private investment.

From a cybersecurity perspective, while quantum communication promises unbreakable encryption, it also necessitates a transition, creating a dual burden of upgrading both quantum and classical infrastructures. From an institutional standpoint, coordination across multiple government agencies and stakeholders remains a non-trivial challenge.

Building India's quantum communication network is not merely a question of technological deployment but one of systemic transformation. It requires a coordinated policy push that integrates legal frameworks, telecom infrastructure, and industrial participation into a cohesive ecosystem.

PPPs must be structured to derisk innovation while enabling scale, and telecom networks must evolve to accommodate quantum layers. Simultaneously, India must position itself within the global quantum order through standards leadership and strategic alliances.

The success of this endeavour will ultimately depend on whether India can move beyond mission-mode experimentation to institutionalised, regulated, and commercially viable quantum infrastructure, elevating it from a strategic capability to a foundational layer of its digital economy. 🌟

*The author is the Founding Partner at
Arthashastra Legal.
feedbackvnd@cybermedia.co.in*



Fibre-ready buildings gain a new edge in property value

Pre-installed FTTx infrastructure is shortening ISP onboarding timelines while strengthening tenant appeal and long-term asset performance.



BY PANKAJ TAMBE

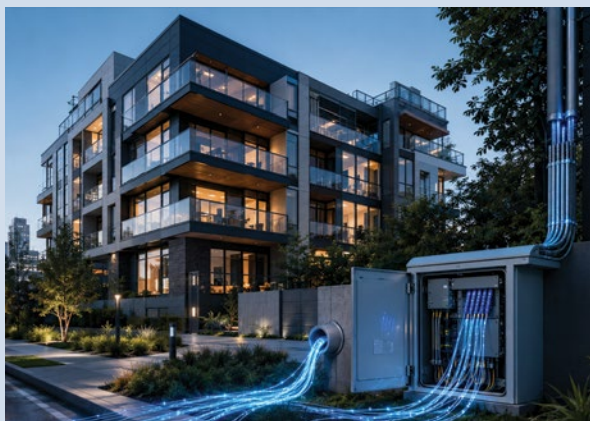
Real estate and digital infrastructure have been converging for some time now. Yet, for much of this period, connectivity has been treated as an amenity to be arranged after a building is ready, rather than as a foundational element to be designed in from the start. That approach is changing, and the

consequences of that change are beginning to show up in how assets are valued, how tenants make decisions, and how quickly buildings can become operationally ready.

The shift is being driven by FTTx fibre-to-the-x, a collective term for the family of fibre-based infrastructure

Connectivity infrastructure is steadily shifting from a post-construction utility into a defining factor in modern real estate valuations and leasing strategies.

Buildings with pre-installed fibre infrastructure are increasingly attracting enterprise tenants nationwide seeking faster, disruption-free onboarding.



IN BRIEF

- Pre-installed FTTx infrastructure can reduce ISP onboarding timelines from weeks to just a few days.
- Fibre-ready buildings improve tenant experience by enabling faster occupancy and reliable digital access from day one.
- Connectivity ratings are becoming a growing factor in leasing, investment due diligence, and asset positioning.
- Shared passive fibre infrastructure lowers deployment costs and enables multiple ISPs to serve the same property.
- Installing fibre pathways during construction is significantly cheaper than retrofitting occupied buildings later.
- Enterprise tenants increasingly view digital infrastructure quality as a core operational and business requirement.

architectures that bring high-speed connectivity into and across buildings. When pre-installed at the construction or fit-out stage, FTTx infrastructure is proving to be one of the more consequential investments a developer or building owner can make.

POOR FIBRE PLANNING DELAYS ONBOARDING

One of the most immediate and practical benefits of pre-installed fibre infrastructure is its impact on ISP onboarding timelines. In buildings without a structured fibre backbone, every new ISP or tenant requiring connectivity must begin a largely fresh process of site surveys, last-mile cable laying, duct access negotiations, and provisioning queues. What should take days can stretch into weeks or even months.

This delay is not a technology limitation. It is an infrastructure gap. Buildings that have invested in carrier-neutral passive fibre infrastructure, including horizontal and vertical distribution pathways, riser management, and termination points, allow service providers to activate within days. The building is ready for connectivity from day one of occupancy. For tenants, this means business continuity. For landlords and developers, it means faster occupancy and fewer service complaints in the critical early period of a tenancy.

Experience across large-scale deployments in commercial and mixed-use developments across India indicates that buildings where fibre infrastructure is planned early and installed before fit-out enable ISP onboarding timelines that are significantly shorter, often by several weeks, compared to buildings where infrastructure is retrofitted post-construction.

BUILDING RATINGS AND DIGITAL INFRASTRUCTURE

A related and growing dimension of this shift is the formal assessment and rating of digital infrastructure. Much as green building certifications created a structured framework for evaluating environmental performance, connectivity-focused building rating systems are now doing the same for digital readiness.

Shared passive fibre networks allow multiple ISPs to operate efficiently while reducing infrastructure duplication across large commercial properties nationwide.

A strong FTTx network with documented passive cabling standards, multiple ISP options, redundant pathways, and clearly defined performance benchmarks positions a building well within these rating frameworks. These ratings are no longer just technical badges. They are increasingly referenced in leasing materials, factored into institutional due diligence, and cited in investment assessments. For developers competing for enterprise tenants or institutional capital, a strong connectivity rating is becoming a credible differentiator. The direction is clear: digital infrastructure quality is moving from a back-of-house operational matter to a front-of-brochure asset story.

