AI REWIRES SATELLITE NETWORKS—TURNING SIGNAL INTO SENSE | 08

₹100

www.voicendata.com

VOL 32 ISSUE 10 OCTOBER 2025

VOICE & DATA

Connecting the Digital World

CyberMedia

GREEN BY DESIGN

India's telecom industry is moving beyond cosmetic sustainability to embed green design, renewable energy, and AI-driven efficiency into every layer of its networks.

76 pages including cover

Special subscription offer on Page 64

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

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

REGISTRATIONS OPEN 2026

Build a successful career with AIMETC

PROGRAMMES OFFERED

MANAGEMENT

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

COMPUTER APPLICATION

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

ENGINEERING & TECHNOLOGY

4 years/3 years* (*for lateral entry)

- **B.Tech. - Computer Science & Engineering (CSE)**
- **B.Tech. - CSE** (Artificial Intelligence & Machine Learning)
- **B.Tech. - CSE** (Internet of Things & Cyber Security including Block Chain Technology)

SOME OF OUR KEY RECRUITERS

Flipkart, wipro, TCS, BYJU'S, upGrad, amazon, ICICI Bank, zscaler, jaro education, BriskLogic, SBI Life, indiamart, ITC, TOMMY HILFIGER, Berger, orange, EMINENCE TECHNOLOGY, eNest, smartData ENTERPRISES ...and many more

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

VOICE&DATA
CONNECTING THE DIGITAL WORLD

Website: www.voicendata.com

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, Suit 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 Archna Printers, D-127, Okhla Industrial Area, Phase-1, New Delhi 110020. Editor: Shubhendu Parth

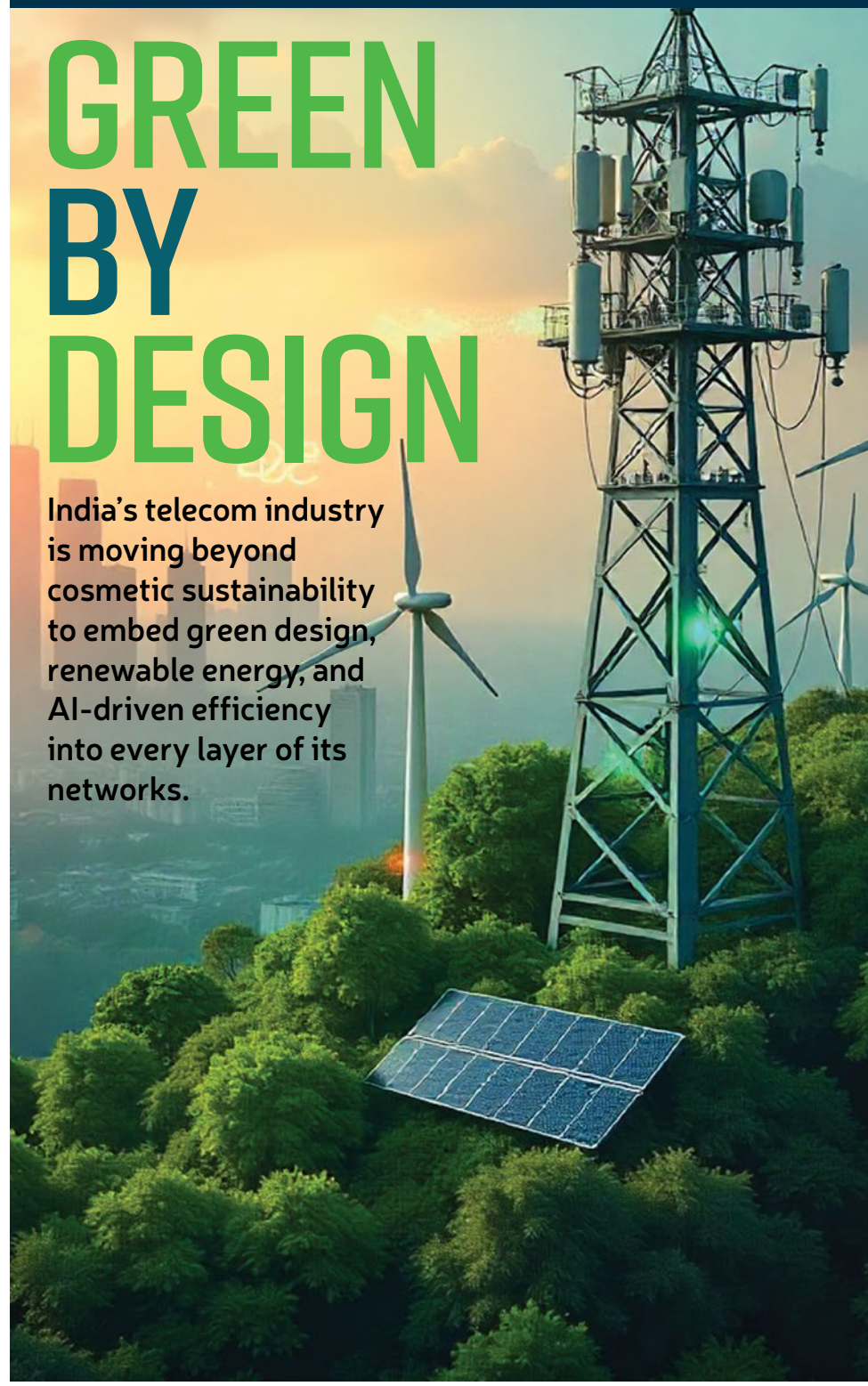
For subscription queries, please email: subscriptions@cybermedia.co.in or send a WhatsApp message to 9289870545.

All Payments Favoring: CYBER MEDIA (INDIA) LTD
Distributors in India: IBH Books & Magazines Dist. Pvt. Ltd, Mumbai.

Corporate Website: www.cybermedia.co.in
www.ciol.com (India's #1 IT Portal)

October 2025

[CONTENTS]



GREEN BY DESIGN

India's telecom industry is moving beyond cosmetic sustainability to embed green design, renewable energy, and AI-driven efficiency into every layer of its networks.

INDUSTRY SPEAK

COMMENTARY

TECHNOLOGY

FOCUS

BROADBAND BYTES

TELECOM TALK

STRATEGY

INTERVIEW

USE CASE

NEWS ANALYSIS

REGULARS

[NEXT ISSUE]

SEPTEMBER 2025

Scan QR Code & Subscribe now...

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

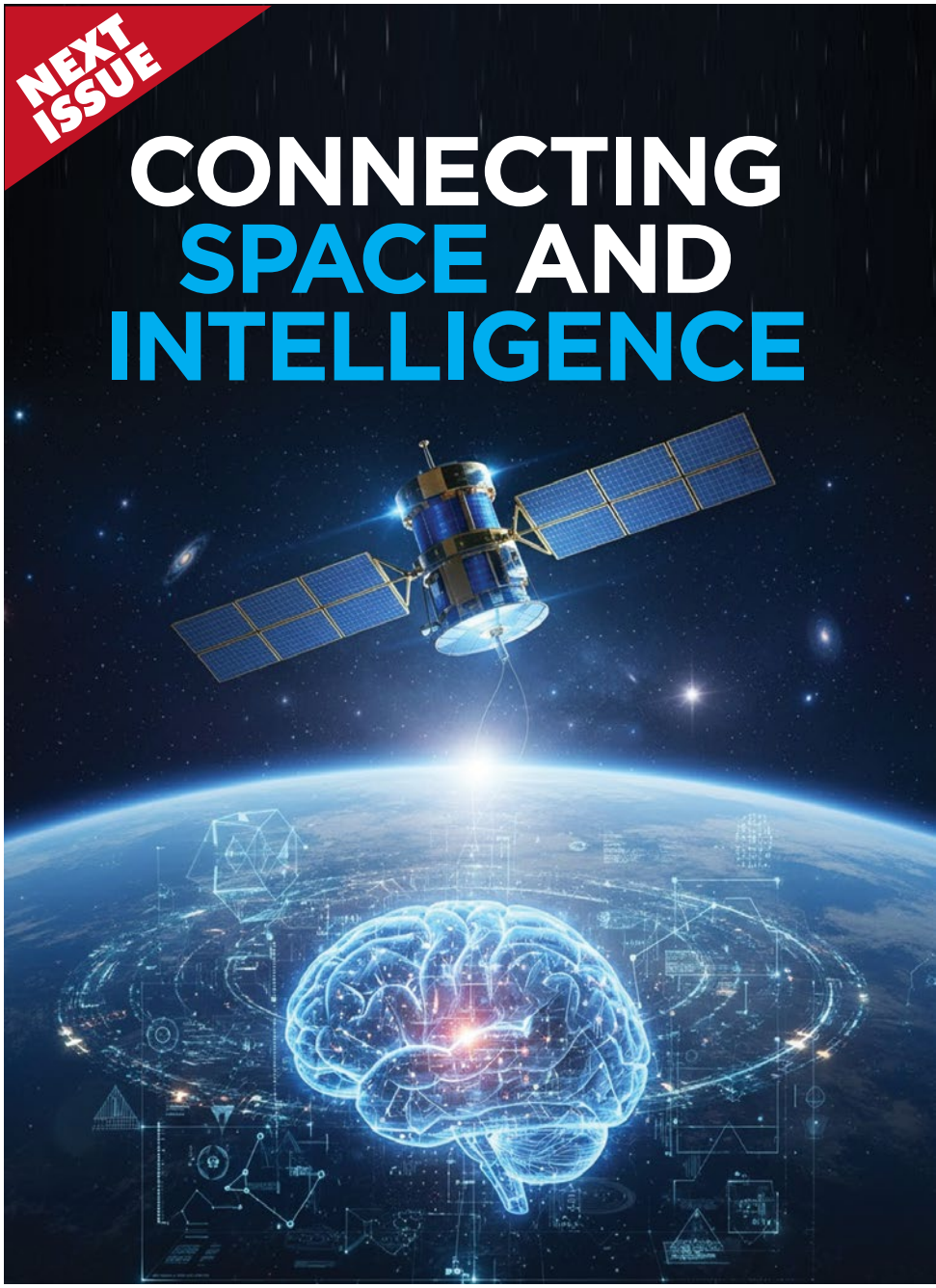
For **subscription queries,** please email: **subscriptions@cybermedia.co.in** or send a WhatsApp message to **9289870545.**

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

mail twitter Linkedin RSS Facebook

FEEDBACK
From Online Readers

Share your views at vndedit@cybermedia.co.in



For any query: ajaydh@cybermedia.co.in

SHUBHENDU
PARTH

[OPENING NOTE]

A2A communication needs a strong trust and control layer

India's AI Mission is progressing at speed—from funding indigenous large language models to rolling out subsidised compute infrastructure. Yet, as the country builds out its foundational AI stack, one critical piece remains underdeveloped: security and trust in Agent-to-Agent (A2A) communication.

Agent-to-Agent communication refers to the structured exchange of information and coordination between AI agents—autonomous software entities that can perceive, reason, and act. These agents, often powered by large language models, are designed to complete complex tasks collaboratively, often with minimal human oversight.

The transformative potential of A2A systems is clear. Agents can divide and conquer problems, automate workflows, and accelerate decision-making. However, this also introduces a new layer of vulnerability. As India scales up AI deployment across sectors—from agriculture to finance—secure, interoperable agentic systems will be essential.

Global developments point to a rapidly maturing A2A ecosystem. In April 2025, Google introduced the A2A protocol, now managed by the Linux Foundation. This protocol defines how agents advertise their capabilities via "Agent Cards", discover one another, and manage task lifecycles. Other protocols, such as IBM's Agent Communication Protocol and Anthropic's Model Context Protocol, have added layers of standardisation to agent interoperability, including access to external APIs and data sources.

Even more experimental approaches, such as Gibberlink—a protocol using data-over-sound for ultra-fast agent interactions—demonstrate the pace of innovation. Open-source multi-agent frameworks such as AutoGen, CrewAI, LangGraph, and Semantic Kernel are enabling developers to build collaborative AI systems that operate with varying levels of autonomy and role specialisation.

Recent announcements at the SAP Connect event in Las Vegas further serve as a case in point. The company introduced more than 40 new AI agents across business functions and previewed support for the A2A protocol within its Joule platform, enabling agents to collaborate across enterprise systems. These agents are designed to automate tasks such as financial reconciliation, supplier bid analysis, and international trade classification—working in coordination to reduce manual effort and accelerate outcomes.

This is not speculative—it is already entering enterprise environments, and India will soon encounter similar architectures across public sector and mission-critical deployments.

However, agentic communication is also a challenge for trust infrastructure. If agents are allowed to issue commands, access sensitive data, or make procurement decisions, how can we verify their identity, authorisation, and intent? What safeguards ensure that adversarial agents do not manipulate interactions or trigger unintended consequences? Who audits inter-agent behaviour?

India's AI Mission already includes a "Safe and Trusted AI" pillar and has taken early steps through the IndiaAI Safety Institute and CERT-In guidelines. But these must now expand to include agent authentication, behavioural auditing, and communication protocol governance. Developing domestic standards for A2A interaction, sandbox testing, and agent certification will be crucial.

Today, A2A communication is more than an engineering advance—it represents the next frontier of trust in AI. If India wants to lead globally in AI deployment, it must focus not only on what AI agents can do, but on ensuring they can be trusted to do it right.

shubhendup@cybermedia.co.in

AI rewires satellite networks—turning signal into sense

AI is transforming satellites from passive relays into intelligent networks that anticipate demand, adapt instantly, and sustain global connectivity.

BY SUBHAS KAMBLE

AI is reshaping how technology functions, and satellite communication (Satcom) is no exception. Once limited to static configurations and scheduled transmissions, Satcom is now evolving into an intelligent, adaptive network that can dynamically respond to real-world needs.

Imagine a scenario in which a major earthquake strikes a remote, mountainous region, completely upending terrestrial communication networks. Cell towers are down, internet cables are severed, and traditional communication methods are rendered unusable.

Yes, you guessed it right: under such conditions, emergency responders will be struggling to coordinate efforts and reach affected areas. It also means that access to reliable communication is paramount for search and rescue operations, medical aid coordination, and the provision of essential information to the affected population.

FROM STATIC LINKS TO INTELLIGENT NETWORKS

Traditional satellite systems offer rudimentary connectivity but often struggle with dynamic demand spikes, the need to optimise bandwidth in congested areas, and the challenge of providing seamless service to mobile units such as rescue vehicles and drones.

This is where AI-enabled satellites make the difference. They transform satellite communication from infrastructure into an intelligent, adaptive network that can dynamically respond to real-world crises, ensuring critical, high-quality, and ubiquitous connectivity even when terrestrial networks fail.

> By merging AI with Satcom, communication shifts from reactive to predictive—networks that sense, learn, and self-heal are now redefining connectivity.

What this means is that, as soon as disaster strikes, AI-driven low-earth-orbit (LEO) constellations detect spikes in communication demand from emergency responder terminals and affected communities. Reacting immediately, algorithms onboard the satellites or in intelligent ground stations dynamically reconfigure their beams through adaptive beamforming. Instead of fixed wide beams, AI directs narrower, more powerful ones to the affected zone, concentrating bandwidth where it is most needed.

The result is instant, allowing rescue teams to access high-bandwidth connectivity for video calls, data transfer, and drone feeds immediately—even in areas without terrestrial support infrastructure.

AI-DRIVEN PRECISION DURING EMERGENCIES

Within the disaster zone, interference and terrain variation affect signal quality. AI-powered Adaptive Coding and Modulation (ACM) continuously monitors channel conditions and adjusts transmission parameters in real time. If signal quality drops, it switches to a more robust coding scheme to maintain reliability; when conditions improve, it shifts back to faster modulation. This automated optimisation ensures that critical communication links remain operational under fluctuating conditions.

As rescue teams move through the terrain, their satellite terminals might switch between different satellites in the constellation or even integrate with any surviving terrestrial hotspots. AI algorithms in the satellite network autonomously manage handovers between satellites and coordinate with ground stations. They predict optimal orbital paths for LEO satellites to maintain continuous coverage and avoid interference.

This provides seamless, "always-on" connectivity for mobile emergency units, ensuring they never lose contact as they navigate the disaster zone and enabling truly ubiquitous communication regardless of location.

SMARTER ARCHITECTURES FOR THE SATCOM WORLD

Behind this intelligence lies the quiet evolution of satellite architecture. Systems have advanced from simple "bent-pipe" relays that merely retransmit signals to "regenerative payloads" capable of processing signals onboard. These modern systems handle error correction, multiplexing, and spatial routing—dramatically improving efficiency and capacity.

AI takes this evolution further by enabling dynamic beamforming, predictive resource allocation, and adaptive modulation that continuously balance performance, power, and bandwidth across the network.

Beyond disaster response, AI is redefining the broader mission of satellite communication. In remote industrial operations—such as offshore rigs or mining sites—it predicts demand surges and allocates resources proactively. In global logistics, it enables real-time tracking and coordination across oceans. And in digital inclusion efforts, it helps bridge the connectivity divide by directing resources to underserved regions, optimising throughput based on usage patterns and population movement.

By learning from environmental data and user behaviour, AI-enabled Satcom networks become not only efficient but perceptive. They can anticipate rather than merely react, self-heal during disruptions, and deliver consistent service quality irrespective of geography. This fusion of machine intelligence with orbital infrastructure marks a pivotal shift—from communication as a passive utility to communication as an intelligent service.

The integration of AI does not simply enhance Satcom—it redefines its purpose. The future of satellite communication will not depend solely on the number of satellites launched, but on how intelligently they collaborate. Networks of autonomous, self-optimising satellites will form a resilient global fabric that ensures the world stays connected when it matters most—whether responding to a humanitarian crisis, enabling industry, or empowering communities in the most isolated corners of the planet.

The author is the AVP and Senior Architect for the Satcom Practice at Sasken Technologies.
feedbackvnd@cybermedia.co.in

Smarter, faster, more human: CX at the edge

Edge-powered CX blends AI speed with human empathy, enabling faster responses, trusted data handling, and deeper customer connections.

BY GURPAL SINGH

Think about the last time you called a service helpline or walked into a store. You probably wanted two things: speed and understanding. A quick resolution matters, but so does the feeling that someone really listened to you. This is where edge-powered customer experience (CX) is starting to change the game—by making interactions faster, smarter, and more human.

Traditionally, most customer data has been sent to faraway data centres for processing. That works, but it often slows things down. Edge computing flips the model by bringing intelligence closer to where the customer is. Data is processed locally, which reduces delays and enables real-time responses.

For a telecom provider handling millions of calls, or a retailer serving customers across cities, these seconds make all the difference. It could mean an instant recommendation, a faster resolution, or simply a smoother experience that feels effortless.

> Edge intelligence provides real-time insights for agents, enabling every customer interaction to be faster, more relevant, and emotionally resonant.

> Trust is strengthened when sensitive data stays local. Edge-powered CX reduces transfer risks while meeting compliance and privacy expectations.

WHERE HUMANS AND AI MEET

There is a lot of excitement about AI in customer service, and rightly so. AI can transcribe calls, analyse tone, and suggest next steps in real time. But no matter how advanced, technology alone cannot replace human empathy. People still want to be heard, reassured, and understood.

This is why the most effective model is a partnership. AI at the edge handles the heavy lifting—sorting data, spotting patterns, and predicting needs—while people bring the empathy and emotional intelligence that no machine can replicate. The result? Service that is both efficient and genuinely human.

Picture a contact centre agent who gets a live prompt that a customer is frustrated. Instead of searching through endless screens, the agent has the right information at hand and can focus fully on the conversation. That is the human-AI balance at work.

RESILIENCE AND AGILITY IN A CHANGING WORLD

Recent years have demonstrated how quickly business conditions can change. Supply chains can be disrupted, call volumes can spike, and customer expectations can shift overnight. Edge-powered CX builds resilience by spreading intelligence across networks.

If one central system faces a disruption, localised processing keeps the customer journey running smoothly. This flexibility also helps organisations scale up quickly, whether it is handling festive shopping surges in e-commerce or sudden spikes in telecom service requests.

TRUST FIRST: SECURING CUSTOMER DATA

In every conversation about technology, trust must come first. Customers today are deeply aware of how their data is used. Edge computing adds a layer of reassurance because it reduces the need to move sensitive information long distances. Processing it locally means greater control, better compliance, and less risk.