FIBRE INFRASTRUCTURE SHAPES ASSET VALUE

Evidence of FTTx infrastructure's impact on property valuations is still developing in the Indian context, but the directional signals are consistent. In commercial real estate, enterprise tenants are demonstrating a willingness to pay a modest premium for buildings that eliminate connectivity uncertainty. In residential real estate, the impact tends to show in absorption velocity projects with pre-installed fibre infrastructure that move faster at the point of sale and experience lower post-possession churn.

For institutional investors and REITs, the value proposition is rooted in income stability. Faster ISP onboarding, lower tenant attrition, and reduced vacancy risk all contribute to more predictable Net Operating Income. As asset managers become more sophisticated in their assessment of building quality, these operational benefits are increasingly reflected in capitalisation rate assumptions.

WHY EARLY FIBRE PLANNING STILL MATTERS

The most cost-effective moment to install FTTx infrastructure is during construction. At the slab stage, installing conduit pathways, riser systems, and equipment spaces adds relatively little to the overall project cost. Retrofitting the same infrastructure into an occupied or completed building is significantly more expensive and disruptive.

This is prompting a gradual but meaningful shift in how developers approach project planning. Connectivity infrastructure, such as structural design and MEP systems, is increasingly entering the conversation at the blueprint stage rather than as an afterthought. When fibre pathways are designed into a building from the outset, the result is a cleaner installation, better performance, and a foundation that can accommodate evolving connectivity needs without requiring structural intervention later.

SHARED FIBRE NETWORKS IMPROVE EFFICIENCY

Pre-installed FTTx also enables a shared infrastructure model that benefits all parties. A common passive network allows multiple service providers to operate within the same building without duplicating physical infrastructure. This reduces capital expenditure, lowers the barriers to ISP entry, and gives tenants genuine choice, a feature that is increasingly valued in both commercial and residential markets.

Shared infrastructure also creates efficiencies in ongoing management. A single, well-documented passive network is easier to maintain, upgrade, and audit than a building with multiple competing cable runs from different operators. This model consistently delivers more efficient deployments and stronger long-term network performance than fragmented, operator-specific installations.

Connectivity is becoming central to how real estate is both developed and experienced. FTTx infrastructure sits at the heart of this transition, enabling faster ISP onboarding, supporting formal building ratings, and contributing to asset valuations in ways that are becoming harder to ignore.

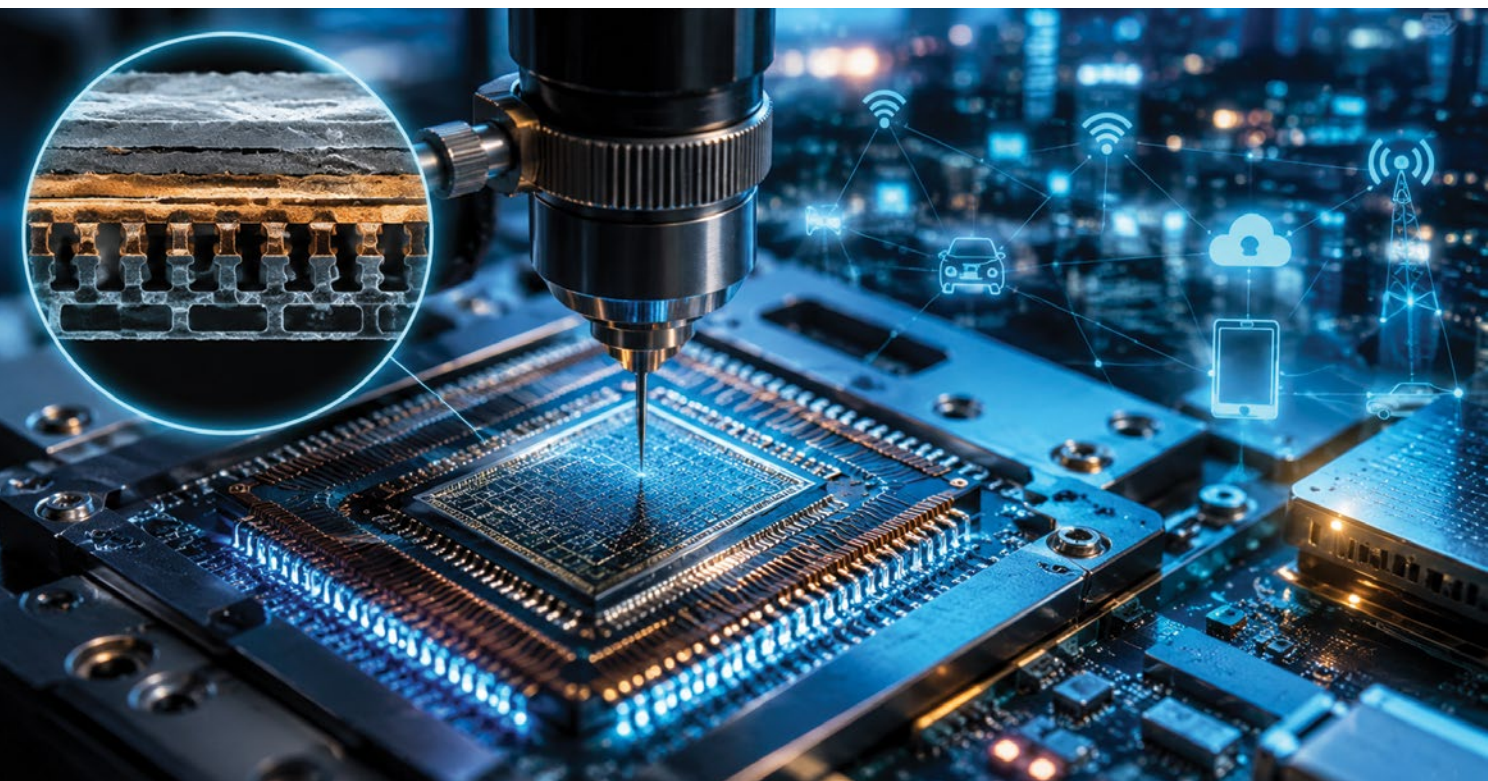
The buildings that integrate this infrastructure early will carry a structural advantage throughout their operational life. The window to do so efficiently during construction is short-lived once a project is complete. 🏗️