For industries such as banking and healthcare, where personal details are highly sensitive, this is a critical advantage. Customers receive personalisation without compromising on privacy.

TURNING SERVICE INTO LASTING LOYALTY

At its heart, customer experience is not about faster systems or smarter analytics—it is about how people feel when they interact with a brand. Do they feel understood? Do they leave the conversation with confidence? Edge-powered CX helps by giving frontline teams the insights they need in the moment.

It could be spotting frustration in a customer's voice before it escalates. Or proactively offering a solution before the customer even notices a problem. These small touches turn transactions into relationships, and relationships into loyalty.

However, the key is that technology can only enable this. The real impact comes from how organisations train, support, and empower their people to use it. Change management, coaching, and a culture that values empathy remain just as important as any tech upgrade.

PREPARING CX FOR AN EDGE-DRIVEN FUTURE

As digital adoption accelerates, edge-powered CX will soon become the standard rather than the exception. Customers will expect not just faster answers, but experiences that feel more personal and more human.

The future of CX is not about choosing between people or technology. It is about how well we bring them together. AI delivers speed, data, and insight. People bring trust, care, and understanding. When the two work in harmony, businesses not only meet expectations but also raise them.

Ultimately, edge-powered CX is about more than just efficiency. It is about building connections that last—one conversation, one interaction, one human moment at a time.

The author is the Global Chief Operating Officer at Startek.
feedbackvnd@cybermedia.co.in

Cyber defence redefined as firewalls give way to foresight

Data security is evolving from reactive protection to predictive foresight—unifying platforms, intelligence, and AI to make organisations breach-ready.

BY DIPESH KAURA

Organisations today expect security teams to achieve the nearly impossible: reduce risk, lower costs, prove the return on investments (ROI), and scale already overextended teams. The demand to do more with fewer resources grows stronger each day. Cybersecurity leaders face the ongoing challenge of demonstrating how risk reduction translates into measurable financial value and converting security investments into tangible business advantages.

In 2025, the global average cost of a data breach was USD 4.4 million, according to research conducted by IBM and the Ponemon Institute. Threats are becoming costlier, and 72% of organisations reported that cyber risks have increased over the past 12 months, according to the World Economic Forum.

Cybersecurity Ventures estimated that the global cost of cybercrime would reach USD 10.5 trillion annually by 2025, and ransomware would cost its victims around USD 265 billion annually by 2031. However, with challenges in quantifying the ROI for cybersecurity solutions, the CISOs are facing a reduction in security budgets. Furthermore, factors contributing to cybersecurity value, such as saved costs from avoiding data breaches, securing customer trust, and brand reputation, are often overlooked.

Today, the question organisations are asking is not whether the attack will occur, but how ready they are when that happens.

The answer lies in organisations shifting toward future-ready security, a strategic approach that enables them to become Breach Ready, Board Ready, and AI-Powered, making cybersecurity measurable and future-proof.

A FUTURE-READY SECURITY PLATFORM?

Cybersecurity technology is evolving. IT environments

> The shift from tools to foresight defines tomorrow's security—where unified, AI-driven defence anticipates threats before they strike.

are becoming increasingly complex, resulting in the generation and consumption of vast volumes of data, while cybercriminals are becoming more sophisticated and creative in their attacks, contributing to the expanding threat landscape. There is a need for a robust cybersecurity strategy that is predictive and dynamic, while being resilient to any changes in the threat landscape and modern SOC.

This is best accomplished with Unified Defence Security Information and Event Management (SIEM) built for the cloud, designed to scale elastically with shifting workloads. By adapting to changes in application and system demands while maintaining consistent detection and response performance, it meets the realities of today's evolving threat landscape.

A modern SIEM should deliver advanced analytics to reduce alert fatigue, provide flexible cloud deployment for future readiness, and integrate intelligence with orchestration and response. The stakes are high, as data breaches result in reputational harm, financial penalties, customer churn, revenue loss, and operational downtime due to ransomware. For the C-Suite, future-ready security is about more than reacting to attacks. It is about anticipating risks and stopping threats before they cause damage.

THREE PILLARS OF FUTURE-READY SECURITY

Today calls for true transformation, one that extends beyond the deployment of cybersecurity tools. With security teams under pressure and attack surfaces expanding, business leaders are asking how security can deliver measurable value across the organisation. To stay ahead, it is critical to focus on the key factors that make security strategies resilient and future-proof.

Breach ready: Traditional security tools and reactive approaches cannot keep pace with today's fast-moving attackers. The most effective strategy is to shift left by unifying SIEM, SOAR (Security Orchestration, Automation, and Response), UEBA (User and Entity Behaviour Analytics), TIP (Threat Intelligence Platform), and TDIR (Threat Detection, Investigation, and Response) in a single cloud platform. This integrated approach delivers faster detection, automated response, and wider coverage across the IT environment.

With unified detection and response, AI-driven anomaly detection enriched with context and pre-built content, and playbooks that streamline workflows, security teams can improve threat hunting, detection, and response while reducing fatigue and accelerating time to action.

Board ready: Cybersecurity has become too critical for business leaders to overlook. It is now a standing topic in the boardroom, with directors demanding clarity on the organisation's security posture. CISOs are not only tasked with reducing risk but also with aligning security to business strategy and defending budgets. To succeed, they need platforms that measure what matters, tie results to ROI, and present clear executive-level dashboards.

By demonstrating measurable outcomes and proven ROI, security shifts from being viewed as a cost centre to a strategic driver of business value. This empowers CISOs to earn board support and secure investments in initiatives that deliver tangible impact.

Agentic-AI power: Rule-based AI solutions fall short in today's rapidly shifting threat landscape because they cannot adapt in real time without constant human input. Agentic AI takes it a step further by combining adaptive learning and independent decision-making with seamless collaboration across the IT environment, all while maintaining human control through a human-in-the-loop approach.

This also reduces noise and false positives, accelerates triage, and enables deeper investigations, driving significant gains in analyst productivity. When embedded into security operations, Agentic AI equips organisations with proactive defence that keeps them ahead of adversaries.

Organisations should adopt a forward-thinking mindset by considering cybersecurity as a journey, not a destination. The commitment they can make to future-ready security is to become Breach Ready, Board Ready, and Agentic AI-Powered.

The author is Country Director for India and SAARC at Securonix.
feedbackvnd@cybermedia.co.in

Connecting the currents of digital finance

India's telcos are building the invisible pipes that keep digital payments, inclusion, and innovation flowing across the nation's financial ecosystem.

BY PRATIMA HARIGUNANI

The word currency must have something to do with current. The value of both water and money lies in how they flow—swiftly, seamlessly, and everywhere. Without motion, both lose their worth. And like water, money needs a sturdy system of wells, tanks, pipes, and taps to do what it is meant to do—flow freely and reach far.

This has never been truer than now, when transactions have shrunk to the swipe and speed of a thumb. The invisible plumbing beneath must work harder than ever to keep pace—and India's telcos are doing precisely that.

TELCOS WRITE INDIA'S NEW DIGITAL BLUEPRINT

Communication costs have dropped by about 33% annually, while processing and storage costs have each fallen around 30%. This has made India one of the most affordable data markets in the world—thanks mainly to the telecom sector's relentless expansion and innovation.

"Telecom networks have driven more than 120% mobile penetration and over 60% smartphone penetration in India," observes Rajashekara V Maiya, VP and Global Head of Business Consulting, Infosys Finacle. "The Jan Dhan initiative has brought over 450 million customers into

"India's open finance initiatives, built on robust telecom infrastructure, have delivered one of the world's largest financial inclusion stories."

RAJASHEKARA V MAIYA
VP & Global Head – Business Consulting, Infosys Finacle

the formal banking system. Meanwhile, the India Stack—with its faceless, paperless, and cashless framework—has catalysed open banking and UPI payments. Add to those initiatives like the Unified Lending Interface (ULI), Open Credit Enablement Network (OCEN), and ONDC, and we are witnessing one of the largest financial inclusion programmes globally—underpinned by telecom and digital infrastructure."

A recent IMF note echoes this view, stating that mobile networks are the backbone of India's digital payments revolution, led by UPI. Shikhar Aggarwal, Chairman, BLS E-Services, reinforces the point: "India has become a global leader in real-time payments, shifting from cash and card to digital-first systems. UPI has made payments quick, secure, and accessible, driving inclusion across individuals and small businesses."

Every tap, transfer, and scan depends on telecom's physical backbone—towers, fibre cables, and data centres. Without the pipes of connectivity, the promise of a cashless economy would remain dry ink on paper.

CONNECTIVITY DRIVES INCLUSION AND INNOVATION

The country's communication backbone has not only powered fintech innovation but also expanded the boundaries of financial access. "India's financial services revolution is being powered by telecom and digital infrastructure," says Anil Chawla, Managing Director, Customer Engagement Solutions, Verint India.

"UPI crossed 14 billion monthly transactions in 2024, and digital lending is projected to reach USD 350 billion by 2030. With 4G, 5G, cloud, and secure connectivity, telcos have become critical enablers of UPI, mobile money, and rural inclusion in partnership with banks, fintechs, and payment players," he added.

Maiya further explains that India's Digital Public Infrastructure model has unlocked "planet-scale

IN BRIEF

- Telecom networks underpin India's financial inclusion, enabling 120% mobile reach, 60% smartphone access, and nationwide seamless UPI adoption.
- UPI crossed 14 billion monthly transactions in 2024, while digital lending is projected to touch USD 350 billion by 2030 on telco-led networks.
- DPI initiatives such as ULI, OCEN, and ONDC demonstrate how open frameworks and telecom connectivity enable inclusive, affordable, and rapid access to credit.
- AI, IoT, and blockchain will transform financial delivery—cutting fraud, personalising services, and boosting real-time intelligence.
- Regulators must balance innovation with stability, ensuring data protection, transparency, and interoperability across digital ecosystems.
- Telcos are evolving into ecosystem partners, powering 5G-enabled banking zones, mobile wallets, and API-based embedded finance platforms.

"Telecom and cloud connectivity are the silent engines behind UPI, mobile money, and digital lending growth across urban and rural India."

ANIL CHAWLA
Managing Director – Customer Engagement Solutions, Verint India

inclusion," with ULI disbursing over USD 5 billion and reaching more than a million clients. "This ecosystem of banks, IT providers, telcos, and startups has helped lift more than 300 million people from below the poverty line to the middle class. All this has been achieved at a fraction of global costs, thanks to real-time, round-the-clock payments and technology-led innovation," he notes.

In rural areas, telecoms' reach has allowed even small merchants to accept QR payments, farmers to receive subsidies directly, and self-help groups to access micro-credit. Fibre connectivity and affordable smartphones have democratised not just communication but opportunity.

BANKING THE UNBANKED THROUGH NETWORKS

The collaboration between telcos and financial institutions has proven vital to expanding reach and redefining customer experience.

Sharing an example, Chawla says, "Bank of Baroda partnered with Tech Mahindra and Verint to transform its contact centre operations using our Quality Bots and Speech Analytics. By automating the evaluation of 100% of customer calls, the bank improved quality scores to 92%, NPS to 50+, sales conversions by 5%, and compliance to 97%."

For Kaushik Chatterjee, Founder and CEO of Lendingplate, the equation is simple: "Compared to limited bank branch coverage, mobile networks reach the remotest regions, offering a broader gateway to financial access. Telecom infrastructure ensures fast authentication, reliable transactions, and shared systems that reduce costs—enabling fintechs to serve rural populations sustainably."

From rural to urban areas, this shift has created an inclusive financial system. Aggarwal adds, "Bank accounts, credit, pensions, and insurance—once a luxury—are now accessible to all. RBI data shows continuous growth in financial literacy and availability of services, enabled by telecom networks and digital infrastructure."

FINTECHS THRIVE ON THE TELECOM BACKBONE

With 4G, the rollout of 5G, affordable smartphones, and API-driven integration, financial services are no longer confined to cities.

"Mobile-first users can now open bank accounts, make UPI payments, apply for loans, and access insurance on their phones," says Chatterjee. "Telecom infrastructure provides the scale, real-time transaction processing, and secure connectivity needed to serve remote districts. It is not just enabling financial services—it is redefining them for a digital-first India."

Aggarwal points out that the collaboration between telcos, banks, and fintechs benefits all parties. "Payment platforms gain from network effects, higher transaction volumes, and data insights to personalise services. APIs allow financial offerings to be embedded into non-financial platforms like e-commerce or social media—creating an interconnected digital economy."

This convergence has blurred industry boundaries. Fintechs today run on telecom bandwidth, while telcos monetise fintech data insights, forming a new cycle of shared growth.

BALANCING REGULATION AND INNOVATION

As this convergence deepens, regulatory frameworks from the RBI, TRAI, and the Data Protection Board become essential to sustain momentum and trust.

"The regulators are ensuring transparency, fairness, and consumer protection," says Chatterjee. "Fintech players welcome these guardrails—they build confidence in the system."

Aggarwal, however, cautions against overregulation: "While minimising systemic risk and ensuring consumer safety is vital, it must not stifle innovation or competition. Regulators need to strike a balance between nurturing creativity and safeguarding stability."

"UPI's success rests on telecom networks that connect millions of users, turning India into a global model for real-time payments."

SHIKHAR AGGARWAL
Chairman, BLS E-Services

Chatterjee adds that interoperability—exemplified by UPI—will be key to the next phase. "Seamless, interoperable frameworks can accelerate digital lending, credit scoring, and cross-platform payments."

Telecom's role in compliance is equally critical. Secure networks, lawful interception systems, and verifiable user identity through KYC ensure that financial data remains protected even as volumes surge.

TECHNOLOGY TRANSFORMS FINANCIAL SERVICES

The entry of emerging technologies such as AI, IoT, and blockchain promises to elevate scale and efficiency—but also introduces new risks.

Maiya notes, "Each new technology amplifies the delivery of financial services by reducing friction. AI and blockchain will cut fraud, improve customer experience, and make transactions faster and cheaper."

Chawla adds, "Customer interactions across mobile, IVR, and digital channels are surging, creating demand for AI-powered chatbots, contextual call routing, and multilingual self-service. At the same time, compliance pressures and fraud risks are rising. For telcos and BFSI firms alike, Customer Experience (CX) is the new frontier—but legacy systems struggle to keep up with its scale and speed."

Aggarwal highlights a recent milestone, "The RBI's Framework for Responsible and Ethical Enablement of Artificial Intelligence introduces seven guiding principles—the Seven Sutras—for the governance, development, and deployment of AI in finance. As fintech expands, the credibility and ethics of AI-driven systems will be under sharper focus."

Blockchain-based smart contracts, predictive analytics for credit scoring, and IoT-enabled asset monitoring are already reshaping how loans, insurance, and payments operate. As data volumes multiply, telecom's low-latency networks and edge computing nodes will be indispensable for real-time financial intelligence.

THE RISE OF TELCO-FINTECH PARTNERSHIPS

India's telcos are no longer mere connectivity providers—they have evolved into integral ecosystem partners. By collaborating with banks and fintechs, they now power mobile wallets, UPI-linked services, and digital lending products that reach deep into Tier-3 and Tier-4 markets.

"As India races towards 2030, it is expected to rank third globally in digitalisation, with the digital economy contributing nearly one-fifth of GDP," notes Aggarwal. "In 2022–23, digital infrastructure, AI, and cloud computing contributed 11.74% to national income—a figure expected to rise to 13.42% by 2024–25. These achievements reflect India's progress towards inclusive, technology-driven growth."

The next stage will demand deeper cross-industry interoperability. Fintech APIs that talk directly to telco billing systems and 5G slicing for secure banking zones could redefine the digital finance experience. For consumers, that means frictionless services; for telcos, new revenue models built on trust.

KEEPING THE CURRENT FLOWING

As India's financial ecosystem continues to expand, telcos will find themselves forging deeper alliances—be it with banks, fintechs, or government platforms. They are the arteries carrying the lifeblood of the digital economy. Trust, reliability, and resilience will decide how far the current flows. As infrastructure becomes smarter and transactions more invisible, the need for continuous security, redundancy, and collaboration will intensify.

If the flow continues unimpeded—without leaks, bottlenecks, or barriers—finance may soon evolve into what we imagine it to be: not bottled water, but a freely flowing current, accessible to all.

pratimah@cybermedia.co.in

TV RAMACHANDRAN

WHEN EVERY SECOND COUNTS, INDIA'S MISSION NETWORK

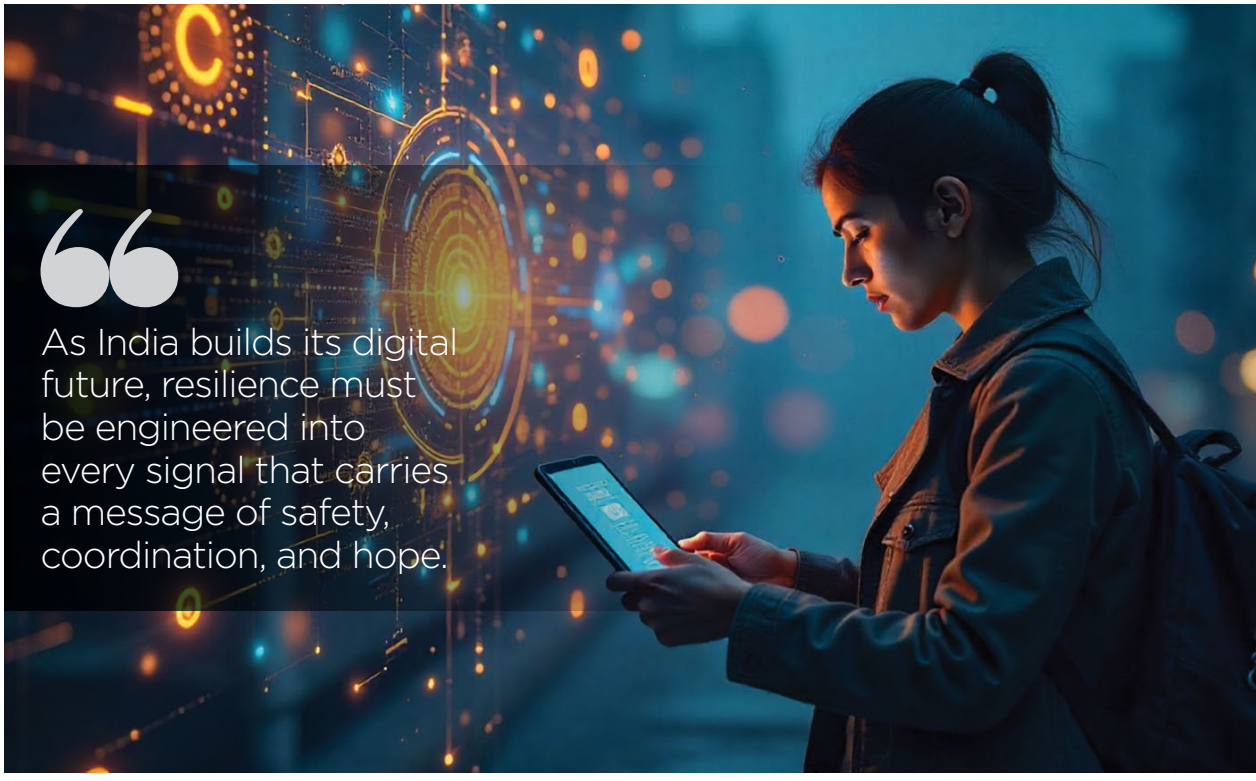
When disasters strike and seconds decide outcomes, India's mission-critical communications network keeps responders connected and lives protected.

In today's lightning-paced, hyperconnected, and increasingly VUCA—volatile, uncertain, complex, and ambiguous—world, instant communication is often taken for granted. We stream videos, send messages, and make calls with ease, rarely pausing to consider the intricate web of systems that keeps us connected. Yet behind this seamless convenience lies a different universe—the world of critical communications (CC).

It is a world where every second counts, and where a missed signal or a failed connection can have catastrophic consequences. Critical communications networks operate quietly in the background, ensuring that the nation's emergency responders, defence forces, disaster management teams, police, and railways remain connected when all else fails. These systems form the invisible backbone of public safety and national resilience, providing a secure communication lifeline in moments of chaos and uncertainty.

LESSONS FROM DISASTER MANAGEMENT

Few citizens realise the extent of India's progress in



> Every message that saves a life in India's disaster zones is powered by unseen, critical communication systems that connect first responders.

building such networks. The Balasore rail tragedy, for instance, demonstrated how effectively police and railway communication systems could coordinate rescue and recovery efforts amid overwhelming challenges.

The evolution of critical communications can perhaps best be seen by comparing two major cyclones that hit India decades apart. In 1999, when the Paradeep cyclone struck Odisha, the country lost over 12,000 lives. At the time, disaster communication systems were limited and fragmented, with alerts slow to reach vulnerable populations. In contrast, in 2023, an equally intense Cyclone Biparjoy struck Gujarat—yet not a single casualty was recorded.

This extraordinary achievement was possible because of the systems painstakingly built by the Department of Telecommunications (DoT) and the Centre for Development of Telematics (C-DoT). Over 32 million early warning messages were sent via the Common Alerting Protocol (CAP) network, enabling mass evacuations and real-time coordination among agencies. The technology worked exactly as intended—proving that timely, reliable communication can save lives on an unprecedented scale.

These lessons reaffirm that in preparing for uncertainty and disasters, communication is not just a tool—it is a weapon of protection. Investing in interoperable and resilient communication systems must therefore remain a national priority. During crises, authorities cannot rely solely on commercial mobile networks, which are vulnerable to overload, or on outdated Professional Mobile Radio systems that lack interoperability and broadband capabilities. Modern critical communications systems based on broadband infrastructure are essential to enable Public Protection and Disaster Relief (PPDR) and to safeguard critical national infrastructure.

CRITICAL NETWORKS VS. PUBLIC SYSTEMS

At its core, a critical communications network is built to serve when everything else collapses. It is engineered for reliability, resilience, availability, and security, ensuring that the correct information reaches the right people at the right time. These systems are indispensable across domains—public safety, emergency response, transport, utilities, healthcare, and even smart cities.

Commercial networks, by contrast, are designed for mass convenience rather than mission-critical reliability. In any large-scale emergency, the public instinctively reaches for their phones—checking on family, streaming live news, or posting on social media. As millions attempt to connect simultaneously, commercial systems get congested. In such a scenario, if first responders used the same networks, they would face the same delays as everyone else.

Critical communications networks eliminate this risk. They prioritise emergency traffic, offering guaranteed connectivity and redundant architecture that prevents failures. Dedicated infrastructure ensures durability, while specialised features like push-to-talk enable instant coordination across teams. In disaster zones, these capabilities can mean the difference between order and chaos.

The importance of critical communications extends to national defence as well. In modern warfare, data is the new ammunition. With operations now spanning land, air, sea, space, and cyber domains, armed forces depend on real-time information sharing to outmanoeuvre adversaries. Cloud technologies are indispensable for fusing distributed data from multiple sensors and for enabling shared computation and storage at scale. Meanwhile, satellite communications ensure long-range connectivity even when terrestrial networks are disrupted, shortening decision-making cycles to seconds and providing a critical tactical edge.

Reinforcing this view, TRAI Chairman Anil Kumar Lahoti highlighted at India's first national conference on critical communications that the subject carries "immense strategic importance for both India and the global community" amid climate vulnerabilities, urban communication challenges, and evolving security threats. His message was clear: the ability to communicate reliably during crises defines a nation's preparedness.

As disasters grow in frequency, India's hybrid broadband alert systems like Sachet are transforming how warnings reach citizens in seconds.

INDIA'S CRITICAL COMMUNICATION BACKBONE

India's journey to strengthen critical communications systems rests on four foundational pillars—infrastructure, policy, spectrum, and standards—each evolving rapidly. For decades, emergency services relied on narrowband technologies such as TETRA and P25 for secure voice connectivity. However, as the need for high-speed data and multimedia communication grew, India began transitioning toward hybrid models that integrate TETRA with 4G/5G broadband (MCX) for video, data, and advanced situational awareness.

This hybrid integration is guided by the Interworking Function, a key enabler that enables seamless communication between Land Mobile Radio or LMR systems and next-generation broadband networks. The DoT, working closely with the National Disaster Management Authority, has expanded mobile-enabled disaster communications nationwide.

One of the most notable initiatives is Sachet, an integrated alert system developed by C-DoT using ITU's CAP standard. It delivers real-time, geo-targeted warnings to citizens via SMS—already covering the entire country. This early warning infrastructure has been credited with saving lives during cyclones, floods, and other natural disasters.

Policy developments have kept pace. Recommendations for critical communications now include assigning exclusive spectrum—10 MHz in the 700 MHz band for LTE-based disaster management networks to enhance railway passenger safety, and another 10 MHz in the 800 MHz band for a nationwide PPDR network. Avoiding silos and ensuring interoperability through open standards are key to maximising the effectiveness of these systems.

Globally, India is not alone in strengthening its critical communications capabilities. The mission-critical communications market is projected to grow from USD 20.9 billion in 2025 to USD 31.1 billion in 2029, at a CAGR of 10.4%, according to The Business Research Company. South Korea pioneered the world's first public safety broadband network, PS-LTE, operational since 2018. Belgium is following suit with a nationwide broadband MC rollout by 2025, while Dubai's Nedaa has developed a secure government broadband network dedicated entirely to professional communications.

These international examples illustrate how nations are prioritising resilient communication as a foundation for safety, governance, and security—an approach India is now accelerating with its own ecosystem of public and private stakeholders.

WARRIORS OF MISSION-CRITICAL COMMUNICATIONS

In an age when uncertainty is constant and every second matters, secure and interoperable communication systems are no longer a luxury—they are a necessity. India's next leap must focus on creating a holistic ecosystem that blends policy foresight, spectrum availability, indigenous R&D, and public-private collaboration.

Building critical communications networks faster and smarter requires dedicated resources and recognition. The policy imperative is clear: ensure dedicated spectrum, promote open standards, certify interoperable devices, and encourage cross-agency collaboration. These steps will make India's critical communications infrastructure more agile, resilient, and future-ready.

As retired Lt Gen Syed Ata Hasnain observed, the silent warriors behind mission-critical communications—engineers, technicians, and planners—rarely receive the recognition they deserve. Their work ensures that when calamity strikes, alerts reach millions, emergency teams stay connected, and the nation's response machinery operates with precision. India owes its safety and stability to these unseen protectors—the guardians of the nation's most vital yet invisible network: its critical communications lifeline.

TThe author is an Hon. FIET (London) and the President of the Broadband India Forum.

Views are personal.

(Research inputs from Garima Kapoor)

feedbackvnd@cybermedia.co.in

7th edition

VOICE&DATA 31 YEARS

CyberMedia

TELECOM LEADERSHIP FORUM

5G+

EMPOWERING INDIA WITH 5G+

A NEW DIRECTION FOR DIGITAL INFRASTRUCTURE

November 2025 | New Delhi

As India moves toward its Vision 2047, technologies such as 5G, AI, IoT, edge computing, and cybersecurity are transforming industries, governance, and innovation. The Voice&Data 5G+ Summit 2025 brings together key visionaries to shape the roadmap for a connected, secure, and future-ready digital infrastructure — paving the way from 5G to 6G.

PARTNER WITH PURPOSE

- **Strategic Brand Positioning:** Establish your leadership in India's 5G+ and 6G ecosystem.
- **Exclusive CXO Access:** Engage 150+ pre-qualified policymakers, enterprise leaders, and decision-makers.
- **Showcase Innovation:** Highlight your solutions, use cases, and thought leadership to an elite audience.
- **Amplified Visibility:** Across Voice&Data, Dataquest, PCQuest, social, digital, and on-ground platforms.
- **Business Acceleration:** Lead generation, partnerships, and solution demonstrations.

SUMMIT HIGHLIGHTS

- **CXO Insights:** CEOs, CTOs, CISOs, and senior IT leaders from telcos, BFSI, healthcare, manufacturing, and utilities
- **Focused Tracks:** Private 5G ROI, enterprise transformation, deep-tech innovation, India's 6G roadmap
- **Innovation Showcase:** Startups and Make-in-India digital infra solutions
- **High-Level Policy Dialogues:** DoT, MeitY, TRAI, and state IT leaders

Shape India's Digital Future – Showcase Your Brand as a Pioneer in Building Viksit Bharat 2047.

Connect with us to explore tailored sponsorship opportunities.

For further information, please contact

Ajay Dhoundiyal, Marketing & Sales: Email: ajaydh@cybermedia.co.in | Phone: +91 99535 40318

GREEN BY DESIGN

India's telecom industry is moving beyond cosmetic sustainability to embed green design, renewable energy, and AI-driven efficiency into every layer of its networks.

BY PRATIMA HARIGUNANI

The problem with wallpapers is that they rarely last long. They fade, peel, or lose their grip. No matter how deftly they are pasted, they remain just that—pasted. Sooner or later, the illusion cracks, revealing that the green branches beneath are not real.

The same holds true when sustainability is applied like wallpaper—an afterthought or a quick cosmetic fix—on today's massive, consequential, and ever-expanding digital infrastructures. The scale, complexity, and permanence of the carbon emissions generated by these digital turbines are staggering.

Every call made, every AI query typed, every reel scrolled through, every virtual meeting joined, and every OTT episode watched adds another layer of soot and guilt to the machines that power the connected world. And the picture is only getting murkier as 5G and 6G rollouts accelerate and artificial intelligence enters the scene with a loud, relentless drumroll.

HOW BLACK ARE OUR DIGITAL BACKYARDS?

A closer look at the data reveals a sobering reality.

A 2025 telecom consumer survey by McKinsey—conducted with 5,000 participants across five countries—found that 45% of retail customers value sustainability in their telecom providers. Yet, the telecom sector continues to lag behind others on several critical sustainability governance parameters, according to McKinsey's benchmark of the Environmental, Social, and Governance (ESG) performance of 75 large global companies across sectors.

To trace this carbon trail, one must examine the multiple layers at which any telecom player impacts the environment. Scope 1 emissions cover direct impact areas such as vehicles and generators. Scope 2 emissions occur further along this chain and relate to how telecom companies power their fixed and mobile networks and data centres. Scope 3 emissions, meanwhile, extend across the entire ecosystem—encompassing the

> Telecom's carbon story runs deeper than towers and cables—it stretches across data, devices, and the invisible grid that powers digital life.

"Diesel gensets will remain vital for uptime, but greener pathways like solar-hybrid grids are already redefining backup power."

JAMESON MENDONCA
Power Generation Business Leader, Cummins Power System

IN BRIEF

- Telecom's sustainability gap remains wide even as 45% of consumers value green practices from their connectivity providers.
- Scope 3 emissions account for 81% of the industry's footprint, yet few operators disclose them or take steps to reduce them.
- Design-led transformation—fibre-first rollouts, AI energy optimisation, and network sharing—drives measurable decarbonisation.
- Renewable-powered data centres, circular hardware reuse, and hybrid energy solutions can reduce carbon intensity at scale.
- Regulatory pushes like India's ESG rules and the EU's CSRD are accelerating greener practices and transparency.
- Green electricity and smarter design could together slash telecom emissions by more than half within this decade.

activities of partners, suppliers, and third parties, as well as the use and disposal of customer equipment and supply-chain components.

The 2025 Carbon Action Report by EcoVadis and BCG revealed that Scope 3 emissions are 21 times larger than Scopes 1 and 2 combined, yet only 24% of companies report on them, and a mere 8% have set reduction targets.

According to a 2024 report by the International Telecommunication Union (ITU) and the World Benchmarking Alliance (WBA), 148 of the 200 companies surveyed reported electricity consumption totalling 518 terawatt-hours (TWh) in 2022—about 1.9% of the world's total.

The report also highlighted that Scope 3 emissions—spanning material suppliers, outsourced device production, and the use of end products—are, on average, six times higher than the combined Scope 1 and Scope 2 emissions. Companies continue to struggle with this due to limited supplier data, double-counting, and inconsistent application of emission-allocation principles.

Data from the ITU further shows that in 2023, greenhouse gas emissions reported by 166 digital companies accounted for 0.8% of all global energy-related emissions. Electricity consumption by data centres—which power AI development and deployment—has been rising by 12% annually from 2017 to 2023, four times faster than global electricity growth. The ITU also reported that annual e-waste generation is increasing by 2.6 million tonnes per year and is projected to reach 82 million tonnes by 2030.

As of FY2025, 77.7% of India's electricity is sourced from renewables, and the country's emissions intensity (CO_2e/Revenue) has reduced by over 80% since 2008, observes Guruprakash Sastry, Associate Vice President and Head – Climate Action at Infosys. "With rapid urbanisation and industrialisation bringing stress on resources, it is important to minimise impact from buildings and related infrastructure," he adds.

"AI can be one of the most powerful enablers of climate goals by analysing complex data and driving smarter, real-time decisions."

GURUPRAKASH SASTRY
Associate Vice President, Head – Climate Action at Infosys

Jameson Mendonca, Power Generation Business Leader at Cummins Power System, notes that under realistic scenarios, AI workloads alone could require 1–1.5 GW of continuous IT power—equivalent to 8.8–13 TWh annually—in India by 2030. "This translates into a significant new draw on grids, water resources, and capital expenditure for cooling and power infrastructure," he explains. "Recent analyses suggest that while AI's share of data centre power today remains in the single-digit to low-teens range, it could climb to 20–40% by 2030, fundamentally reshaping the power-consumption profile of digital infrastructure."

According to Arvind Khurana, Regional VP and Country Head for Cloud and Network Services at Nokia India, telecom networks today account for a substantial share of global energy consumption and carbon emissions, particularly as 5G densifies networks and data traffic continues to soar.

SCOPE 3: THE TOUGHEST NUT TO CRACK

The telecom industry accounts for a significant share of global greenhouse gas emissions, roughly 3–4% of the total. According to BCG's Telco Sustainability Index 2024, key categories such as commitment to sustainability, emissions and energy management, and customer enablement either showed no improvement or declined.

The study also noted that in the area of biodiversity, telecom operators are only beginning to recognise their potential impact. Alarmingly, the proportion of companies setting emission-reduction targets dropped by four percentage points.

Scope 3 emissions account for 81% of the industry's total. The index found that only a few telecom players have managed to reduce these emissions, largely due to weak reporting on leased upstream and downstream assets. Even companies with net-zero commitments often lack comprehensive long-term roadmaps and measurable interim milestones. Many remain entangled in the complexities of vast, global supply chains—not only in devices but also in networking equipment.

"Scope 3 is the toughest challenge," explains Jaspreet Singh, Partner and Chief Revenue Officer – Consulting, Grant Thornton Bharat. "Over 70% of a telco's emissions come from its supply chain—chipsets, device manufacturing, tower equipment, and logistics. Unlike Scope 1 (direct) or Scope 2 (purchased energy) emissions, Scope 3 requires alignment with vendors across continents. It is difficult because telcos do not control their supply chains end-to-end, yet regulators and stakeholders are increasingly demanding disclosure."

Mendonca adds that Scope 1 and Scope 2 emissions for data centres are expected to rise in the short term. "Hence, there is a huge focus on reducing the carbon footprint of these categories through the use of renewable energy and hybrid solutions," he notes.

The challenge extends beyond telecom operators to their vendors. The Telco Vendor Sustainability Analysis Report 2025 by ResearchandMarkets estimated that total emissions (Scope 1 + Scope 2 market-based + Scope 3, or "S1–3m") for vendors reached 481 million metric tonnes of CO_2-equivalent in 2023, while S1–3m emissions stood at 254.7 metric tonnes per USD 1 million in revenue, down from 271.9 in 2022. The scenario is expected to become even more complex as AI advances. OpenAI, for instance, has plans for data centres valued at nearly USD 850 billion, while HSBC analysts forecast that global AI infrastructure investment could reach USD 2 trillion.

Amid this growing challenge, many telecom companies have yet to grasp or disclose the scale of their climate impact fully. The 2024 EY Climate Action Disclosure Barometer found that the quality of climate-related disclosures by telcos and technology firms stands at just 55%—well below the 94% coverage benchmark. Only 36% reference climate-related issues in their financial statements, and just 51% currently disclose transition plans for adopting renewable energy.

"Networks themselves must become inherently greener, with AI and automation reducing radio emissions without losing quality."

ARVIND KHURANA
Regional VP & Country Head for Cloud and Network Services at Nokia India

FLIPPING THE DIP WITH DESIGN THINKING

The answer, unsurprisingly, lies in scraping off the wallpaper and doing some deep, structural cleaning—followed by genuine renovation. Not the kind that involves dusting carpets or hanging new curtains, but a fundamental rethinking of networks, infrastructure, and operations at the design level.

A fundamental transformation begins when sustainability moves from an aesthetic upgrade to an architectural principle. Carbon consciousness must seep into the blueprint of how networks are conceived, built, and operated. Telcos can begin by implementing software-driven network reconfigurations to enable remote monitoring, management, and equipment upgrades—minimising travel, downtime, and energy use.

Another promising step is network sharing. As McKinsey observed, infrastructure sharing can reduce total emissions by up to 10 per cent, primarily from Scope 3, while cutting material consumption by over 30 per cent—without compromising network quality.

Design-level thinking also means choosing low-emission materials for constructing towers, devices, and network equipment, and embedding circular-economy principles at every stage of product and infrastructure life cycles.

"Design thinking can embed sustainability at every stage," affirms Singh. "At the network-planning stage, this means prioritising fibre over copper and reducing tower duplication through infrastructure sharing. In hardware manufacturing, it involves using eco-friendly materials and modular designs that extend equipment life. In software and energy management, AI/ML-led traffic routing can optimise power use and reduce idle energy consumption. This approach turns sustainability from an afterthought into a core design principle."

Singh cites real-world examples: Bharti Airtel's 'Green Towers' project, which reduces diesel dependence through hybrid solutions; Vodafone Group's circular economy model for network hardware reuse; and NTT Japan's use of AI to optimise energy consumption across its networks.

Khurana adds: "From energy-efficient chipsets to AI/ML-driven software, we are working to ensure that networks themselves become inherently greener. With our AI/ML-based Energy Efficiency solution, part of our Autonomous Networks portfolio, we are helping telecom operators cut Radio Access Network emissions by automating idle-equipment shutdowns and optimising radio transmission power—all while maintaining service quality. These coordinated efforts across hardware, software, and infrastructure can deliver significant environmental gains."

Sastry takes a broader view of AI's role: "AI can be one of the most powerful enablers of positive climate goals, as it can analyse vast datasets, optimise systems in real time, and drive smarter decisions."

Mendonca believes that diesel gensets will remain indispensable as reliable backup systems to meet rising power demands and ensure uninterrupted uptime. "At the same time," he adds, "global forums are actively pursuing greener pathways, with data centres worldwide exploring solar integration, renewable-backed grids, and hybrid solutions as part of their sustainability roadmaps. India's data centre sector is at a defining inflexion point—balancing the need for resilient backup power with the responsibility to advance toward greener, more sustainable energy in the age of AI."

Mendonca notes that Cummins is already helping data centre customers transition to cleaner alternatives—supporting the use of alternative fuels, optimising engines to minimise NOx formation, and deploying scrubbers, filters, and other after-treatment systems to further reduce emissions.

FROM GREY TO GREEN TO GREENER

All is not dull in the telco green war rooms. McKinsey

"Over 70% of a telco's emissions come from its supply chain—chipsets, devices, and logistics that operators can't fully control."

JASPREET SINGH
Partner and Chief Revenue Officer – Consulting, Grant Thornton Bharat

estimates that nearly 60% of an integrated operator's emissions can be reduced for less than USD 100 per metric tonne of CO_2. Up to 15% of decarbonisation measures could even generate cost savings exceeding the initial investment. In fact, the study found that half of all emissions can be cut by using green electricity to power networks, data centres, and the upstream supply chain.

The report, Greening Digital Companies 2025, by the ITU and WBA, reinforces this optimism. Of the 200 digital companies studied, 23 operated on 100% renewable energy in 2023, up from 16 in 2022. Moreover, 49 companies released standalone climate reports, signalling greater transparency and accountability. Even in the complex domain of Scope 3, progress was visible: the number of companies publishing targets for indirect emissions from supply chains and product use rose from 73 to 110.