*The author is the Vice President and Business Head – Mobility with iBUS Networks.
feedbackvnd@cybermedia.co.in*



Chip reliability critical in the connected world

As connected electronics grow more complex, advanced materials analysis is becoming critical to predicting chip reliability and long-term resilience.



BY DR RAJEEV GAUTAM & PARIKSHIT SENGUPTA

The modern world runs on chips, and their reliability is more important than ever. Think about electric vehicles navigating busy streets or the medical devices that keep people alive in emergencies; the dependability of semiconductors is now directly tied to safety, trust, and the seamless functioning of these systems.

As electronics increasingly interconnect, the repercussions of any failure have expanded significantly. A localised issue can now lead to far-reaching disruptions across communication networks, industrial platforms, and essential infrastructure.

For CXOs, semiconductor reliability has evolved beyond a mere technical specification; it is now a key factor

Semiconductor reliability is increasingly shaped by invisible material interactions that emerge only under prolonged thermal and electrical stress conditions.

As AI systems, EVs, and communication networks scale rapidly, chip resilience is becoming a global strategic infrastructure and business concern.

influencing business success. A single chip's malfunction in a crucial system can trigger millions in unforeseen downtime, inflict significant reputational harm, and heighten compliance vulnerabilities. Conversely, maintaining service continuity through dependable component performance safeguards financial stability and cultivates a lasting competitive advantage.

MATERIALS FAILURES SHAPE CHIP RISKS

The heart of this reliability dilemma often rests on a frequently overlooked truth: the majority of failures do not stem from circuits or systems but from the fundamental materials themselves. Today's semiconductor devices are defined by extraordinary complexity. Ultra-thin films, heterogeneous material stacks, advanced packaging architectures, and extreme operating environments are no longer exceptions; they are the norm. Each layer and interface introduces potential reliability risks, many of which remain invisible during conventional electrical testing and only emerge after prolonged field operation.

Consequently, in highly scaled and complex devices, reliability cannot be merely "tested in" at the final production stage. It must be comprehensively understood, predicted, and engineered, starting with the material stage itself. As feature sizes shrink and chip density increases, tolerance margins narrow sharply. Trace contamination at parts-per-billion levels, slight deviations in film thickness, or residual stresses introduced during deposition and packaging can alter device behaviour over time. In a networked environment, even temporary disruptions can precipitate significant operational failures, safety hazards, or a widespread erosion of trust in the system's reliability.

THERMAL STRESS DRIVES RELIABILITY GAPS

These difficulties are exacerbated by thermal stress. Contemporary electronic components, which drive AI accelerators, electric vehicle powertrains, and high-frequency communication networks, function at power densities previously unseen. Consequently, increased temperatures accelerate the degradation of materials, including electromigration, interdiffusion, and dielectric

breakdown. Managing heat is therefore not only a design challenge but a core materials challenge, requiring deep insight into how materials behave under sustained electrical and thermal stress.

According to broader industry consensus and leading semiconductor research consortia, this reality is driving a fundamental shift in the industry's approach to reliability. Instead of focusing primarily on reactive failure analysis, manufacturers are increasingly adopting predictive quality strategies. The objective is no longer just to explain why a device failed but to understand where degradation begins, well before functional failure occurs in the field.

ADVANCED ANALYSIS REVEALS HIDDEN RISKS

Such an approach depends on precise, repeatable, and highly sensitive material characterisations. Advanced analytical techniques effectively shine a light on the unseen, enabling engineers to detect composition, stress, interfaces and even nanoscale defects that electrical tests alone cannot characterise.

Many reliability risks do not manifest as sudden failure events but as gradual, progressive degradation across interfaces or within material structures. Without early detection of these subtle changes in the development cycle, managing long-term device reliability becomes an insurmountable task.

SUPPLY CHAINS COMPLICATE CHIP QUALITY

The global nature of semiconductor supply chains adds another layer of complexity. The geographical distribution of fabrication, packaging, assembly, and testing operations makes it more difficult to ensure consistent material quality.

Even when using identical process recipes, outcomes can diverge due to subtle differences in raw materials, processing parameters, or environmental conditions. Without uniform analytical methods and correlated data across sites, such variability can quietly undermine yield and long-term reliability.