So, can telecom industry players go green in a scalable, pragmatic, and effective way?

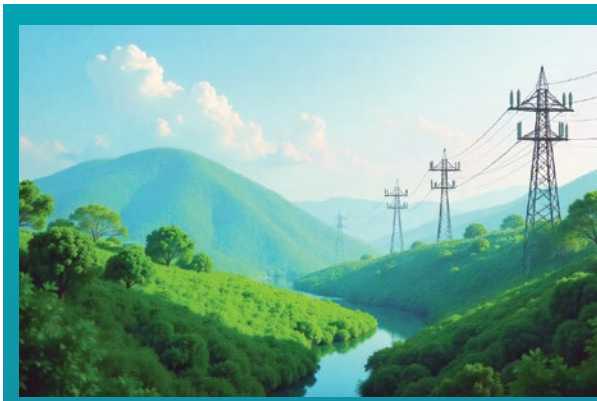
"Yes, but the journey is complex," responds Singh. "Telcos operate largely on legacy infrastructure—copper networks, diesel-powered towers, and ageing switching systems—all of which inherently carry higher carbon footprints. Transitioning to greener operations demands a phased shift: modernising networks, decommissioning legacy assets, and embedding renewable energy into everyday operations." Pragmatism, Singh notes, lies in scalable interventions—energy-efficient base stations, network sharing, and fibre-first rollouts—rather than expecting overnight transformation.

Emerging advances are already showing promise. Fibre-first deployments, energy-efficient 5G and 6G architectures, AI-powered network optimisation, renewable-powered data centres, and innovations in passive infrastructure collectively point toward a future of faster and cleaner connectivity. Singh explains, "Fibre-first deployments can cut energy use by up to 70%

ENGINEERING NET-ZERO INFRA

- **Cut direct emissions:** Streamline operations to reduce Scope 1 and 2 impacts through efficient assets and low-carbon maintenance.
- **Target Scope 3 hotspots:** Address emissions from handsets, network gear, and construction through sustainable sourcing and reuse.
- **Accelerate energy transition:** Shift grids and networks to renewables via PPAs, RECs, and on-site generation with storage support.
- **Optimise infrastructure:** Deploy RAN centralisation, dynamic power management, and AI-driven data-centre optimisation for measurable savings.
- **Adopt green materials:** Use green steel, scrap-based steel, Direct-Reduced Iron, and green hydrogen in construction and manufacturing.
- **Advance circular supply chains:** Strengthen supplier standards on recycling, waste reduction, and sustainable manufacturing.
- **Ensure carbon transparency:** Standardise measurement, reporting, and verification across partners for credible climate disclosures.

As AI workloads surge, power demand could reshape networks, making sustainability both a moral imperative and an engineering challenge.



DESIGNING SUSTAINABLE NETWORKS

- **Design for sustainability:** Embed carbon-smart planning from site layout and materials to software and power optimisation.
- **Go fibre-first:** Replace copper with fibre to cut energy use by up to 70 per cent and improve efficiency.
- **Share smarter:** Expand network- and tower-sharing to cut Scope 3 emissions and material use without hurting quality.
- **Power green:** Run data centres and RAN sites on renewable-backed or hybrid grids with solar-integrated edge networks.
- **Optimise with AI:** Use AI/ML for predictive load balancing, automated shutdowns, and real-time traffic control.
- **Close the loop:** Reuse, refurbish, and recycle network hardware to extend asset life and minimise waste.
- **Audit and act:** Employ carbon accounting, digital twins, and lifecycle assessments for data-driven decision-making.
- **Collaborate for impact:** Work with industry alliances and policymakers to scale interoperable, low-carbon network standards.

compared to copper. Newer 5G and 6G standards are 10 times more energy-efficient per bit, while AI-driven optimisation using predictive load balancing significantly reduces energy waste. Renewable-powered data centres with solar-backed edge sites and green cooling systems also reduce duplication and emissions."

Mendonca adds that as data centres grow in scale, sustainability is emerging as a key competitive differentiator. "This is where Life Cycle Assessments and Environmental Product Declarations become vital," he says. "For a data centre, this spans both upstream, or embodied impacts—such as construction materials, IT equipment manufacturing, and cooling and power infrastructure—as well as operational impacts like electricity consumption."

Carbon auditing tools now offer deeper visibility, while digital twins and simulations help telcos model greener network configurations before rollout. These tools enable data-driven decision-making—for example, simulating the emission impact of diesel versus solar energy mixes for towers. Compliance is not merely a nudge but a catalyst, Singh observes: "Regulatory pushes like India's ESG disclosure framework or the EU's Corporate Sustainability Reporting Directive compel telcos to act faster. Beyond compliance, early movers gain investor confidence and brand advantage in an ESG-conscious market."

Ultimately, green consciousness is no longer a nice-to-have accessory—it is a strategic necessity. Sustainability by design marks a pivotal shift for the industry. As the 2025 Carbon Action Report by EcoVadis and BCG cautions, neglecting supply chain emissions (Scope 3) could cost companies over USD 500 billion annually in global liabilities by 2030. Yet the same report offers hope: investing in climate action for supply chains today can deliver a three- to sixfold return through avoided regulatory costs and operational efficiencies.

Unless it is O Henry's The Last Leaf, it is far better to grow a real leaf than to paint one. Last or first, on a corporate sustainability report or a balance sheet, a green leaf always brings hope.

pratimah@cybermedia.co.in

LT GEN DR SP KOCHHAR

INDIA'S SPECTRUM RETHINK: UNLOCKING THE DIGITAL FUTURE

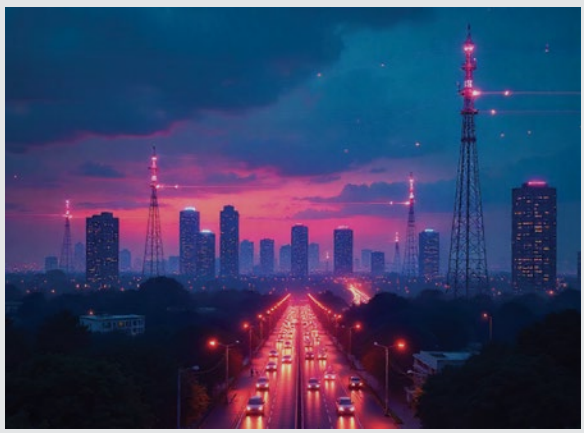
India's surging data needs demand a smarter spectrum policy—refarming, fair auctions, and a mid-band strategy are key to sustaining its digital growth.

India's digital journey is nothing short of remarkable. With over 365 million 5G subscribers and growing, the telcos have helped the nation emerge as a global leader in mobile connectivity. However, to keep pace with the swelling demand and rapid technological evolution, the telecom sector must optimise its spectrum strategy, the invisible backbone of all wireless communications. Let us delve into the critical components of this strategy: spectrum refarming, sharing frameworks and future spectrum auctions, illustrating how these pillars are vital to building a Digital India that is competitive, inclusive and future-ready.

THE SPECTRUM IMPERATIVE: A GROWING DEMAND

Spectrum is the lifeline for the telcos and, by extension, India's digital economy. As more Indians come online and emerging technologies, such as the Internet of Things (IoT), artificial intelligence or AI-driven networks, and autonomous systems, grow, wireless data consumption

Refarming idle government spectrum unlocks national assets for telecom use, boosting 5G capacity while protecting mission-critical services.



IN BRIEF

- India needs over 2 GHz of new mid-band spectrum by 2030 to meet the soaring demand for data and comply with global IMT-2020 standards.
- Refarming 687 MHz from government users boosts available spectrum to 1,587 MHz without disrupting critical national operations.
- High reserve prices have slowed past spectrum uptake; rational pricing can drive faster rollouts and affordable networks.
- Spectrum costs already consume 26% of operators' recurring revenues, one of the highest rates globally, and negatively impact investments.
- The 6 GHz band is critical for 5G and future 6G; licensed use ensures better coverage, capacity and rural inclusion.
- Private 5G should stay with licensed operators to safeguard security, revenue equity and efficient network management.

is soaring exponentially. Meeting this surging network load requires more spectrum, particularly mid-band frequencies that strike a balance between geographic coverage and network capacity.

Currently, India holds approximately 900 MHz of IMT spectrum (per Circle) for mobile services. However, to deliver world-class 5G performance and fulfil international IMT-2020 standards requirements, the telcos estimate that India needs to more than double the current amount, or an additional 2 GHz of mid-band spectrum would be required by 2030. The 6 GHz band could be the only viable solution for addressing this shortcoming.

REFARMING: UNLOCKING IDLE NATIONAL ASSETS

The Government of India took a landmark step this year by approving the refarming of 687 MHz of spectrum previously held by government agencies such as the defence forces and ISRO. This initiative, strongly backed by the telcos through sustained advocacy, raises India's total IMT spectrum from 900 MHz to approximately 1,587 MHz, a game-changer in addressing network capacity constraints.

Refarming is not just spectrum reallocation; it represents a strategic unlocking of underutilised national assets. Many government departments hold spectrum that can simultaneously fulfil their operational mandate while enabling commercial use for 5G and upcoming 6G services.

This phased refarming approach ensures that critical government functions continue uninterrupted, while significantly boosting spectrum availability for the telcos. Ultimately, it positions India to capture the vast socioeconomic opportunities that 5G promises, including an estimated USD 41 billion GDP boost by 2030, primarily driven by the deployment of mid-band spectrum.

FUTURE AUCTIONS: PRICING TO STIMULATE GROWTH

Past spectrum auctions in India have been marred by high reserve prices, resulting in significant portions of

> Rational spectrum pricing could accelerate India's digital rollout, making high-quality mobile broadband affordable and widely available.

spectrum remaining unsold and constraining network investments. Unsold spectrum translates directly into slower network expansion and limits consumers' access to affordable, high-quality mobile services.

The telcos firmly believe that auction reserve prices must be realistic and reflective of India's market and financial realities. Aligning reserve prices with roughly 50% of the Telecom Regulatory Authority of India's valuations, down from the prevailing 70%, is likely to promote competitive bidding, attract new entrants, and encourage more aggressive network rollouts.

The acquisition of new bands to support 5G and enhanced 4G networks has resulted in a gradual increase in the spectrum cost burden between 2015 and 2023. This currently stands at 26% of the operators' recurring revenues and is among the highest in the world.

Rationalised spectrum pricing can be seen as a catalyst for the recent accelerated 5G rollouts and improved network quality in India. However, the burden of spectrum cost will continue to influence India's progress towards its digital goals for years to come.

THE 6 GHZ BAND: THE MID-BAND CORNERSTONE

Among all spectrum bands, the 6 GHz range stands out as the linchpin for India's mid-band strategy. Given that a large portion of existing 5 GHz unlicensed Wi-Fi spectrum remains underutilised, delicensing the remaining 6 GHz band for Wi-Fi would be a lost opportunity. Licensed deployment of the full 6 GHz band provides a superior balance of coverage and capacity, enabling the delivery of robust mobile broadband to both urban and rural areas in India. Occupying this mid-band spectrum is critical not just for meeting immediate 5G needs but for sustaining network excellence through 6G and beyond.

PRIVATE 5G: LICENSED OPERATORS SHOULD LEAD

The debate over direct spectrum allocation to enterprises for private 5G networks continues, but telcos firmly advocate for a model in which licensed service providers manage these networks.

Telcos have invested trillions in licensed spectrum and infrastructure, bringing expertise, economies of scale, and regulatory oversight that are crucial to both security and performance. Enterprises can benefit from customised connectivity solutions via network slicing. Direct spectrum allocation, on the other hand, risks National Security, Government revenues and regulatory equity, potentially skewing competitive fairness and complicating network interference management.

POLICY CHOICES SHAPING WIRELESS ACCESS

As India looks to the immediate future, the priorities for telecom operators are clear: ensuring that the full 1200 MHz in the 6 GHz band is allocated for IMT and refining auction methodologies with realistic pricing that promotes efficient spectrum use without compromising competition.

Over the medium and long term, the sector must prepare for the demands of 6G spectrum, developing strategies for new frequency bands and evolving network architectures that will define the next decade of wireless innovation.

India's telecom sector stands ready to lead the next digital revolution. Building on a strategy that simultaneously unlocks idle spectrum, along with market-friendly auction frameworks, is imperative.

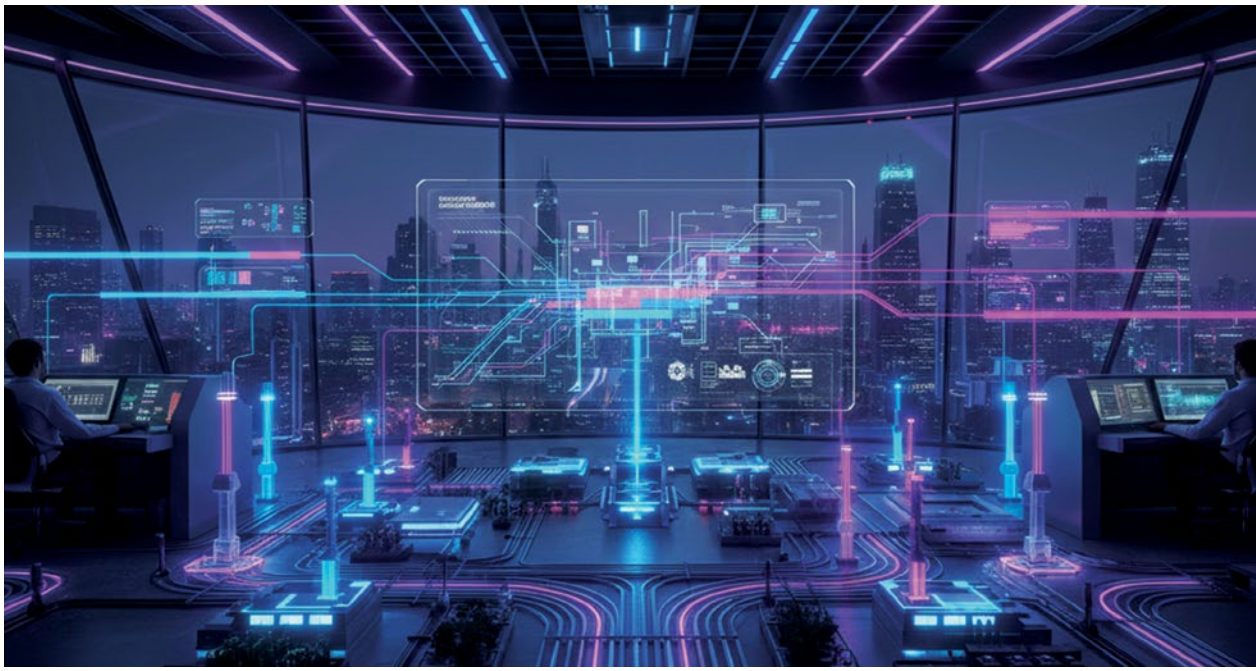
The spectrum policy choices made today will determine the quality, affordability, and inclusivity of connectivity for the country's 1.4 billion-plus citizens tomorrow. Through thoughtful and collaborative policymaking, India can emerge as a global leader in advanced wireless technologies, transforming societies, fuelling economies, and expanding opportunities for all.

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

Telcos find new lifeline in spectrum slicing

As revenues shrink and competition intensifies, spectrum-as-a-service offers telcos a shared model to unlock growth while empowering enterprises.



BY PRATIMA HARIGUNANI

It sounds like an April Fool's prank when you first hear the words Spectrum-as-a-Service. However, it is not just another phrase in telecom jargon—it goes several steps beyond. At first glance, it even feels like an oxymoron, something telcos would never entertain. After all, there is nothing more elusive, regulated, scarce, and competitively sensitive than spectrum for telcos. Over the decades, auctions, litigations, and policy debates have revolved around this single word. So, how could anyone think of slicing it?

Yet the question has never been more urgent. Telcos are struggling with both internal inefficiencies and external shocks—falling ARPUs, vanishing voice revenues, hyperscaler competition, and customer fatigue. With margins under pressure and monetisation pipelines drying up, the search for a new growth model is inevitable. Could slicing the spectrum offer that lifeline?

Is it not like attempting to cut through a steel truck—immense, expensive, and difficult to move? Yet, what if this seemingly absurd thought were possible? Imagine a company that owns a heavy vehicle and decides to rent out each component—one drives it, others share the seats, and someone uses its cargo hold. Suddenly, a static capital asset becomes a revenue-generating service.

Now, this metaphorical "what if" is becoming real. Spectrum can indeed be sliced and offered as a service. After cars, homes, software, and even rockets, spectrum has entered the as-a-Service age too. The question is—how does it work, and what makes it viable?

UNDERSTANDING THE MODEL AND HOW IT WORKS

At its core, spectrum-as-a-service is a commercial and technical model where Mobile Network Operators (MNOs)

"Licensed telecom operators are best placed to lease spectrum securely, ensuring national revenue protection, service reliability, and regulatory parity."

LT GEN DR SP KOCHHAR
Director General, Cellular Operators Association of India

dynamically allocate portions of their licensed spectrum to enterprises, vertical industries, and service providers on a usage or subscription basis.

Stan Gray, SVP of IoT Broadband and High-Cat Vertical Sales at Telit Cinterion, describes it as a flexible model that eliminates the need for enterprises to license spectrum or build full private networks. "Enterprises can leverage 5G capabilities such as reliability, slicing, and low latency without managing their own infrastructure or acquiring spectrum licences directly," he says. "The MNO remains the custodian of the network, offering virtualised, logically isolated services tailored to specific needs."

Stefan Voll, Senior Director of Business Development at Adtran, adds that spectrum services function as a wholesale layer within optical transport networks. "They are positioned between traditional offerings such as dark fibre and capacity services. While enterprises usually buy single-capacity services or fully managed optical fibre networks, spectrum services are often sold between service providers or for large-scale AI and data centre interconnects," he explains.

The appeal of the model is obvious. Telecom operators face relentless challenges: growing data consumption, shrinking margins, declining ARPUs, and rising infrastructure costs. On top of that, they face competitive pressure from hyperscalers, satellite operators, and private 5G networks. In such a landscape, the ability to monetise existing fibre and spectrum infrastructure becomes crucial. Spectrum-as-a-service enables operators to extend capacity, create differentiated services, and participate in enterprise digital transformation without massive new investments.

By partitioning the optical spectrum—both terrestrial and submarine—operators can allocate specific frequency bands to multiple end users. It is a shift from traditional ownership to shared utilisation, similar to the transition in cloud computing from hardware ownership to shared resource pools.

IN BRIEF

- Spectrum-as-a-service lets operators lease licensed spectrum dynamically, turning unused bandwidth into enterprise connectivity.
- It gives telcos a fresh revenue stream while enterprises gain private-network performance without capital or licence barriers.
- Programmable optics, ROADMs, and C+L-band cables make fine-grained spectrum slicing practical and commercially viable.
- The model supports 5G slicing and fuels diverse use cases—from AI and data centres to industrial IoT and healthcare.
- Telcos must achieve orchestration maturity and cultural change to monetise slicing at scale and sustain long-term growth.

Voll points out that this is not entirely new. "Spectrum services have long existed in submarine networks," he notes. "In terrestrial systems, they were once limited to research and education networks. But today, with exponential growth in AI and data centre interconnect

"As 5G standalone networks evolve and edge computing expands, spectrum-as-a-service enables telcos to reposition as end-to-end digital solution providers."

STAN GRAY
SVP – IoT Broadband & High-Cat Vertical Sales, Telit Cinterion

traffic, the concept is being revisited to accelerate deployment and share investment. Operators want to offer something more valuable than static dark fibre."

TECHNOLOGIES ENABLING SPECTRUM SLICING

The viability of spectrum-as-a-service depends on the advancement of optical and software-defined technologies that enable precision slicing and orchestration. Through programmable optics and advanced multiplexing, operators can divide infrastructure and offer dedicated capacity blocks to multiple clients.