Advanced materials analysis is helping manufacturers identify degradation risks early, before failures emerge across real-world deployments at scale.

For organisational leadership, this situation necessitates a proactive, strategic response. CXOs need to demand a cultural shift in supplier validation that goes beyond the high-level considerations of electrical compliance and requires vendors to provide rigorous, materials-level proof that their components will be stable. Building strong materials analysis capabilities is no longer a mere technical exercise; whether in-house or through model partnerships, this investment is nothing less than a critical risk-mitigation strategy that protects product lifecycles and supply chain integrity.

This is particularly significant for India's burgeoning semiconductor industry. As the nation develops its skills in design, fabrication, packaging, and electronics manufacturing, it must meet demanding global reliability standards from the start. India's aspirations in the semiconductor sector demand more than just large-scale manufacturing; they also necessitate a steadfast commitment to quality and reliability.

Establishing strong material characterisation methods from the beginning is essential. This will ensure that Indian-made devices not only meet but also exceed the reliability standards set by international markets. Moreover, this approach will shorten the learning curve and build trust with international collaborators.

SAFETY-CRITICAL SYSTEMS DEMAND RELIABILITY

The significance of comprehending materials at the atomic or molecular level is particularly pronounced within safety-critical domains. The reliability of semiconductor chips directly affects both human safety and compliance with regulatory mandates across sectors such as automotive electronics, industrial automation, and healthcare technologies. Material analysis is essential for validating the resilience of these components under extreme temperatures, mechanical strain, humidity, and prolonged operational periods.

Consequently, international regulatory agencies and industry standards organisations are adapting their

frameworks to reflect these considerations. Frameworks such as the automotive industry's AEC-Q100 standards for integrated circuits and stringent medical device compliance protocols like ISO 13485 increasingly demand scientific evidence that materials and interfaces will remain stable under real-world conditions, not merely that devices passed initial, short-term qualification tests.

Advanced analytical techniques, including spectroscopy, elemental analysis, surface characterisation, and thermal measurements, enable manufacturers to build evidence with absolute certainty. When combined with process data and modelling, these insights support the early identification of risk patterns, improving manufacturing yields while simultaneously strengthening long-term reliability.

MATERIALS ANALYSIS AS STRATEGIC FORESIGHT

In a deeply connected world, reliability cannot be defined by isolated performance benchmarks. It must be measured in resilience over time, across environments, and within complex systems of systems. Achieving that resilience requires a deeper understanding of materials, not as static inputs, but as dynamic contributors to device behaviour throughout the entire semiconductor lifecycle.

As the industry enters its next phase of growth, advanced materials analysis will be less about measurement alone and more about strategic foresight. In the race toward faster, smaller, and more powerful electronics, long-term success will favour organisations that recognise that dependable technology begins long before the first chip is powered and that digging deeper into materials is the ultimate key to building electronics the world can rely on. 🧩

Dr Gautam (left) is the President, and Sengupta is the Group Field Officer – Materials and Semiconductor at HORIBA India, respectively.

feedbackvnd@cybermedia.co.in



PCQUEST MAY 2026 EDITION INDIA PLAYS. BUT WHO OWNS THE GAME?

ALSO READ MORE ON

- How AI is reshaping games and the designers who build them
 - Why mobile apps must defend themselves in real time
- How AI and biometrics are redefining high-stakes examination infrastructure
- AI debt is the real GenAI trap • Inside India's evolving esports growth engine
 - 7 most anticipated games of 2026
- Your gaming laptop choice might already be outdated
- REVIEW: EvoFox Deck 2 | OnePlus Nord Buds 4 Pro | Mini UPS for AirFiber V3.0



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

Beyond BharatNet: Building resilient rural networks

India's rural digital expansion will depend on integrated towers, fibre, backhaul, and resilient networks built for difficult terrain and reliable uptime.



BY SHASHANK AGARWAL

India's digital transformation is often measured in subscriber growth, data consumption, and the expanding reach of digital services. There are more than 950 million active internet users in the country today. Almost 57% of them live in rural areas, which are growing almost four times faster than urban areas.

With an estimated one billion users overall and over one billion broadband subscriptions, India is well on its way to becoming one of the world's greatest digital ecosystems. But access is not the only thing that matters for inclusion; a stable, high-quality network experience in the most remote parts of the country is what really matters.

Connecting rural India is no longer just about expanding coverage footprints but about sustaining resilient network operations at scale.

Shared infrastructure models are emerging as the only viable path for expanding telecom connectivity in low-ARPU rural markets.

Getting more people online is only one part of connecting India. It is about finding a way to fix a complex infrastructure problem in places where making money is hard, getting approvals is hard, the terrain is unpredictable, and keeping operations going is hard. Not just one asset, but the whole network stack working together is what makes last-mile connectivity work. 38% of people in India still do not use the internet, even though it is growing quickly.

This shows how big the difference is between people who can get online and those who cannot.

RURAL NETWORKS AS INTEGRATED SYSTEMS

Towers, fibre, and backhaul all depend on each other to connect rural areas at the ground level. People often talk about these things separately, but they work together as one system. The access layer consists of towers that bring the signal closer to the end user.

Fibre has the capacity and transport needed to handle more traffic. Backhaul, which can be done via fibre, microwave, or satellite, ensures that local connections are actually connected to the larger network. The user experience will suffer if even one of these things is weak.

A tower without dependable backhaul cannot support meaningful data demand. Fibre without reliable power or active equipment support cannot ensure service continuity. Rural connectivity, therefore, is not an asset deployment exercise; it is an integration exercise.

This is exactly why big national programs like BharatNet need to be looked at through the lens of execution. There is no doubt that they are strategically important, but putting them into action shows how hard it is to build infrastructure in rural India. It is not just about putting up towers



IN BRIEF

- Rural connectivity depends on towers, fibre, and backhaul functioning together as one integrated infrastructure system.
- BharatNet execution challenges highlight the complexity of approvals, terrain, power, and multi-agency coordination.
- Rural telecom rollout remains commercially difficult due to low ARPU and longer infrastructure payback cycles.
- Shared towers, fibre corridors, and ducts are becoming critical for reducing duplication and improving viability.
- Long-term operations and maintenance planning are essential for sustaining uptime in remote rural deployments.
- India's digital inclusion goals will depend on networks designed around rural realities rather than urban assumptions.

BharatNet's rollout challenges reveal how terrain, permissions, logistics, and maintenance shape real-world connectivity outcomes.

or laying fibre, but getting right-of-way clearances from many governments, figuring out how to cross railroads and highways, ensuring workers can get to the site, setting up a reliable power supply, and coordinating the work of many agencies across different parts of the network.

In many cases, delays emerge because field-level conditions are more complex than central planning assumptions. A site may be technically feasible but difficult to access. Land may be identified, but local approvals may take time. Fibre may be laid, but restoration and protection remain weak, leading to repeated disruptions. Across hills, forests, rivers, and scattered settlements, deployment becomes slower, costlier, and operationally fragile. These are not peripheral issues: they define the pace and quality of rollout.

THE ECONOMICS OF RURAL EXPANSION

For telecom operators and infrastructure providers, the economic equation in rural markets is equally important. Rural rollout is strategically necessary, but commercially unviable. Operators have to commit large sums of capital upfront in markets where average revenue per user (ARPU) remains low, and demand grows gradually. The ROI is therefore long and harder to estimate.

This makes rural expansion fundamentally different from urban densification. In cities, the business case is supported by higher traffic, stronger monetisation, and faster tenancy creation. In rural India, the model has to accommodate lower revenue density and longer payback periods. That is why rollout decisions are shaped not just by coverage obligations, but by questions around long-term utilisation, infrastructure reuse, operating cost optimisation, and the ability to aggregate demand over time.

In this context, infrastructure sharing becomes central to viability. No operator can afford to treat rural deployment as a stand-alone, fully duplicated build in every geography. Shared towers, shared fibre corridors,

common ducts, and collaborative deployment models reduce capital duplication and improve the economics of expansion. They also shorten rollout timelines by lowering the number of fresh permissions and parallel site builds required.

The future of rural connectivity will depend significantly on how effectively the sector adopts such shared models. Passive infrastructure sharing has already demonstrated its value in improving efficiency and reducing costs. The next step is to deepen coordination amongst operators, public programmes, utilities, transport authorities, state agencies, and local administrations. In low-ARPU markets, coordination is not an administrative advantage; it is a commercial necessity.

BUILDING RESILIENT RURAL CONNECTIVITY

The other major shift is that we must look beyond just commissioning. The industry's focus has traditionally been heavily on milestones during the deployment phase, but the true value lies in resilience once deployment is complete. For rural networks, there are problems with power failures, fibre cuts, adverse climatic conditions, equipment maintenance issues, and uptime challenges in geographically dispersed locations. Without incorporating O&M from the beginning, there will be a continuing imbalance in service quality once the assets are in place.

Rural connectivity should not be viewed as a compliance-driven agenda. It is a long-term infrastructure opportunity that calls for patient capital, shared deployment frameworks, and a realistic understanding of ground conditions. India's digital ambitions will not be fulfilled by urban-centric network logic alone. They will be fulfilled when the last mile is designed with its realities in mind. In the end, connecting every village is less about reaching more points on the map and more about building networks that can endure. 🌱

The author is the Managing Director of Salasar Techno Engineering.

feedbackvnd@cybermedia.co.in



CCTV shifts from surveillance to security risk

New certification norms can bring traceability, firmware checks, and compliance discipline to a CCTV ecosystem that scaled before safeguards matured.



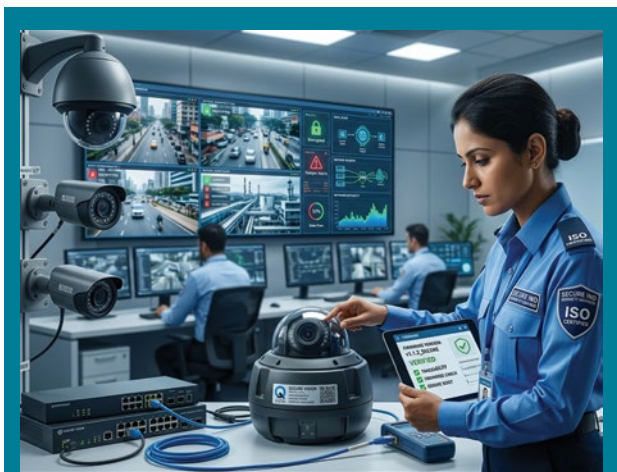
BY ARVIND BALI

In 2016, as India accelerated the deployment of CCTV cameras across enterprises, urban infrastructure, and residential complexes, the expansion was largely driven by a growing need for monitoring and safety. At the same time, several domestic companies entered the market with the intent to build Indian brands and, eventually, a self-reliant ecosystem.