C-band and hybrid C+L-band cables, which combine higher capacity and wider frequency support, have played a pivotal role. So, have tools such as Reconfigurable Optical Add-Drop Multiplexers (ROADMs), coherent transponders, and wavelength-division multiplexing systems. These technologies allow operators to carve out and manage separate optical slices without compromising network integrity.

"Consider one European infrastructure provider," says Voll. "They operate regional managed optical fibre networks—owning the fibre and optical line system—while customers manage the transponders delivering capacity at the wavelength level."

He cites further examples: "In long-haul AI and data centre networks, a single customer may consume the full spectrum. Research networks in Europe often exchange spectrum to extend reach without heavy capital investment. Some service providers even purchase a share of the DWDM spectrum from others to meet short-term capacity needs."

Gray points out that device trends, such as the emergence of 5G RedCap and eRedCap, further strengthen the case. "These mid-speed, cost-conscious devices fit perfectly with service-based spectrum delivery. They bridge the gap between high-end mobile broadband and low-power IoT, creating scalable, efficient, and customised opportunities for virtualised spectrum."

Together, these developments make spectrum sharing not just a technological feat but a practical business model for future connectivity ecosystems.

BUSINESS AND INDUSTRY IMPLICATIONS

Spectrum-as-a-service has the potential to reshape telecom economics. As Gray observes, "With consumer mobile markets nearing saturation and the ROI on 5G investments still uncertain, operators are looking for innovative monetisation strategies. The spectrum-as-a-service model aligns with the enterprise need for flexible, high-performance connectivity without the capex burden of private networks."

Market data support the financial rationale fir this. According to Fortune Business Insights, the global optical wavelength services market could reach USD 17.65 billion by 2032, while Grand View Research projects the dark fibre network market to grow from USD 6.25 billion in 2024 to USD 13.45 billion by 2030.

The Light Communication Alliance (LCA) captures the sustainability angle: use bandwidth only when required, reducing energy consumption and avoiding underutilisation. "This approach allows operators to optimise both spectrum and power usage," LCA notes. "It ensures that capacity is allocated dynamically, benefiting both efficiency and the environment."

For telcos, the rewards go beyond cost savings. By packaging dedicated spectrum capacity as a managed service, they can serve sectors undergoing digital transformation—manufacturing, logistics, utilities, and healthcare—each with distinct latency and reliability requirements. For instance, a hospital may require a secure, isolated spectrum slice for telemedicine, while an automotive firm may demand ultra-low-latency connectivity for Vehicle-to-Everything (V2X) systems.

The model also allows CSPs to shift from transactional relationships to long-term enterprise partnerships, positioning them as enablers of digital innovation.

"India's restrictions on foreign ownership in optical transport networks give local service providers a strong edge in serving AI and data centre demand."

STEFAN VOLL
Senior Director – Business Development, Adtran

"Operators can fully leverage existing network assets while opening new revenue streams," Gray notes. "It is a fundamental reorientation from selling connectivity to selling outcomes."

INDIA'S READINESS AND REGULATORY PERSPECTIVE

India represents a unique opportunity for spectrum-as-a-service due to its policy framework, market scale, and ongoing enterprise digitisation wave. However, it also poses distinctive regulatory challenges.

As Voll observes, "India's restrictions on foreign ownership of optical transport networks give local service providers a strategic edge in catering to global hyperscalers and AI-driven enterprises. Indian players can design, build, and operate networks on behalf of international clients, effectively localising global traffic flows."

Lt Gen Dr SP Kochhar, Director General of the Cellular Operators Association of India (COAI), has been categorical about the need to manage spectrum through licensed operators. In his statement on the Proposal for Direct Allocation of Spectrum to Private Networks, he noted:

"Direct spectrum allocation to enterprises is not tenable in India due to multiple considerations related to national revenue, telecom architecture, and security. Radio frequencies cannot be geographically contained; signals from private networks can spill beyond intended premises, interfering with public networks and affecting reliability and quality of service. Such risks are best managed by licensed Telecom Service Providers."

COAI's stance aligns closely with the logic of Spectrum-as-a-Service. Under this model, enterprise needs—whether for manufacturing automation, smart campuses, or logistics networks—can be met through licensed operators via leasing, network slicing, or managed services. This ensures both operational efficiency and regulatory compliance.

WHAT TELCOS MUST DO

For telcos, spectrum-as-a-service demands more than technology—it calls for new business thinking, operational maturity, and policy alignment.

- **Reinvent the business model:** Shift from bandwidth sellers to orchestrators of service-centric, outcome-driven enterprise connectivity solutions.
- **Invest in orchestration tools:** Deploy automation, AI, and advanced platforms to manage concurrent network slices efficiently, securely, and at scale.
- **Reskill and realign teams:** Develop cross-functional talent where sales, engineering, and operations collaborate to deliver tailored enterprise value.
- **Embed sustainability goals:** Optimise energy and spectrum use to cut costs, meet ESG commitments, and make green efficiency a business advantage.
- **Align with regulation:** Operate within licensed spectrum-leasing frameworks to ensure security, compliance, and national revenue protection.

> Spectrum slicing could rewrite telecom economics, helping operators monetise assets and enterprises scale smarter connectivity.

As India rolls out enterprise 5G and prepares for AI-driven industrial use cases, the model offers an avenue for monetisation without direct spectrum ownership. Combined with domestic production of optical equipment and data centre growth, this could establish a new revenue layer for Indian telcos while strengthening digital sovereignty.

OPPORTUNITIES, CHALLENGES, AND THE ROAD AHEAD

Spectrum services introduce a versatile option for building and expanding connectivity infrastructure. They support diverse deployment models—from metropolitan data corridors to rural access networks—enabling resource sharing and optimised capital use.

"There are strong applications outside AI and data centres," says Voll. "In rural regions, smaller operators often lack the funds to deploy full-scale DWDM systems. Sharing infrastructure through spectrum services provides a viable and sustainable model for driving digital transformation in such areas."

Revenue opportunities also extend to differentiated service levels, such as guaranteed latency for V2X applications, mid-speed industrial IoT connections, or secure, isolated slices for healthcare systems. Spectrum services can add monitoring and management layers to access and metro networks, enhancing the value of fibre assets beyond static leasing.

However, the transition is complex. Gray cautions that the shift demands a fundamental rethink of telco operations. "Operators must evolve from being network owners to orchestrators of service-centric experiences. It is about designing networks that adapt dynamically to enterprise needs rather than selling fixed capacity."

This evolution requires significant organisational realignment. Multiple concurrent network slices—each with unique performance metrics—necessitate advanced orchestration platforms and robust automation. Sales and engineering teams will need to collaborate more closely, offering consultative services rather than standardised bandwidth packages.

From a strategic standpoint, spectrum-as-a-service is not just about monetisation—it is about redefining telcos' role in the digital economy. As connectivity becomes embedded in every business process, telecom operators must position themselves as infrastructure enablers for industry transformation.

The shift also presents an opportunity to align with global sustainability goals. Efficient spectrum utilisation means less redundant equipment and lower power consumption. When paired with renewable energy adoption across networks, this could contribute meaningfully to operators' net-zero commitments.

SLICING THE TRUCK, STEERING THE CHANGE

What once seemed implausible—slicing something as intangible yet precious as spectrum—is now technically feasible and commercially relevant. Spectrum-as-a-Service extends the logic of cloud computing to the very fabric of connectivity.

For operators, it represents more than just another service model; it is an opportunity to reinvent revenue streams and restore value in an industry squeezed between costs and competition. Enterprises, in turn, gain the flexibility, reliability, and control of private networks without the burden of spectrum ownership. It is also a rare win-win moment in telecom's long struggle with profitability and performance.

Like slicing that proverbial steel truck, the process requires precision, the right tools, and a willingness to rethink ownership. It is not a butter knife task; it is a deliberate, engineered transformation requiring both sharp technology and strategic foresight.

As networks evolve toward 5G Advanced and 6G, this model could redefine how capacity is managed and monetised. For telcos seeking new growth engines and sustainable operating models, spectrum-as-a-service may well represent the next major pivot—where infrastructure becomes intelligent and spectrum itself becomes a service.

pratimah@cybermedia.co.in

PCQUEST

SM Consulting
Business & Technology Consulting | Learning & Development

3DC DIGITAL DATA PRIVACY COMPLIANCE DEMYSTIFIED WORKSHOP

Delhi | Mumbai | Pune
Chennai | Bangalore | Hyderabad

STEPS TO DPDPA 2023 COMPLIANCE WORKSHOP

Safeguarding Business Operations of Your Enterprise

Why Attend This Workshop

Mandatory Compliance: The DPDP Act, passed in August 2023, mandates strict compliance for safeguarding personal data.

Severe Penalties: Non-compliance can result in penalties of up to **₹250 crore.**

Top Priority For Leadership: Data protection is now a critical concern for IT leaders and senior management across industries.

Long Implementation Process: Achieving full compliance can take **10-12** months for large enterprises.

Actionable Guidance: The workshop offers practical strategies to implement the DPDPA framework effectively.

Addressing Key Challenges: Learn how to overcome the most pressing challenges in adopting new data protection protocols.

Protect Against Risks: Gain essential knowledge to safeguard your organization from legal risks and potential data breaches.

Key Workshop Modules

- Understanding the Act
- Organizational Initiatives
- Data Principal Rights
- Penalties & Harm Audits
- Building Organizational Change
- Data Inventory & Mapping
- Reviewing SLAs
- Data Protection Impact Assessments (DPIA)

Who Should Attend

- Chief Risk Officers (CROs) and Data Privacy Officers (DPOs)
- CISOs and IT Decision Makers & Influencers
- IT and Cyber Security Heads
- VPs, Directors and GMs of IT and Cybersecurity
- Data Protection and Compliance Leaders
- Cyber Law Practitioners and Cyber Investigators

CONTACT US

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

Scan the QR code for event registration and more information

[COMMENTARY]
COMPONENT MANUFACTURING

Made in India: Building the backbone of IoT hardware

From imported modules to home-grown chips, India's IoT hardware story is evolving into one of design control, ecosystem depth, and strategic resilience.

BY NIKUL SHAH

For years, India's Internet of Things (IoT) deployments relied heavily on imported components and modules. Companies assembled devices locally but sourced critical parts, sensors, passive components, wireless modules, and silicon from suppliers in China, Taiwan, and other countries.

That model delivered rapid adoption but left the country exposed to supply chain shocks, currency swings, and margin pressure. Today, a confluence of policy moves, capital allocation, and industry shifts is changing that calculus and nudging IoT hardware toward more indigenous solutions.

On the demand side—which is already large and growing fast—market estimates show that India's IoT devices market generated about USD 2.89 billion in revenue in 2024 and is forecast to expand at a strong compound annual growth rate over the decade. The scale of this demand is creating a viable domestic market for home-grown hardware suppliers, both established electronics manufacturers and a new cohort of specialised IoT module and sensor startups.

POLICY SUPPORT DRIVING LOCAL MANUFACTURING

Government policy is the visible catalyst. Production-linked incentive (PLI) schemes have been extended to telecom and networking, and most recently to passive electronics, a crucial input for IoT devices.

In March 2025, the cabinet approved a PLI package for passive components with an outlay of Rs 229.19 billion (about USD 2.68 billion), explicitly intended to boost

India's push for IoT self-reliance is gaining pace as startups, EMS firms, and policy incentives converge to reduce import dependence and build capacity.

domestic capacity for resistors, capacitors, inductors, and other components used in IoT hardware. These incentives make local production financially attractive and reduce the relative cost gap with imports.

The India Semiconductor Mission and related display and fab incentives further back this shift by offering fiscal support, in some cases up to 50% of project cost for approved semiconductor and display fabs, creating the long-term possibility of locally produced silicon for edge and connectivity chips. That kind of support is essential because chip fabs and display facilities require heavy capital and long lead times.

REDUCING IMPORT RELIANCE WITH LOCAL SUPPLY

The backdrop is a large import bill. Recent trade analyses put India's telecom, electrical, and electronics imports at around USD 89.8 billion for 2023–24, underscoring the extent to which the value chain has been imported to date. Reducing that import dependency is therefore both an economic and a strategic objective: every per cent of local value-addition translates into jobs, investment, and resilience.

On the semiconductor front, practical projects are materialising. For example, a HCL-Foxconn joint venture approved in 2025 involves a planned investment of roughly Rs 37.06 billion (about USD 435 million) for a wafer facility capable of producing 20,000 wafers per month and 36 million display driver chips per year; commercial production is targeted for the mid-2020s.

Projects like this reduce reliance on foreign fabs for specific chip types used in IoT displays and controllers.

LAYERS OF MADE IN INDIA IOT STACK

In the IoT ecosystem, indigenous capability spans multiple layers. At the component level, it includes passive parts, connectors, and discrete sensors. At the module level, it extends to integrated Wi-Fi, Bluetooth, and GSM boards. The silicon layer covers microcontrollers or MCUs, power management ICs, and, increasingly, application-specific chips. At the systems layer, it encompasses domestically engineered end devices and firmware optimised for local networks and use cases.

IN BRIEF

- India's IoT market, worth nearly USD 3 billion in 2024, is creating strong demand for locally sourced components and manufacturing capacity.
- Policy measures such as PLI and the India Semiconductor Mission are enabling a structured shift toward indigenous hardware production.
- Startups and EMS firms are driving modular, locally sourced IoT designs that reduce dependence on imported modules and shorten lead times.
- Sectors like utilities, logistics, and agriculture are early beneficiaries of localisation due to volume, cost sensitivity, and standardised design.
- Challenges persist around high-precision component manufacturing, testing infrastructure, and funding for early-stage hardware ventures.
- Over the next decade, India is expected to localise more of its IoT value chain, from passive parts to silicon, building a resilient ecosystem.

Startups and mid-sized electronics firms are now shipping indigenously sourced sensor boards, power modules, and enclosures for solutions such as smart metering, industrial monitoring, and agricultural sensing. While earlier designs relied on imported modules, engineers are increasingly redesigning PCBs to integrate locally manufactured passive components and regionally sourced RF modules, reducing costs and shortening lead times.

With modular design, local sourcing, and strategic incentives, India's IoT ecosystem is evolving from an assembler to a true hardware innovator.

BUSINESS MODELS DRIVING LOCALISATION

Several emerging business models are accelerating the adoption of locally sourced hardware. Contract Manufacturing Organisations (CMOs) and Electronics Manufacturing Services (EMS) firms act as scale partners for product companies, while component distributors serve both CMOs and OEMs. Design-for-Manufacturability and co-engineering services are helping reduce design iterations and simplify the transition to local components without compromising performance.

Another key trend is modularisation. IoT product teams are standardising on modular radio and sensor stacks built with either imported or local parts, enabling staged substitution as local suppliers mature. This hybrid approach reduces risk while encouraging gradual localisation.

MARKET CHALLENGES AND BOTTLENECKS

Despite momentum, several constraints slow the transition. High-precision passive components and advanced analogue chips are expected to remain imported mainly in the near term, as domestic production of some categories requires specialised equipment and scale economies. The quality, consistency, and reliability testing infrastructure also needs expansion; certification labs, EMI and ESD testing, and interoperability validation are still concentrated in a few urban areas.

Working capital and access to early-stage funding for hardware startups are comparatively limited in India, making it expensive to scale manufacturing lines and invest in testing. Finally, ecosystem coordination—aligning suppliers, design houses, CMOs, and policy incentives—is complex and takes time.

STRATEGIC WINS AND SECTORAL IMPACT

Where localisation is advancing fastest, it is delivering clear wins. Utilities and smart-metering projects benefit from local assembly and component sourcing because deployment volumes are high and device specifications are commoditised. Industrial IoT in sectors such as manufacturing and logistics offers advantages, including reduced lead times and support for bespoke firmware. In agriculture, cost-sensitive sensor nodes become more affordable when passive parts and enclosures are sourced locally.

The macroeconomic payoff is also significant. Lowering a portion of the roughly USD 90-billion electronics import bill by building domestic capacity would support export competitiveness in the medium term and create manufacturing jobs across states.

PRIORITIES FOR INDUSTRY LEADERS AND POLICYMAKERS

To keep momentum, three priorities stand out. First, invest in downstream assembly and quality assurance infrastructure to ensure domestically produced components meet global standards. Second, align financial incentives (PLI, credit facilitation, capex support) with early-stage investments and working capital for hardware startups. Third, accelerate skills development in electronics manufacturing and testing—from technicians to firmware engineers—through focused programmes and industry-academic partnerships.

A coordinated approach that links incentives for passive components, chip packaging, fab investments, and EMS capabilities will narrow the gap between assembly and true indigenous production.

REALISTIC TIMELINES AND LONG-TERM GAINS

The shift from import dependence to indigenous IoT hardware is progressing steadily, though incrementally. Policy measures such as the PLI scheme and the India Semiconductor Mission have established a structured roadmap, while industry investments are beginning to expand domestic capacity for specific component categories.

A phased evolution is expected: over the next two to five years, India is likely to localise a greater share of passive components, PCBs, and modules. In the following five to ten years, as incentives continue and semiconductor fabrication capacity comes online, higher-value silicon and display driver chips should see meaningful domestic production.

This will not yield overnight self-sufficiency, but it will create a far more resilient and competitive IoT hardware ecosystem anchored n India.

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

Powering India's cloud with sustainable data hubs

India's data centre boom is reshaping digital infrastructure, demanding clean energy, local innovation, and policy alignment to sustain its growth.

BY DAVID SEHYEON BAEK

India's digital economy is scaling at an unprecedented pace. From UPI transactions and OTT streaming to 5G-enabled factories and AI-driven platforms, the sheer volume of data generated in the country is exploding. By 2030, India's data traffic will be many times greater than today, driven by half a billion new internet users, the expansion of connected devices, and the rapid rise of AI applications. At the centre of this surge lies one critical infrastructure: data centres.

These facilities—warehouses of servers that process, store, and distribute information—are the beating heart of the digital economy. Yet they are also energy-hungry behemoths, consuming electricity at levels comparable to small cities. For India, building a sustainable data centre strategy is not just about server racks and fibre-optic cables. It is about securing the energy that powers them, while balancing economic growth, climate commitments, and global competition with giants like China and the United States.

> India's next phase of digital expansion hinges on how well it powers data sustainably while meeting surging demand for AI and cloud infrastructure.

> Clean energy, distributed infrastructure, and indigenous innovation are becoming cornerstones of India's sustainable data centre strategy.

MARKET GROWTH AND INVESTMENT MOMENTUM

India's data centre sector is already booming. Industry estimates show that the country's capacity stood at about 1,263 megawatts (MW) in April 2025 and is projected to exceed 4,500 MW by 2030—a more than threefold rise at a CAGR of 35–40%. The real estate footprint is expected to reach nearly 55 million square feet by the end of the decade.

This expansion is being matched by capital. According to IBEF, the sector has attracted USD 14.7 billion in investment since 2020, with another USD 20–25 billion expected by 2030, much of it from foreign institutional investors. Mumbai (41%), Chennai (23%), and Delhi NCR (14%) continue to dominate India's data centre landscape, while Tier 2 and Tier 3 cities such as Lucknow and Patna are now emerging as new destinations for edge facilities.

Leading players include Amazon Web Services, Microsoft Azure, Google Cloud, AdaniConneX, Yotta, and CtrlS. Notably, the Adani Group alone has announced USD 10 billion in new investment to build 10 GW of capacity over time.

POLICY REFORMS AND DATA SOVEREIGNTY

India's Digital Personal Data Protection Act mandates that sensitive personal data and critical personal data be stored domestically, though cross-border transfers are permitted under strict conditions. These rules are prompting companies to expand local infrastructure and making India one of the most attractive destinations for hyperscale investment.

Policy is also intertwined with sovereignty: data localisation is not just about efficiency—it is about safeguarding citizen data, reducing dependence on foreign jurisdictions, and strengthening control over national digital infrastructure.

RISING ENERGY DEMAND AND SUSTAINABILITY

This boom carries a significant energy cost. According to Mercom India's estimates, as of 2023, data centres consumed around 2% of India's total electricity —about 139 billion kWh—and demand is expected to surge as AI workloads intensify.

Reports also reveal that the bulk of power for data centres in India still comes from coal, though renewables account for about 30% of the supply. This means the country's COP26 commitment to achieve 50% non-fossil electricity by 2030 will require the sector to integrate far more renewable energy.