However, beneath this rapid growth lay a structural constraint. While cameras were being installed at scale, the underlying ecosystem—from components to firmware—remained heavily dependent on imports. What India was building was not a fully indigenous surveillance network, but one assembled on external technological foundations.

India's CCTV expansion created domestic brands and distribution reach, but control over core components and system behaviour remained limited at scale nationally.

As surveillance networks expand, India's challenge is shifting from camera deployment to securing the intelligence layer that increasingly shapes governance and critical infrastructure.



IN BRIEF

- India scaled CCTV deployment before building control over components, firmware, and platforms.
- Local assembly created market presence, but not full technological ownership of the stack.
- Modern cameras are IP-connected edge nodes that can expand cyber risk across enterprises and cities.
- Firmware opacity, weak credentials, and unsecured data flows can turn cameras into attack points.
- Regulation from April 2026 brings traceability and firmware checks after years of deployment.
- India's next opportunity lies in trusted hardware, indigenous firmware, and video intelligence platforms.

LOCAL ASSEMBLY AND LIMITED OWNERSHIP

The early growth of India's CCTV industry followed a pattern in which local companies handled branding, distribution, and assembly but relied on completely knocked down (CKD) and semi-knocked down (SKD) imports for core components and system architecture.

This created a system in which market presence was local but technological control was not. A few companies, including CP Plus, were able to scale and establish a strong domestic presence. Yet even in such cases, the foundation remained linked to imported systems.

In contrast, global manufacturers such as Hikvision and Dahua Technology built vertically integrated ecosystems, controlling components, firmware, and platforms. This enabled them to shape not just production, but also system behaviour and data movement. The outcome was a structural imbalance: India expanded deployment, but not control.

IMPORT DEPENDENCE WITH HIGHER STAKES

This trajectory mirrors India's earlier dependence on mobile handset manufacturing, where imports dominated before policy interventions such as the Production Linked Incentive scheme helped build domestic manufacturing capacity.

However, surveillance infrastructure carries a different category of risk. Telecom networks handle communication, but CCTV systems capture continuous visual data about physical environments.

This distinction changes the implications of dependency. In telecom, the concern is interception of communication. In surveillance, it extends to visibility into movement, behaviour, and spatial patterns. Control over technology, therefore, becomes directly linked to control over real-world intelligence.

SECURED TELECOM BUT EXPOSED CAMERAS

India demonstrated strategic intent in the telecom sector

The strategic concern is no longer only who supplies the camera, but who controls firmware, updates, data flows, platform links, and integration over time.

by restricting participation by vendors such as Huawei and ZTE in critical infrastructure. These decisions were driven by national security considerations and the need to protect communication networks. However, similar scrutiny was not applied at the same scale to surveillance systems.

As CCTV deployments expanded across smart cities, enterprises, and residential complexes, the emphasis remained on rapid installation rather than ecosystem control. This created a divergence between two critical layers—communication networks that were secured early, and surveillance systems that scaled without equivalent safeguards.

EVERY CAMERA BECOMES A NETWORK NODE

The role of CCTV systems has evolved significantly over the past decade. Modern cameras are no longer passive recording devices. Each unit captures high-definition video, processes data locally, connects to IP networks, and integrates with cloud platforms.

In effect, every camera operates as a distributed edge computing node within a larger system. At scale, this creates a dense, interconnected grid of devices that continuously generate and transmit data. While this enhances capabilities such as remote monitoring and real-time analytics, it also expands the surface area for potential cyber threats.

VULNERABILITIES ACROSS THE FULL STACK

The risks within surveillance systems extend across multiple layers, beginning with firmware—the embedded software that controls device behaviour.

In many cases, firmware is proprietary and difficult to audit, limiting visibility into how systems function. This creates the possibility of hidden access pathways or unauthorised control mechanisms. Remote update capabilities, while necessary for maintenance, can also introduce vulnerabilities if not secured.

Data flow presents another dimension of risk. Beyond video footage, CCTV systems generate metadata that can reveal behavioural patterns and operational insights. If transmitted through unsecured channels or external dependencies, this data may be exposed to unauthorised access.

Network vulnerabilities further increase exposure. Weak credentials, outdated software, and unpatched systems can allow unauthorised entry into devices, which can then serve as access points into broader enterprise or city-level networks.

The scale of such risks has been demonstrated by incidents such as the Mirai botnet attack, in which compromised devices, including cameras, were used to cause large-scale disruptions to Internet infrastructure.

FROM MONITORING TO NATIONAL SENSING

As deployments increased, CCTV networks became embedded in governance and operational systems, supporting policing, traffic management, infrastructure monitoring, and urban planning.

This integration has effectively transformed surveillance systems into a nationwide sensing grid—one that continuously observes and records activity across environments.

With each camera acting as a connected edge device, weak security can expose enterprises, smart cities, and public systems to wider systemic risk at scale.

Certification, trusted supply chains, and indigenous video intelligence can help India move from assembly strength to stack-level control and value creation.

If compromised, such systems can enable mapping of sensitive locations, tracking of movement patterns, and accumulation of long-term intelligence. CCTV infrastructure, in this context, moves beyond monitoring and becomes part of a broader strategic framework.

Several countries recognised these risks and introduced restrictions on surveillance technologies from specific vendors. The United States limited the use of such equipment in federal systems and classified certain manufacturers as national security risks. Countries including Australia, Japan, and Canada adopted similar measures.

These actions were based on a consistent principle: control over the technology stack determines control over data access and movement.

REGULATION AFTER RAPID CCTV ROLLOUT

India has begun addressing these concerns through regulatory measures. The mandate for certification standards, effective from April 2026, introduces requirements such as component traceability, firmware transparency, and compliance validation.

These measures align with frameworks, including the Telecommunication Act 2023 and the Digital Personal Data Protection Act 2022, aimed at strengthening governance across digital infrastructure and data protection.

However, these interventions come after years of large-scale deployment, indicating that security frameworks are now being integrated into an already expanded ecosystem.

FROM MONITORING TO NATIONAL SENSING

The surveillance industry is also undergoing a transition in which value is created. Indian companies are increasingly focusing on video intelligence—developing systems for anomaly detection, behavioural analysis, and integrated command platforms. These technologies enable real-time interpretation of video data, moving beyond storage to actionable insights.

This marks a shift from simply capturing footage to understanding and acting on it, repositioning surveillance within a broader digital intelligence framework.

BUILDING CONTROL ACROSS THE CCTV STACK

India's experience with the Production Linked Incentive scheme in mobile manufacturing demonstrates how targeted policy can shift an ecosystem from import dependence to domestic capability. Applying a similar approach to surveillance could reshape the sector.

Expanding such incentives to include surveillance hardware and components can reduce reliance on imports. Developing trusted supply chains will be critical to ensure system integrity and reliability.

Equally important is the creation of indigenous firmware capabilities, which would provide greater control over how devices operate and communicate. At the same time, platform-led innovation in video intelligence can enable Indian companies to move higher in the value chain.

Enforcing data sovereignty frameworks will be essential to ensure that data generated within the country remains governed by domestic regulations and oversight.

As surveillance systems continue to expand, the central question is shifting. It is no longer limited to how many cameras are deployed, but extends to who controls the systems behind them, who has access to the data they generate, and how that data is used.

In a network where every camera functions as a node and every node produces intelligence, control over technology and data will determine how secure the system truly is. 🧠

The author is the Vice Chairman of GTS TechLabs and Board Advisor of Globe Teleservices.

feedbackvnd@cybermedia.co.in



India's new online gaming rules end grey zones

India's new gaming framework shifts regulation beyond the skill-versus-chance debate toward tighter oversight, compliance, and platform accountability.



BY ANANAY JAIN

India's online gaming industry is heading into a hard reset. A new legal regime, the Promotion and Regulation of Online Gaming Act, 2025, operationalised through the Promotion and Regulation of Online Gaming Rules, 2026, comes fully into force on 1 May 2026.

After more than a decade of fragmented state level regulation, drawn-out court battles over the “skill versus chance” debate, and persistent regulatory fog, the Centre has finally stepped in. The line it has drawn is decisive, which some would say blunt.

India's online gaming industry is entering a stricter era in which monetisation models matter more than the old skill-versus-chance debate across platforms.

The new regulatory framework places payment providers, advertisers, and intermediaries directly within the nationwide gaming compliance and enforcement structure.

The headline shift is unmistakable; all online money games are banned, whether they rely on skill or chance. That distinction, for years the industry's legal framework, no longer matters. Online gaming in India had taken shape within the margins of state gambling laws, surviving on exemptions, interpretations and legal interpretations.

That ecosystem scaled at pace, reaching roughly USD 3.7 billion in FY24. However, the momentum was abruptly disrupted on August 25. Deposit-and-win formats were criminalised not just for operators but also for advertisers, celebrity endorsers, and even payment intermediaries. At first glance, it looks bleak. But that is not the whole picture.

What the new regime actually does is re-engineer the industry around two clearly permitted categories: competitive esports and online social games that offer free play or rely on non-wagered monetisation.

INDIA REWRITES NATIONAL GAMING RULES

The Online Gaming Authority of India is at the heart of the new setup. Established as an attached office of the Ministry of Electronics and Information Technology (MeitY) and headquartered in Delhi, the Authority comprises senior officials from the Ministries of Home Affairs, Finance, Law, Information and Broadcasting, and Youth Affairs and Sports. It is also intended to function primarily as a digital office, in line with the industry it oversees.

The Authority has a broad spectrum of responsibilities. It will conduct legal scrutiny, publish a list of banned online money games, investigate complaints, issue binding guidance and codes of practice, hear appeals from users, and coordinate with banks and other law enforcement agencies. If anything, it is the national platform that now serves as the sole point of contact for online gaming regulation.