Cooling alone accounts for nearly 40% of total energy use, according to Eco-Business, underscoring the need for sustainable design as a core priority. Encouragingly, IBEF projects that green-certified facilities will increase from 25% today to 30–40% by 2030—evidence that operators are beginning to align climate goals with commercial expansion.

STRATEGIC PRIORITIES FOR THE NEXT DECADE

Securing clean and reliable energy: India must ensure that low-carbon sources power its data centres. Long-term power purchase agreements (PPAs) with renewable developers, hybrid solar-wind-battery models, and incentives for green energy integration will be critical. In the medium term, India should also explore nuclear options, such as small modular reactors, something that the US and China are piloting to ensure stable baseload power for digital infrastructure.

Designing green data centres: Cooling offers the most immediate gains. Technologies such as liquid immersion and evaporative cooling, along with AI-optimised thermal management, should become standard. Locating facilities in cooler geographies or near renewable corridors can further reduce costs and emissions. Tax incentives and green certifications will accelerate adoption.

Expanding distributed infrastructure: Three-quarters of India's current data centre capacity remains concentrated in Mumbai, Chennai, and Delhi NCR, but this imbalance will shift as Tier 2 and Tier 3 cities expand. Distributed infrastructure will reduce stress on metro power grids and bring capacity closer to users. Edge data centres—smaller facilities sited closer to demand—will be critical for latency-sensitive applications such as AR/VR, smart manufacturing, and connected mobility.

Aligning energy and data policy: Today, project approvals for data centres often focus on land and fibre,

> As data centres reshape India's digital backbone, green energy adoption will decide whether growth remains sustainable and globally competitive.

while power supply is treated as secondary. Coordinated planning between the Ministry of Power, the Ministry of Electronics and IT, and state governments will be essential. Blended renewable purchase obligations and infrastructure financing frameworks must explicitly integrate the data centre sector.

Building indigenous technology: India still depends on imported servers, chips, and cooling systems for hyperscale deployments. To mitigate supply risks, it must invest in indigenous R&D for energy-efficient chipsets, domestic server manufacturing, and green cooling technologies. Public–private R&D partnerships, backed by academia and startups, will be key to long-term self-reliance.

Leveraging geopolitical advantage: Data centres are not just digital infrastructure—they are strategic assets and tools of diplomacy. The US leverages hyperscalers, while China backs state-run mega-farms. India can build its own leverage by hosting sovereign cloud platforms, protecting undersea cables, and offering regional partners access to its data capacity. This, however, requires robust domestic infrastructure, backed by secure, renewable energy supplies.

LESSONS FROM CHINA AND THE UNITED STATES

China has scaled rapidly, building vast data farms in Guizhou and Inner Mongolia powered by hydropower and coal. The US, meanwhile, has relied on hyperscalers signing nuclear and renewable PPAs to guarantee carbon-free power for decades.

India must take a hybrid path by encouraging private investment while maintaining strategic oversight. Unlike China, it cannot rely on coal without undermining its climate goals. Also, unlike the US, the country lacks abundant venture capital and flexible power grids. Its approach must therefore blend regulation, incentives, and innovation to create a sustainable path.

PURSUING A SUSTAINABILITY-FIRST APPROACH

India's net-zero 2070 pledge places the data centre industry firmly within the national decarbonisation agenda. Sustainability must not remain an optional metric but become a defining standard. If embraced as a guiding principle, India could emerge not only as a digital powerhouse but also as a global model for green data infrastructure.

This opportunity extends beyond national borders. Other emerging economies in Africa and Asia face the same dual challenge of data growth and energy constraints. By developing sustainable, cost-effective models, India could export its know-how in digital infrastructure, much like it has with UPI and Aadhaar in digital public platforms.

BALANCING GROWTH WITH RESPONSIBILITY

The coming decade will test India's ability to reconcile expansion with sustainability. Policymakers will need to decide whether scarce renewable power should be prioritised for data centres or for manufacturing. Industry will need to balance rapid growth with ecological responsibility. Hence, India must manage hyperscaler dominance while encouraging investment.

These challenges are not deterrents—they are a call for strategic planning. If India balances its energy and data ambitions effectively, it can avoid the pitfalls seen elsewhere and build a resilient, sovereign, and competitive digital ecosystem.

Data centres are the cathedrals of the digital age—monuments not of glass and stone, but of servers, fibre, and electricity. For India, building them at scale is a necessity, not a choice. But powering them sustainably, securely, and strategically is a greater challenge.

As China and the United States race for both digital dominance and energy independence, India must craft its own model—anchored in clean energy, distributed and green infrastructure, indigenous innovation, and geopolitical foresight. The stakes are high, but so are the rewards. Success would not merely make India a participant in the global digital order—it would make it one of its architects.

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

[COMMENTARY]
WI-FI

Rethinking enterprise connectivity with managed Wi-Fi

As digital transformation accelerates, managed Wi-Fi is emerging as the backbone of agile, secure, and insight-driven enterprise connectivity in India.

BY NAVNEET SHARMA

In the past decade, enterprise Wi-Fi has evolved from a basic utility into a mission-critical foundation for business operations. Amid this transformation, Managed Wi-Fi has emerged as a transformative model, one where enterprises no longer just "buy and maintain" infrastructure but instead consume it as a fully managed, secure, and scalable service.

This shift comes as Indian businesses navigate digital transformation at an unprecedented pace. Cloud adoption, hybrid work, mobility, and the proliferation of connected devices are stretching the limits of traditional IT networks. For instance, 67% of Indian companies are already transitioning their applications to the cloud, while nearly 80% are adopting a hybrid approach—balancing on-premise systems with cloud platforms for agility and control. This cloud-led momentum is fuelling a new wave of digital innovation powered by advanced network connectivity. The demand today is no longer just for "faster speeds" but for agility, reliability, and security at scale.

INDIA'S ENTERPRISE CONNECTIVITY STRAIN

While cloud and AI are opening new frontiers of growth, they are also revealing a hard truth: India's enterprise connectivity infrastructure is under strain. As organisations race to modernise, many are realising that traditional Wi-Fi and LAN setups were never designed for the scale, speed, and security that digital-first operations now demand.

Fragmented networks remain one of the biggest pain points. Large enterprises often operate across multiple locations—factories, branch offices, retail outlets, and data centres—each relying on a patchwork of routers, access points, and service providers. The

> In India's race to digitise, managed Wi-Fi is the missing fulcrum: it brings agility, visibility, and security without burdening IT with complexity.

lack of centralised visibility makes it nearly impossible to monitor performance consistently or enforce uniform security policies.

For IT teams, this translates into rising overheads and operational complexity. Scalability poses another hurdle. A manufacturing plant deploying IoT sensors to monitor equipment health may find its legacy Wi-Fi network unable to handle thousands of concurrent connections reliably. Likewise, BFSI institutions that expand digital banking services face regulatory pressure to secure transactions end-to-end—a challenge that ad hoc networks can seldom meet.

Above all, security risks loom large. In hybrid work environments, unsecured access points or poorly managed guest logins create vulnerabilities that cybercriminals quickly exploit. For IT services firms handling sensitive global client data, even a minor breach can lead to disproportionate reputational and financial damage.

This is where Managed Wi-Fi becomes critical. It enables enterprises to enhance operational efficiency, improve customer experience, and foster innovation. More than a technology upgrade, Managed Wi-Fi is a strategic enabler that aligns network infrastructure with measurable business outcomes.

DRIVING EFFICIENCY AND COST CONTROL

One of the most pressing challenges for CIOs is managing fragmented networks. Traditional Wi-Fi demands constant patching, troubleshooting, and hardware refreshes, tying up skilled engineers in maintenance rather than innovation. Managed Wi-Fi reverses this model by offering a fully outsourced, SLA-driven service.

Enterprises no longer need to purchase, configure, or maintain access points and controllers. Instead, they pay a predictable subscription fee that covers design, deployment, monitoring, and upgrades. For example, a large retail chain rolling out digital-first stores across multiple cities can standardise its network architecture, monitor performance centrally, and roll out updates seamlessly—all without expanding its in-house IT team.

The result is a lower total cost of ownership (TCO) and far greater agility in scaling operations.

IN BRIEF

- Managed Wi-Fi turns infrastructure ownership into a subscription service, bundling design, monitoring, updates, and SLAs under one roof.
- With 67% of Indian firms moving to the cloud and ~80% adopting hybrid models, networks must deliver agility, resilience, and integrated security.
- Centralised management dissolves network fragmentation and allows uniform policy enforcement across branches, campuses, and retail outlets.
- Embedded security (NGFW, UTM, identity-based access) ensures compliance and reduces breach risk across distributed, hybrid environments.
- Pay-as-you-grow scalability handles surges in IoT, branch expansion, and user density without disruptive infrastructure overhauls.
- Analytics and AI make the network a source of insight — enabling proactive tuning, anomaly detection, and strategic decision support.

STRENGTHENING SECURITY AND COMPLIANCE

As Indian enterprises digitise, cybersecurity has become a boardroom concern. Traditional Wi-Fi networks—with unsecured guest access points or inconsistent patch management—expose organisations to breaches that can erode customer trust and invite regulatory penalties.

> CIOs can free up resources and shift from reactive firefighting to strategic innovation when connectivity becomes a managed, data-aware service.

Managed Wi-Fi solutions incorporate enterprise-grade security protocols, including next-generation firewalls (NGFW), Unified Threat Management (UTM), and identity-based access control. Features like OTP-based visitor logins, policy-based access controls, and real-time threat monitoring ensure that only authorised users and trusted devices connect to enterprise networks.

In regulated sectors such as BFSI and healthcare, this translates to audit readiness and stronger compliance with data protection frameworks. Banks, for example, can leverage Managed Wi-Fi to ensure consistent encryption and monitoring across branches, protecting sensitive transactions while meeting regulatory obligations.

SCALING NETWORKS FOR BUSINESS GROWTH

In a country where enterprises expand at breakneck speed, networks must scale just as fast. Adding offices, onboarding thousands of employees, or deploying IoT devices should not require a complete network overhaul. Managed Wi-Fi provides a pay-as-you-grow model, allowing enterprises to add capacity, users, and sites with minimal disruption. Centralised network orchestration ensures expansion is rapid, predictable, and secure.

Consider a manufacturing enterprise deploying IoT-based predictive maintenance across multiple plants. With Managed Wi-Fi, the company can securely connect thousands of sensors, scale capacity on demand, and monitor the entire ecosystem from a single dashboard—improving productivity without adding IT complexity.

ENHANCING USER EXPERIENCE AND PRODUCTIVITY

In today's digital workplace, poor connectivity has a direct impact on productivity. Managed Wi-Fi delivers seamless roaming, high availability (with uptime of up to 99.5%), and application-aware bandwidth allocation. This ensures that business-critical workloads, such as video conferencing, cloud ERP, or virtual collaboration, receive priority over non-critical traffic.

Knowledge workers in IT and ITeS firms, for instance, benefit from consistent and secure access, whether in the office, working remotely, or on client sites. For customer-facing sectors like hospitality and retail, frictionless Wi-Fi access directly enhances customer satisfaction and brand engagement.

UNLOCKING INSIGHTS THROUGH NETWORK DATA

One of the most underappreciated benefits of Managed Wi-Fi is its ability to turn the network into a source of actionable intelligence. With built-in analytics and AI/ML-driven dashboards, enterprises gain visibility into user behaviour, application performance, and threat patterns.

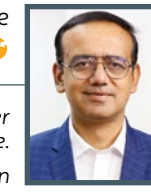
This visibility is particularly valuable in sectors such as education and large events, where footfall analytics can guide crowd management, or in corporate campuses, where usage data helps IT teams fine-tune performance and pre-empt outages. By shifting from reactive troubleshooting to proactive optimisation, Managed Wi-Fi transforms the network from a cost centre into a strategic asset.

MANAGED WI-FI: A STRATEGIC IMPERATIVE

As India accelerates toward its goal of becoming a major digital economy, connectivity can no longer be treated as an operational utility. It is now a strategic enabler that determines how effectively enterprises adopt cloud, scale AI, safeguard data, and deliver superior customer experiences.

Managed Wi-Fi marks a decisive step in this evolution. By combining operational efficiency, enterprise-grade security, scalability, and data-driven insights, it empowers organisations to turn their networks from a cost burden into a competitive advantage. For CXOs, this means elevating connectivity to a boardroom-level priority. The question is no longer "Do we need Wi-Fi?" but rather "How can Managed Wi-Fi future-proof our digital enterprise?"

In the coming decade, the enterprises that lead will be those that treat connectivity not as an afterthought but as the foundation of digital competitiveness. Managed Wi-Fi is more than a technology solution—it is the connective tissue of India's digital future.

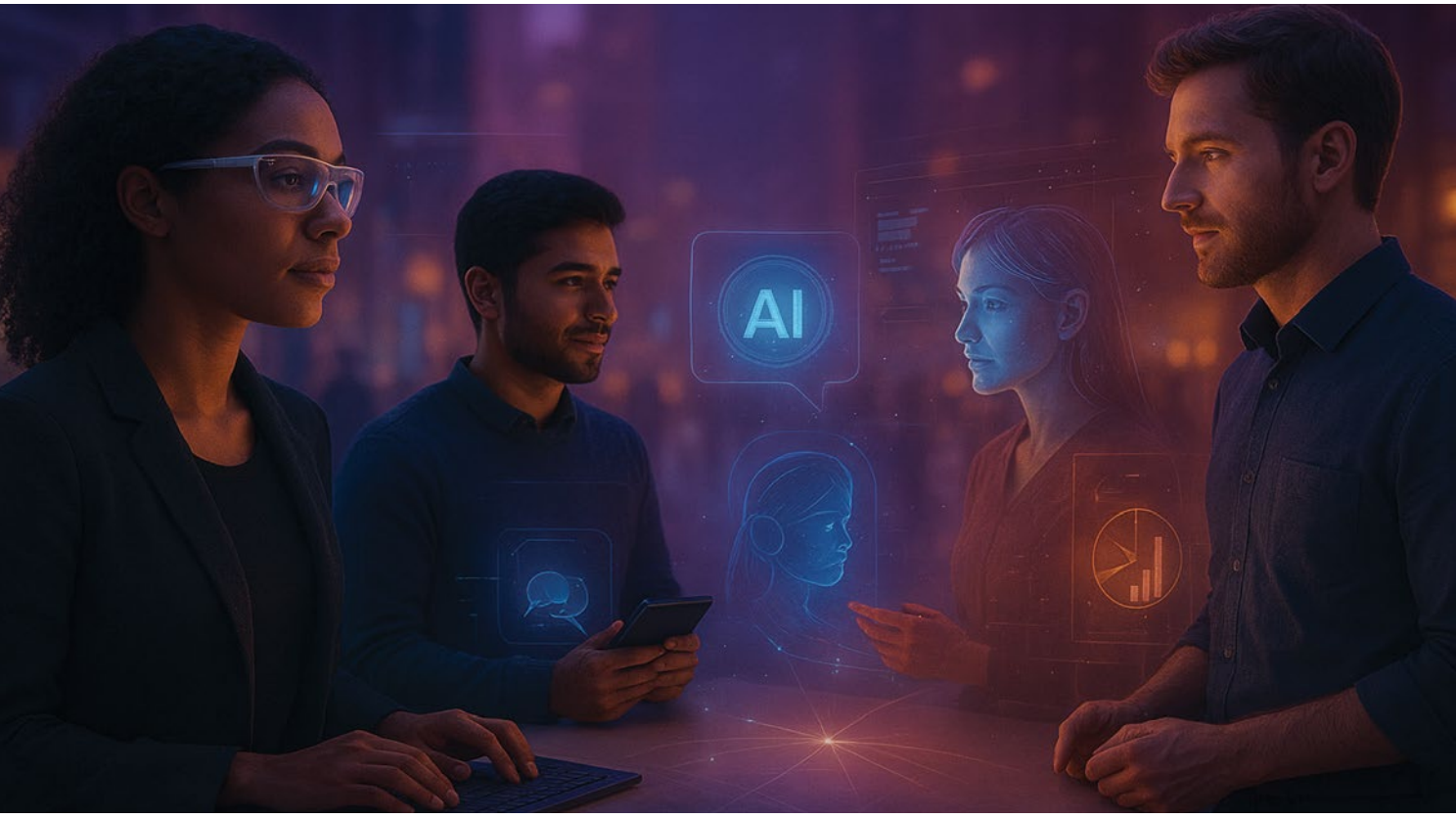


The author is the Chief Operating Officer of ACT Enterprise.

feedbackvnd@cybermedia.co.in

In the age of personal AI, broadcast fades to whisper

AI is redefining communication—shifting societies, enterprises, and individuals from shared narratives to curated realities.



BY PROF NITIN SINGH

Hyper-personalisation in social networks is not just a technological trend. It is a phenomenon quietly reshaping how societies think, how businesses operate, and how individuals make choices.

For most of the twentieth century, communication was defined by scale. A single message was broadcast through newspapers, radio, or television and consumed by millions. Marshall McLuhan's phrase, "The medium is the message," captured that era well.

Today, the medium is fragmented. Social networks no longer address the crowd; they communicate with individuals. Algorithms track likes, pauses, and moods, curating individual worlds based on engagement rather than truth or chronology.

> Personal AI is reshaping human dialogue—turning algorithms into silent mediators that shape what we read, believe, and act upon.

As the line between social and enterprise AI blurs, the next frontier of communication will be defined by intent, not just intelligence.

Personalisation, once associated mainly with Facebook, TikTok, or Instagram, has now crossed into enterprise information systems. In organisations, personalisation has moved beyond an abstract premise to a concrete application.

At Siemens, predictive analytics modules flag contracts and projects at risk of delay. General Electric uses maintenance systems that generate automated alerts for equipment likely to fail across its industrial operations. Unilever uses procurement dashboards to provide supplier-specific information that supports sourcing decisions. At IBM, leadership platforms track costs, approvals, and project progress in real time.

These cases show that personalisation has shifted from newsfeeds to decision intelligence in enterprises. What social networks achieve with attention, enterprises accomplish with action.

THE EVOLUTION OF PERSONALISATION

Unlike what many may believe, hyper-personalisation is not the creation of artificial intelligence (AI). Instead, its roots lie in human communication. Throughout history, leaders have adapted their messages to the audience's mood, fears, and hopes. For example, Winston Churchill inspired courage during wartime by matching his words to the nation's emotional state: "We shall fight on the beaches, we shall fight on the landing grounds, we shall fight in the fields and in the streets."

Shakespeare's Mark Antony demonstrates how messages evolve with audience sentiment, beginning with "Friends, Romans, countrymen, lend me your ears" and gradually transforming audience grief into fury.

Today, algorithms read micro-expressions, analyse tone of voice, and evaluate sentiment at a scale unimaginable in earlier times. Alvin Toffler's observation in Future Shock, "Technology feeds on itself. Technology makes more technology possible," remains strikingly relevant.

This observation resonates quite aptly with the rise of new technologies in hyper-personalisation. Generative

IN BRIEF

- Communication has moved from mass broadcasting to hyper-personalised messaging, reshaping how people, platforms, and organisations interact.
- AI personalisation mirrors human communication, adapting tone and content to emotion, intent, and behaviour across digital ecosystems.
- Technologies such as generative AI, NLP, IoT, and edge computing enable adaptive, privacy-conscious personalisation at scale.
- As algorithms curate choices, they influence politics, consumption, and public opinion—demanding responsible design and transparent governance.
- Bias, data misuse, and filter bubbles threaten trust, making fairness and ethical oversight integral to AI-powered communication systems.
- The future of personal AI lies in empathy-driven algorithms that enhance understanding rather than manipulate engagement.

> Hyper-personalisation must evolve with conscience, ensuring AI listens to humanity without amplifying its divisions.

AI now creates dynamic content tailored to individual preferences, while natural language processing engines such as chatbots calibrate tone and recommendations in real time through continuous conversation.

Similarly, computer vision is reshaping retail by recognising customer behaviour in physical stores, and wearable devices, along with IoT sensors, feed health platforms with streams of personal data. At the same time, edge computing and federated learning enable personalisation without exposing sensitive data, enabling enterprises to deliver customised interactions while maintaining privacy.