Start with the regulation; the Act outlines the endpoint, but it is the Promotion and Regulation of Online Gaming Rules, 2026, which tells you how that system is going to work. Framed by MeitY and enacted after extensive inter ministerial consultation and legal vetting, these Rules are



IN BRIEF

- India's new online gaming law bans all online money games regardless of skill or chance classification.
- Esports and online social games now operate under a single centralised regulatory framework nationwide.
- The Online Gaming Authority of India becomes the central body for oversight, appeals, and enforcement.
- Payment providers and advertisers can now face liability for enabling banned gaming transactions or promotions.
- Registration rules focus heavily on monetisation models, financial exposure, and user risk assessments.
- Platforms must implement grievance systems, disclosures, age controls, and fair play monitoring mechanisms.

Esports and social gaming platforms now gain regulatory clarity, but only within a far tighter compliance and oversight framework across India today at scale.

the user manual of the new regime. This is it to practice: theory has finally become process.

Essentially, the Rules are about creating structure out of confusion. They articulate a precise framework for classifying games, enforce timelines for regulatory decisions and centralise oversight in a single national authority. For an industry that has existed for many years with atomised supervision and changing goalposts, it is a real change in itself.

Next comes registration, but not uniformly. Initial concerns notwithstanding, the Rules deliberately avoid imposing a blanket requirement that every online game be registered. And that requirement applies only to e-sports and to those classes of online social games that the government might be able to notify in the end, by reference to factors such as risk, scale, and financial exposure for users. It is a more measured approach than many anticipated.

COMPLIANCE MOVES TO THE CENTRE STAGE

Upon registration, the Authority issues a digital certificate valid for up to 10 years. And the Rules leave no room for creative interpretation here: online money games are simply not eligible for recognition or registration as e-sports under any framework.

The registration also comes with strings attached. Approval-secure platforms incur ongoing obligations, provide clear disclosures of their data retention, have named points of contact, and include detailed directions for facilitating payment. This is not a time-sensitive hurdle; it will become part of your compliance relationship.

From there, the Rules shift focus to what really matters now: where the money flows. The Authority will look closely at whether users are depositing funds, whether they expect financial returns, and whether in game assets can be monetised beyond the platform. The old skill versus chance debate recedes into the background. The revenue model moves firmly to the foreground.

That obligation does not stop with game makers. Payment providers, advertisers, and intermediary

companies are now on the hook, too. They can be responsible for verifying registrations and blocking transactions from gambling products that promote banned money games. All user protections are built into the framework.

The Rules include user safety features that need to reflect a game's risk profile. These can include age verification, age-based access limits, time limits, parental controls, reporting tools, counselling support, and systems to monitor fair play. Most importantly, platforms must disclose such features when applying for classification or registration.

The Rules also serve to reinforce user rights by establishing a grievance mechanism. Every social game or esports platform will need a two-tier internal grievance mechanism. It allows users to first approach the platform and, within 30 days, escalate unresolved issues to the OGAI. Another remedy might be to appeal to the Appellate Authority in MeitY, which is responsible at various levels. There is proportionality in penalties and actions taken to enforce.

The Authority must consider factors such as the seriousness of the violation, the harm inflicted on users, and, indeed, whether the lack of compliance is repeated or deliberate.

Taken together, the Rules narrow the field but clarify the path ahead. Money based gaming is firmly off the table.

E sports and social games, by contrast, now have a single, central framework to operate within. For developers, platforms, payment players, and advertisers, this is the moment to stop, reassess, and redesign. The uncertainty has not disappeared, but for the first time in years, the rules of the game are at least visible. 🍀

The author is a Partner and National Media and Entertainment Industry Leader at Grant Thornton Bharat.

feedbackvnd@cybermedia.co.in



Pixxel plans orbital data centre satellite with Sarvam

The satellite, Pathfinder, will process AI and hyperspectral data in space, reducing delays and reliance on the ground.

Bengaluru-based space technology company Pixxel has partnered with AI firm Sarvam to develop India's first orbital data centre satellite, named Pathfinder, with launch targeted for the fourth quarter of 2026.

Under the partnership, Pixxel will design, build, launch, and operate the 200 kg-class satellite, while Sarvam will provide the AI infrastructure and onboard language models required for real-time data processing in space.

Unlike conventional satellites that depend on low-power edge processors and ground stations for computation, Pathfinder will carry data centre-class

GPUs capable of running AI workloads directly in orbit. The satellite will also host Pixxel's hyperspectral imaging camera, enabling onboard analysis of high-resolution Earth observation data.

The companies said the mission aims to process and analyse data in space rather than transmitting large volumes of raw imagery back to Earth. The approach is expected to reduce latency and improve response times for applications such as climate monitoring, resource management, defence, and infrastructure tracking.

The project is also intended to support India's sovereign AI ambitions by reducing dependence on foreign cloud infrastructure and enabling AI models developed in India to operate entirely onboard an Indian satellite system.

The mission will test AI inference, thermal management, radiation resilience, power systems, and onboard computing performance under operational space conditions. Managing heat dissipation and maintaining stable power during orbital eclipses remain among the technical challenges for space-based data processing systems.

The satellite will be developed at Pixxel's upcoming Gigapixxel manufacturing facility, which is designed to support production of up to 100 satellites.



Find more smiles at NormanAndOzi.com



Find more smiles at NormanAndOzi.com

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 PROGRAMMES 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 Programmes

High-Impact Verticals We Specialise 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

Partnerships & Advertising Enquiries

Ajay Dhoundiyal – Marketing Alliances & Business Solutions : ✉ ajaydh@cybermedia.co.in, ☎ +91-9953540318



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 | Recognised by UGC under 2(f)



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