BALANCING INNOVATION AND RESPONSIBILITY

Such technological power comes with profound responsibility. For instance, in social networks, hyper-personalisation can shape elections, polarise societies, and deepen echo chambers. In enterprises, AI influences creditworthiness, pricing, and vendor selection. In public policy, algorithms affect subsidies, infrastructure priorities, and energy pricing.

Shoshana Zuboff, in The Age of Surveillance Capitalism, asks three critical questions: "Who knows? Who decides? Who decides who decides?" These are central to preserving trust in institutions.

The convergence of social AI and enterprise AI points to algorithms that not only curate information but also anticipate actions—predicting supply disruptions, guiding investments, and shaping citizen-centric policies.

The risks are significant: will these systems empower better decision-making, or will they quietly eliminate choices? Peter Drucker's warning, "The greatest danger in times of turbulence is not the turbulence; it is to act with yesterday's logic," is particularly relevant across industries.

At the end of the day, hyper-personalisation must prioritise people, society, and ethics before efficiency. Technology, algorithms, and abundant data already exist; the challenge lies in responsible governance.

Opportunities are immense, but so are the challenges. Filter bubbles and echo chambers narrow perspectives. Privacy concerns intensify as every action becomes fuel for personalisation engines. Algorithmic manipulation can invisibly nudge consumption, preferences, and even beliefs. Bias in AI models risks reinforcing structural inequalities in access to loans, jobs, or healthcare. Governance and fairness are therefore not optional—they are essential.

SPOTTING EMERGING TRENDS IN HYPER-AI

Three emerging trends are expected to define the future of hyper-personalisation. First, personalisation will shift from reactive to proactive, anticipating needs before they are expressed, whether in preventive healthcare alerts or optimised travel recommendations.

Next, privacy-preserving personalisation, enabled by frameworks such as federated learning, will allow customisation without exposing raw data. Third, regulation—through frameworks such as the EU's AI Act and global data-privacy laws—will shape the equilibrium between innovation and human rights.

Hyper-personalisation offers immense opportunities for value creation, enhanced experiences, and innovation. Yet it also raises critical questions about privacy, fairness, and trust. The responsibility lies with researchers, technologists, policymakers, and consumers to ensure that personalisation empowers rather than exploits.

Ultimately, technology does not define humanity; it reveals it. At its best, personalisation amplifies human potential, broadens perspectives, and strengthens the foundations of society rather than weakening them.

The author is a Professor of Business Analytics at IIM Ranchi and Visiting Fellow at Hong Kong Poly University, and Ural Federal University, Russia.

(The views expressed are those of the author and do not necessarily reflect official policy, position, or endorsement of the organisations or institutions he works with.).

feedbackvnd@cybermedia.co.in

"Collaboration is key to India's IoT success"

Sachin Arora *is a veteran of India's telecom and connectivity ecosystem, currently serving as Head of Connectivity & IoT at Giesecke+Devrient (G+D), India. With over two decades of experience spanning strategy, operations, R&D, and business transformation, he leads G+D's efforts in eSIM and iSIM adoption, secure IoT stacks, and cross-industry deployment.*

In a conversation with ***Pratima Harigunani,*** *he unpacks the key hurdles and opportunities in India's IoT connectivity journey—from regulatory friction and fragmentation to latency and security trade-offs—and offers a side-by-side comparison of emerging telco technologies. This candid exchange reveals where operators must invest, adapt and innovate to win in the connected future. Excerpts:*

What is new for Indian telecom operators in the IoT connectivity market, particularly in sectors like manufacturing?

India's convergence of 5G, the Internet of Things (IoT), and embedded SIM (eSIM) or integrated SIM (iSIM) technologies is opening up enormous opportunities for telecom operators. In manufacturing, operators can enable smart factories through real-time monitoring, predictive maintenance, and robotics-driven automation.

In logistics, IoT supports asset tracking, fleet management, and supply chain optimisation, while eSIM-enabled devices simplify deployment and remote management.

What is happening in verticals like logistics, automotive, and utilities?

The automotive sector is rapidly moving toward connected vehicles, with operators powering telematics, diagnostics, and secure over-the-air updates. In utilities, IoT is transforming grids, water systems, and metering through secure, reliable two-way connectivity and large-scale device rollouts.

Across all these sectors, telcos that invest in scalable, secure, and standards-compliant IoT platforms will be best positioned to lead.

What should Indian telcos do—and do differently—now?

To fully capitalise on the immense potential of IoT connectivity in India, telecom operators must go beyond traditional roles and invest strategically across infrastructure, platforms, and partnerships.

On the infrastructure side, telcos need to accelerate the rollout of next-generation networks such as 5G, NB-IoT, and edge computing, supported by scalable fibre backhaul, small cells, and cloud-native platforms. This will ensure reliable, low-latency, and wide-area coverage, essential to supporting millions of connected devices across sectors such as manufacturing, logistics, utilities, and automotive.

Equally important is the partner ecosystem. Telcos must collaborate with technology vendors, device makers, cloud providers, and system integrators to deliver end-to-end IoT solutions that combine connectivity with device management, analytics, and security.

By building comprehensive IoT platforms with services such as predictive maintenance, smart asset tracking, and remote monitoring, operators can unlock new revenue streams while meeting sector-specific enterprise needs.

What could play the party-popper—any major challenges that could hinder Indian telcos as they move forward to tap IoT as a business stream?

Telcos in India face regulatory, technological, and operational hurdles as they scale IoT connectivity due to market fragmentation. The regulatory landscape is still evolving, with fragmented policies around spectrum, data privacy, SIM management, and data residency.

SACHIN ARORA
Head – Connectivity & IoT, Giesecke+Devrient, India

> The future of IoT in India will depend on automation, secure SIM lifecycle management, and closer collaboration across the connectivity ecosystem.

Greater engagement with regulators is needed to establish consistent, practical frameworks that balance growth with user protection. Technologically, interoperability across diverse devices, integration with legacy systems, and ensuring robust security remain major challenges.

Providing wide-area, reliable, and low-latency coverage, particularly in remote or industrial areas, also demands significant infrastructure investment. The way forward lies in end-to-end stacks automation, remote SIM life cycle management through eSIM and iSIM platforms, GSM Association or GSMA certified frameworks like SGP.32. At G+D, we believe collaboration, innovation, and strategic investment will enable Indian telcos to overcome these barriers and unlock the transformative potential of IoT across industries.

How is secure IoT connectivity shaping automation and efficiency in the Indian manufacturing sector?

Secure IoT connectivity is significantly transforming automation and efficiency in the Indian manufacturing sector by enabling real-time data exchange, facilitating predictive maintenance, and minimising downtime. It allows seamless machine-to-machine communication, which is essential for the development of smart factories and intelligent industrial operations. Robust security measures play a critical role in building trust in automated processes and protecting valuable intellectual property.

When choosing between spectrum-based and fibre-based connectivity for industrial IoT, what factors—such as scalability, latency, and security—should enterprises consider?

Enterprises should carefully assess scalability, latency, and security when deciding between spectrum-based and fibre-based connectivity.

Spectrum-based solutions such as 4G and 5G private networks offer greater flexibility, especially for mobile or remote devices across a manufacturing site. In contrast, fibre connectivity is ideal for fixed locations requiring high bandwidth and consistent performance, such as core factory operations.

From a latency perspective, fibre provides ultra-low delay and exceptional reliability, making it well-suited for mission-critical workloads. Spectrum-based connectivity, particularly 5G, also delivers near-real-time responsiveness, though minimal wireless overhead may slightly increase latency.

What about the security?

Fibre offers strong physical security due to its wired nature, but remains vulnerable to physical damage, such as accidental cuts. Spectrum-based connectivity relies on advanced encryption protocols and SIM-based authentication mechanisms to mitigate risks related to wireless interception or unauthorised access. Each option presents distinct advantages, and enterprises should choose based on operational needs, balancing mobility, performance, and security requirements.

How crucial and manageable is the security aspect of IoT infrastructure?

Secure onboarding is critical and can be achieved through hardware-based authentication methods such as IoT SIMs, eSIMs, and secure elements to verify device identity from the start. Protecting data requires implementing end-to-end encryption, Virtual Private Network or VPN tunnels, and secure APIs to safeguard information in transit and at rest.

Effective device management involves continuous monitoring, timely firmware updates, and regular patching to proactively address vulnerabilities. Additionally, robust lifecycle control platforms are essential to manage key functions such as device provisioning, remote updates, suspension, and secure decommissioning—preventing potential security gaps throughout the device's operational life.

By integrating technologies like eSIM, In-Factory Profile Provisioning, and iSIM, organisations can build secure, scalable, and cost-efficient IoT infrastructure that supports devices from deployment through decommissioning.

pratimah@cybermedia.co.in

CyberMedia

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

LEAD THE CONVERSATION USING CYBERMEDIA'S 360° GTM STRATEGY.

UNMATCHED REACH ACROSS OUR FLAGSHIP BRANDS

DATAQUEST
Enterprise & Tech Leadership

PCQUEST
CIOs, Tech Influencers & SMBs

VOICE&DATA
Telco & Digital Infra Leaders

DQCHANNELS
ICT Partners & Channel Decision Makers

OUR BESPOKE B2B MARKETING PROGRAMS BUILD,ENGAGE AND SCALE COMMUNITIES THROUGH

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

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

DELIVER INFLUENCE AND OUTCOMES WITH CYBERMEDIA

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

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

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

[USE CASE]
MESSAGING

Banking on richer, safer digital conversations

RCS redefines banking communication with verified security, two-way interactivity, and measurable engagement that builds digital trust at lower cost.

BY ANIKETH JAIN

For banks, the primary goal of customer communication is to engage effectively through channels that drive growth while maintaining the highest levels of security and compliance.

Yet, despite heavy investments in digital transformation, many institutions continue to depend on legacy communication systems. These outdated tools not only increase operational costs but also expose banks to greater security and compliance risks. Traditional methods like SMS and email place additional strain on IT teams and create vulnerabilities within the security framework.

Rich Communication Services (RCS) has emerged as a modern alternative—a messaging protocol that replaces traditional SMS with richer, interactive, and more secure communication. Unlike SMS, which is confined to plain text, RCS supports images, videos, file sharing, carousels, quick reply buttons, and read receipts—all delivered through a customer's default messaging app.

For banks, RCS offers a powerful way to modernise customer engagement while cutting operational expenses. With enterprise-grade security and advanced interactivity, RCS can reduce support costs by up to 60% and minimise fraud through verified business profiles and encrypted exchanges. It empowers banks to deliver multimedia alerts, real-time updates, and actionable buttons, transforming how customers interact with financial institutions.

By integrating RCS into their communication strategy, banks can strengthen customer trust while differentiating themselves in a crowded digital marketplace.

HOW RCS STRENGTHENS SECURE BANKING

In today's hyper-digital economy, customers expect speed and safety in equal measure. Banks that can assure both are more likely to win lasting loyalty.

Unmatched security features: Security is non-negotiable in banking communications, and RCS meets this need with end-to-end encryption and verified business profiles that make impersonation nearly impossible. Every message originates from the bank's verified sender, helping customers instantly distinguish legitimate communication from scams. This is crucial at a time when more than 60% of consumers express concerns about data misuse during banking transactions.

Superior engagement rates: RCS achieves a 90% open rate within 15 minutes of delivery, outperforming SMS and email by a wide margin. Banks leveraging RCS have seen an 86% improvement in read rates compared to email and a 120% boost in clicks over SMS. This higher engagement directly translates into faster customer actions and reduced support overheads—especially vital for fraud alerts or transaction confirmations.

Interactive features: Modern banking demands seamless two-way communication without overloading support teams. RCS addresses this by offering interactive features enabling customers to act instantly—confirming transactions, reporting suspicious activity, or updating account details. Notably, 89% of consumers say they prefer such direct, two-way interactions, leading to higher satisfaction and lower call-centre volumes.

RCS DRIVES MEASURABLE IMPACT

As banking shifts toward conversational, real-time engagement, RCS offers measurable operational and strategic advantages.

Reduced support costs: Interactive RCS messages enable banks to handle routine customer service queries more efficiently, allowing customers to check balances, verify transactions, and update preferences within the same message thread. This self-service model not only enhances the customer experience but also frees up human agents to handle complex queries.

Improved conversion rates: With high readability and interactive functionality, RCS ensures quicker responses to time-sensitive communications—from fraud alerts and payment confirmations to account updates. Faster action means fewer fraudulent losses and smoother resolution of customer issues.

Enhanced analytics: RCS allows banks to track open rates, response times, and feature usage with far greater accuracy than traditional SMS or email systems. These insights enable targeted communication strategies and measurable ROI.

MEASURING SUCCESS WITH RCS

For banks implementing RCS, measuring success requires looking beyond basic delivery rates and focusing on deeper engagement and impact metrics. Key performance indicators include message open times and response rates, the usage of interactive features, and improvements in customer satisfaction scores.

Banks should also track the reduction in support tickets, higher transaction completion rates, and fewer security incidents, all of which reflect the actual value of RCS in enhancing communication efficiency and customer trust.

DESIGNING TOMORROW'S TRUSTED COMMUNICATION

As digital banking continues to evolve, the need for secure and engaging customer communication becomes increasingly critical. RCS goes beyond being a simple SMS upgrade, positioning itself as a strategic investment for banks. By enabling verified sender profiles, it enhances security and builds customer trust, while interactive features drive customer engagement. Automated interactions help reduce operational costs, and faster customer responses improve fraud prevention. Together, these capabilities allow banks to deliver branded, trustworthy, and future-proof communication experiences.

RCS holds strong potential to overtake SMS as the leading channel for banking communications. By blending the universal accessibility of messaging with the advanced features modern banking demands, it delivers both reach and functionality. With Apple's recent commitment to support RCS, the platform is poised to become the new standard for secure banking communication.

For banks aiming to elevate customer communications without compromising security, RCS offers a strategic pathway to strengthen relationships, improve efficiency, and build digital trust. With rising customer expectations and sophisticated security threats, the blend of verified identity, encryption, and interactive features makes RCS a vital tool for future-focused banks.

The author is the Co-founder & CEO of Fyno.
feedbackvnd@cybermedia.co.in

Breaking data barriers with light

Li-Fi uses the power of light to deliver ultra-fast, secure, and interference-free connectivity—illuminating a new frontier in digital communication.

BY PRATIMA HARIGUNANI

It may not be as revolutionary as Edison's bulb, but it promises to shine with brighter, faster, and ultra-low-latency connectivity than the lanterns before it. Li-Fi—or Light Fidelity—is light-driven connectivity that uses the power of light for data transmission. In a world dominated by Wi-Fi, this technology presents an intriguing alternative for illuminating specific connectivity needs.

By harnessing the expansive, unlicensed light spectrum for data transfer, Light Communication (LC) offers a compelling and sustainable response to the growing demand on traditional radio-frequency (RF) networks, explains Marc Fleschen, Chairman of the Light Communication Alliance.

The concept originated in Optical Wireless Communication, where unguided visible, infrared, or ultraviolet light is used to carry a signal. This broad field includes two key technologies.

The first is Visible Light Communication (VLC), which transmits signals within the visible spectrum (380–700

> Where radios struggle, light steps in—creating secure, high-density microcells that turn ceilings into networks and seats into ports of private bandwidth.

> Li-Fi doesn't replace Wi-Fi; it complements it, offloading traffic, boosting security, and unlocking new services from asset tracking to in-flight broadband.

nm) using light-emitting diodes (LEDs). VLC works like Morse code, rapidly switching LEDs on and off at frequencies imperceptible to the human eye. The speed of these oscillations enables vast amounts of data to move in fractions of a second.

Li-Fi operates by encoding data in modulated light waves emitted from LEDs. When information is transmitted, the LED's brightness oscillates at ultra-high frequencies—far beyond human visual perception. These light pulses represent binary codes of 1s and 0s, which a photodetector at the receiving end captures and demodulates back into electronic data. In essence, Li-Fi is light's own Morse code, turning illumination into information.

As a high-speed, bidirectional, mobile communication system, Li-Fi provides additional capacity for surging downlink demand, complementing both wired and wireless networks.

Another branch is Free-Space Optical (FSO) communication—a point-to-point system usually deployed outdoors that eliminates the need for cabling in backhaul networks. This makes FSO ideal for short-range and indoor applications where traditional cabling is cumbersome or expensive.

WHY LI-FI STANDS OUT FROM WI-FI

With LEDs, light bulbs emit rapid light pulses instead of radio waves. These pulses, packed with information, allow Li-Fi to communicate at remarkable speeds with receivers that decode this optical Morse code. Some players claim that Li-Fi can be up to 100 times faster than Wi-Fi, offering 'lightning-fast' (pun intended) transfer rates due to the vast bandwidth available in the light spectrum.

Unlike Wi-Fi, light waves can even penetrate water and operate effectively in dense or enclosed environments—an advantage for submarines, industrial environments, hospitals, and classrooms. Li-Fi is also less susceptible to interference and hacking. Since light cannot cross walls, light-bound data can be confined to controlled areas, enhancing privacy and network security.

Li-Fi can coexist seamlessly with conventional connectivity such as Wi-Fi and 5G while mitigating electromagnetic interference—critical in hospitals, aircraft, and industrial plants. Because it uses non-ionising radiation, it is considered safe for human exposure, addressing health concerns often associated with prolonged RF exposure. "Li-Fi has been tested rigorously, even on aircraft in mid-air, and proven 100 per cent safe," assures Fleschen.

Trials have demonstrated potential transmission rates exceeding 224 Gbps, elbowing out WiGig in sheer speed. "The physical confinement of data within a room offers a unique layer of security that Wi-Fi cannot match," Fleschen explains. "This transforms a perceived limitation into a strategic advantage for high-security or sensitive environments. Li-Fi is not a replacement for Wi-Fi but a specialised, high-value solution for targeted applications such as Fixed Wireless Access."

Fleschen notes that LC offers unmatched benefits in data speed, military-grade security, immunity to electromagnetic interference, and spectrum efficiency. "Laboratory demonstrations have shown access points aggregating 2 Tbps using Vertical Cavity Surface Emitting Lasers in a Multiple Input Multiple Output configuration with energy consumption below 2 watts—achieving energy efficiency close to 1 pJ/bit, which meets 6G requirements," he says.

The unregulated visible and infrared spectrum enables reuse without interference, offering an immense, untapped bandwidth that alleviates the spectrum crunch of traditional wireless networks.

BEYOND SPEED: UNLOCKING NEW POTENTIAL

Proponents argue that Li-Fi can address the limitations of Wi-Fi and cellular networks—spectrum congestion, security vulnerabilities, and inconsistent user experiences—while reducing infrastructure complexity and power use. It is particularly suitable for environments where radio frequencies are prohibited, restricted, or unreliable, such as hospitals, aircraft, schools, and defence sites.

> From labs to live pilots, the roadmap runs through interoperable standards, cheaper optics and a "tungsten moment" that scales from rooms to campuses.

The potential bandwidth of 360 terahertz (360,000 GHz) is more than 10,000 times wider than the radio portion of the spectrum, enabling exceptionally high data rates in unlicensed frequencies. This also helps offload Wi-Fi traffic in congested wireless LANs. Applications could range from residential broadband to in-flight connectivity, where every seat already has a built-in light source above.

Li-Fi also enhances localisation and asset tracking thanks to its small coverage area. Its higher data density (data rate per unit area) outperforms RF, making it ideal for precise asset monitoring or indoor navigation.

However, Fleschen emphasises that LC and Wi-Fi are fundamentally complementary, not competitive. "The strategic objective is not to replace Wi-Fi but to create a more robust, secure, and versatile communication ecosystem by integrating LC where its unique strengths provide optimal value," he says.

INDIA'S LI-FI OPPORTUNITY TAKES SHAPE

India's rapidly expanding digital infrastructure provides fertile ground for experimenting with light-based communication. The government's focus on 5G, smart cities, and digital inclusion is also stimulating interest in emerging wireless alternatives that can extend broadband to areas where RF networks are either congested or impractical.

Several pilot projects are exploring Li-Fi for classrooms, rural health centres, and underground facilities where fibre or Wi-Fi coverage is limited. The technology's immunity to electromagnetic interference and ability to confine data within a physical boundary make it particularly suited to defence, aviation, and healthcare environments.

Experts note that Li-Fi's high data density and spatial reuse could help address India's persistent last-mile and indoor-coverage gaps. By combining Li-Fi with optical-fibre backbones and 5G networks, service providers could deliver low-latency broadband to high-density zones—without additional spectrum-licensing costs.

However, the path to adoption remains steep. Industry leaders point out that Li-Fi needs strong policy support, cost-effective components, and standardised integration into Wi-Fi ecosystems before it can scale. Still, India's optical-fibre footprint, semiconductor push, and Make in India initiatives may create a conducive environment for local Li-Fi manufacturing and R&D over the next few years.

TRIALS THAT LIT THE WAY FORWARD

Li-Fi first captured global attention when Prof Harald Haas, Chair of Mobile Communications at the University of Edinburgh, coined the term during his TED talk in 2011. His company went on to launch the first commercial Li-Fi systems at MWC Barcelona in 2014. Since then, adoption has been fragmented but steadily expanding.

In the UK, mobile operator O2 conducted a pilot with pureLiFi, installing nine Li-Fi-enabled LED bulbs in its Slough headquarters. The system allowed data to be transmitted via light, creating a bi-directional, high-speed, fully networked communication setup simply by modulating bulb brightness.

In Spain, ADIF, the state-owned railway infrastructure manager, trialled Li-Fi at Málaga's María Zambrano station to complement 5G, where Wi-Fi signals typically degrade.

In the Netherlands, the Dutch armed forces explored Li-Fi through KIXS (part of JIVC) in collaboration with TNO and Trulifi by Signify. For military operations in remote locations where traditional networks face logistical constraints, Li-Fi offered a compelling alternative. It was tested for secure rooms, ammunition bunkers, and Fast Field Data Links, where a broadband link across runways was established in ten minutes, delivering 50 Mbps—without any cables.

Because Li-Fi uses only a light beam, it meets aviation-safety regulations and cannot be intercepted, jammed, or tracked beyond the light cone. "As Li-Fi works via light and does not cause radio interference, we have proved its great value for the Dutch armed forces," said Lt Col Harm de Jong, senior officer at KIXS. "The

> Li-Fi's unmatched speed, safety, and spectrum freedom make it a vital complement to Wi-Fi and cellular networks in the evolution towards 6G and beyond.

next step is to integrate Li-Fi into our IT standards and processes."

For defence use, Li-Fi can be installed in tents or field posts using simple fixtures and accessed securely with USB keys, offering a quick, cable-free solution to mission-critical communication needs.

CHALLENGES ON THE HORIZON

Despite the optimism, Li-Fi is not yet a mainstream technology. Its ecosystem, standards, and cost structure still need consolidation before widespread adoption. Wi-Fi, equipped with powerful antennas and higher transmit power, still offers superior range.

According to the Light Communication Alliance Annual Report 2022, Li-Fi standards need both pace and ecosystem coordination for smooth growth. The initial Draft 1.0 of the IEEE 802.11bb specification was submitted to the working group for approval, defining the LC spectrum from 800 nm to 1,000 nm to ensure interoperability between systems. It also proposed that all 802.11bb devices reuse existing 802.11 PHY modes and chipsets—a design choice expected to accelerate adoption by leveraging the Wi-Fi supply chain.

The standard, officially ratified in June 2023, marked a pivotal moment for the industry. Fleschen calls it a "monumental achievement" that strategically positions Li-Fi as a complementary and integrated technology alongside Wi-Fi. "For the first time, Li-Fi solutions can exist inside the Wi-Fi ecosystem, enabling seamless coexistence and interoperability with existing wireless infrastructures," he says.

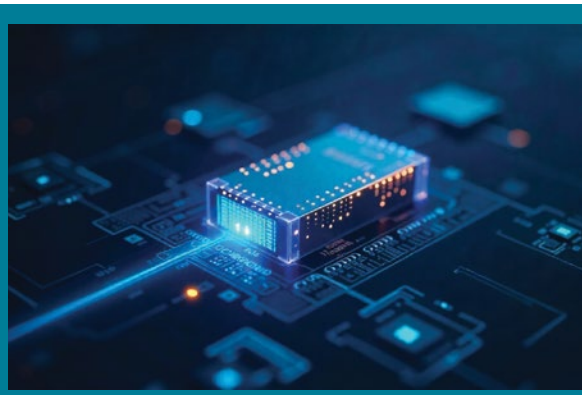
Still, challenges remain. "Li-Fi requires a clear line of sight between transmitter and receiver," Fleschen adds. "Physical obstructions such as walls will block light signals. While this restricts coverage, it is also Li-Fi's greatest security and interference-immunity advantage."

WIRED OPTICAL EDGE

Wired optical systems—such as Passive Optical Networks (PONs) and optical ring architectures—form the foundation of today's high-capacity, energy-efficient infrastructure.

- **Energy efficiency and sustainability:** Passive Optical LANs can cut electricity use by up to 82 per cent versus Ethernet LANs. Optical rings reduce power needs by 69 per cent, while FTTH (PON-based) consumes just 5 kWh per line compared with 15 kWh for ADSL and 50 kWh for 3G/4G.
- **High Capacity and Scalability:** Optical fibres deliver multi-Gbps access and Tbit/s throughput; upgrades require minimal hardware change, ensuring long-term scalability.
- **Lower TCO:** Passive optical LANs cut both CAPEX and OPEX, offering a more sustainable investment than traditional Ethernet LANs.
- **Longevity and eco-design:** Fibre networks last ~50 years, inherently eco-designed to reduce environmental footprint over time.
- **Transparency and low latency:** Optical Add/Drop Multiplexer (OADM) technology limits OEO conversions, lowering energy use and latency across metro and core networks.
- **Service support:** Optical ring topologies enable emerging services such as M2M communication through efficient broadcast-and-select techniques, supporting Industry 4.0 automation.

> Li-Fi must strengthen its standards, ecosystem, and cost structure for wider adoption, while Wi-Fi remains dominant with superior power, range, and reliability.



WIRELESS OPTICAL EDGE

Wireless optical technologies—Li-Fi and Optical Camera Communication (OCC)—extend the optical ecosystem to the network edge, combining flexibility with energy efficiency.

- **Energy reduction:** Li-Fi and OCC help lower end-to-end communication energy use, complementing wired optical backbones.
- **High speed and mobility:** Li-Fi provides Wi-Fi-like mobility and handover, achieving very high data rates through the light spectrum.
- **Enhanced security:** Because light cannot penetrate walls, Li-Fi ensures superior physical-layer data protection—ideal for sensitive or confined environments.
- **EM-safe operation:** Li-Fi supports communication in electromagnetic-sensitive zones such as hospitals or nuclear facilities where RF signals are restricted.
- **Indoor positioning:** OCC uses smartphone cameras for precise indoor geo-mapping and location-based services in large venues.
- **Compatibility and adoption:** OCC works with most smartphones and existing LED lighting, enabling low-cost, large-scale deployment in public and commercial spaces.

Ecosystem readiness, standardisation, and cost of hardware—particularly laser-based transmitters—remain hurdles that manufacturers and regulators must address collaboratively.

Even as Li-Fi moves toward maturity, research continues to push boundaries in optical communication. Innovations such as ultrasonic beams from 3D-printed metasurfaces are being tested to create localised sound pockets—inaudible to bystanders but useful for secure speech zones or personalised audio in vehicles and public spaces.

Similarly, metasurfaces using nanomaterials can now split a single light beam into multiple directions, offering a glimpse of how next-generation optical systems might evolve. These developments indicate that the future of communication may extend beyond Li-Fi, towards hybrid optical–acoustic models.

Drawing an analogy from history, when Edison's bulb brightened the world, it was not his alone—Joseph Swan had lit the way earlier, and tungsten filaments later transformed the bulb's efficiency. Likewise, Li-Fi may only be at its bamboo stage, awaiting its own 'tungsten moment' to propel it into everyday use.

Li-Fi represents more than just another connectivity technology. It symbolises a paradigm shift—moving communication literally into the light. It holds immense promise for niche environments where security, bandwidth, and electromagnetic compatibility matter most.

While Wi-Fi and cellular networks will continue to dominate mainstream connectivity, Li-Fi's specialised strengths—speed, safety, and spectrum freedom—make it a critical complement in the evolution towards 6G and beyond.

It may not yet be the light sabre that slays Wi-Fi, but it is certainly the next bulb in the series—shining a little brighter, faster, and smarter each time. And perhaps, like Edison's spark, it will illuminate not just our rooms but the very future of connectivity.

pratimah@cybermedia.co.in

Beyond VPN: Building trust into network access

As cyberthreats grow more complex, enterprises are shifting from VPNs to ZTNA to achieve secure, scalable, and context-aware access for remote users.

BY NAHIM FAZAL

In today's rapidly evolving digital landscape, securing an organisation's network has become more critical than ever. While traditional methods such as Virtual Private Networks (VPNs) have been the go-to solutions for remote access to corporate resources, security architects have been facing scalability challenges with these solutions.

With cyberthreats becoming increasingly sophisticated and the demand for seamless, secure connectivity growing, it is time to consider a more robust alternative: Zero Trust Network Access (ZTNA). Implementing ZTNA over traditional VPNs offers significant security, usability, and operational advantages, especially in today's cloud-centric, remote work environments.

> VPNs may connect users, but ZTNA connects them intelligently—verifying identity, context, and intent before granting application access.

> The shift from VPNs to ZTNA marks a decisive move toward adaptive, context-driven security built for today's distributed workforce.

By replacing traditional VPNs with ZTNA, security leaders can enhance their organisation's security, improve the user experience, and support the dynamic needs of an enterprise workforce.

However, there is a popular misconception among organisations that implementing ZTNA means they are deploying zero trust and do not need to take any further action. ZTNA is not zero trust; it is one component of a zero-trust architecture. According to Gartner, ZTNA refers to products and services that create an identity- and context-based logical access boundary that encompasses an enterprise user and an internally hosted application or set of applications.

ZTNA creates a logical access boundary around the applications, hiding them from discovery and restricting access to a set of named entities. The policy enforcement point verifies the identity, context, and policy adherence of the specified participants before granting access, thereby minimising lateral movement across the network.

IMPROVED SCALABILITY, DISTRIBUTED CONTROL

Unlike traditional network-based tunnelling methods such as VPNs, the ZTNA architecture uses Policy Enforcement Points (PEPs) that sit closer to applications, regardless of where those applications are hosted. This distributed design helps reduce latency, improve traffic efficiency, and enhance scalability. Because the number of PEPs can be dynamically adjusted based on network requirements, ZTNA is particularly well-suited to modern distributed environments spanning both on-premises and cloud infrastructures.

Within a ZTNA framework, PEPs perform several essential functions. They control access by ensuring that only verified users can reach preapproved applications and resources. They also enforce organisational security policies in real time, maintaining compliance and consistency across multiple environments.

Continuous monitoring is another vital function, enabling the detection of abnormal user activity

IN BRIEF

- Traditional VPNs face scalability and visibility challenges as networks expand across cloud and on-premises environments.
- ZTNA uses distributed policy enforcement and decision points to manage access closer to applications, reducing latency and improving performance.
- Applying the zero-trust principle of "never trust, always verify" minimises lateral movement and limits the impact of compromised credentials.
- Least-privilege access ensures users can access only the applications or data necessary for their role, reducing the attack surface.
- Continuous logging and monitoring enhance visibility into user behaviour and support compliance and forensic investigations.
- Secure storage of log data is critical for accountability and regulatory adherence in zero-trust deployments.

> By integrating access control, monitoring, and policy enforcement, ZTNA delivers the resilience and precision that traditional VPNs lack.

or potential threats as they occur. In addition, PEPs integrate seamlessly with identity and access management systems, ensuring that user authentication and policy retrieval are handled securely and efficiently. Together, these capabilities make PEPs the backbone of a scalable, secure, and adaptive ZTNA deployment.

Working in conjunction with the PEP is a policy decision point (PDP). The PDP evaluates access requests against security policies. It determines whether a user or device should be granted access to a specific application or resource based on the policies in place.

It also considers various contextual factors, such as user identity, device health, location, time of access and other attributes, to make informed decisions. This provides a centralised point for managing and enforcing access policies, ensuring consistency and compliance across the organisation.

The role of the PEP is to act as a gatekeeper, allowing or blocking connections based on the risk scoring provided by the PDP. The algorithms and logic used to make policy decisions are stored in the policy engine.

To address scalability challenges, a resilient PDP architecture must handle a large number of requests. Therefore, a distributed architecture is implemented.

ZTNA can overcome the scalability challenges posed by VPNs by establishing one-to-one connections to specific applications rather than relying on broad tunnelling.

LIMITING EXPOSURE THROUGH LEAST PRIVILEGE

ZTNA is based on the zero-trust principle: "never trust, always verify." This means that, regardless of the source of the connection, a consistent set of policy controls will be applied. This, when combined with least privilege, ensures that users are granted access to only the resources on that network they absolutely need. Once granted access, they have the minimum privileges applied when interacting with those resources.

If an attacker compromises a user's identity, their ability to move laterally is severely constrained, as they will have access only to the resources approved for that identity. ZTNA grants access on a per-application basis, unlike traditional VPNs that provide broad network access, making network reconnaissance by attackers much more difficult.

However, it is critical that additional security controls, such as the principle of least privilege, are used to supplement ZTNA to prevent an attacker from reaching critical data if that is the attacker's strategic objective.

ACHIEVING DEEPER VISIBILITY AND CONTROL

Traditional VPNs provide limited insight into user activity. Once traffic exits the VPN server and enters the internal network, the VPN no longer tracks or logs actions, leaving administrators blind to what users do beyond the initial connection. In contrast, PDP in a ZTNA framework continuously logs all access requests, policy evaluations, and security decisions. This comprehensive visibility strengthens oversight and accountability across the network.

Many organisations struggle with incomplete user-to-application mapping in their existing deployments. During the initial phase of ZTNA implementation, logging becomes a crucial tool for identifying which users are accessing specific applications and resources. These insights form the foundation for building precise policy controls that restrict access based on verified identities and contextual parameters.

The expansion of logging capabilities, however, introduces a need for secure data storage. Log data, while essential for compliance and auditing, must be safeguarded to prevent misuse or tampering. When managed properly, these detailed records provide organisations with the enhanced visibility and control that traditional VPNs cannot offer.

The author is a Senior Director Analyst at Gartner.
feedbackvnd@cybermedia.co.in

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:** M M Y Y Y Y

Organisation: _____ **Designation:** _____

Delivery Addess: _____

_____

City: _____ **State:** _____ **Postal Code:** _____

Mob [•]: _____ **Tel:** _____ **Email [•]:** _____

GST No. [•]: _____ **PAN No. [•]:** _____

☐ **I am paying ₹** _____ **by DD/Cheque No.:** _____ **Dated:** M M Y Y Y Y

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:** M M Y Y Y Y **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

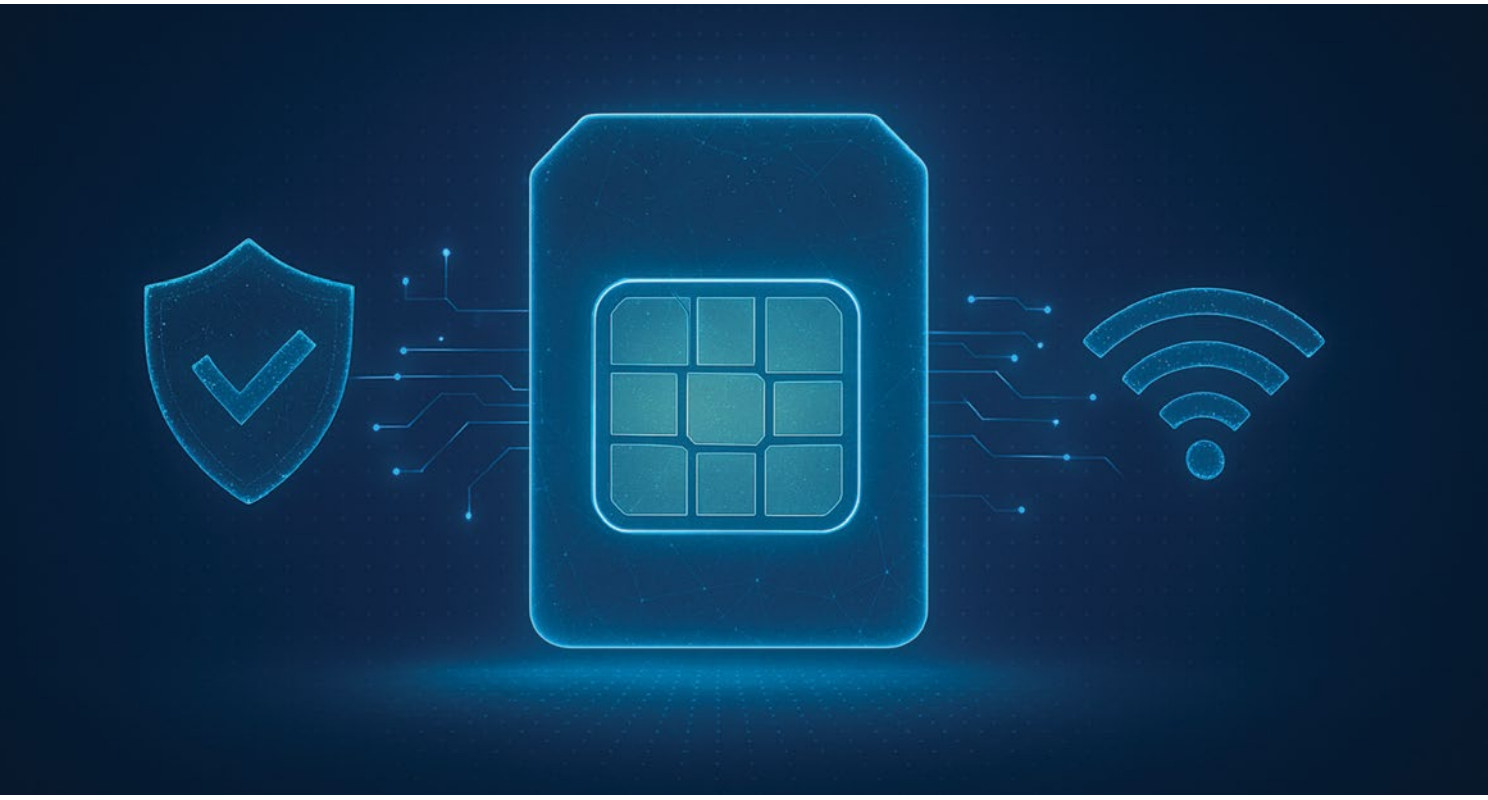
For Subscription queries:
9289870545

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.

Invisible SIMs, smarter security, stronger connectivity

As eSIMs and iSIMs scale from smartphones to massive IoT, convenience rises—and so do digital threats—demanding default-on security and disciplined use.

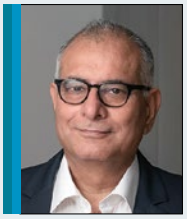


BY PRATIMA HARIGUNANI

There is the OG Don—the 1978 one—and there is the one that followed in 2006. What is the biggest difference between the two? Wait. Pause before you blurt out the names of Amitabh and Shah Rukh. If you think for a moment longer, you may recall that both the cops and the goons were chasing a diary in the first one—something that flew through the air more than once and had its own volleyball moments between good guys and criminals alike.

That red diary was replaced by a thin, sleek CD in the next Don. And as the world moves deeper into software, AI, and invisible data, who knows — someday the goons and the cops might be after a quantum wave. Floating in

> From chips to code, the SIM has gone invisible—bringing sleek form factors and global scale, but demanding default-on security and relentless monitoring.



"Software-only ecosystems remain prone to cyberattacks and misuse unless anchored with strong cryptography, secure elements, and trusted execution."

RAHUL TANDON
Senior VP – Connectivity Services, India, IDEMIA Secure Transactions

the air, full of data, and impossible to touch. That would make quite a film.

But would the central plot really change? Does invisibility, intangibility, and omnipresence make things easier for the good guys—or actually help the bad ones? Enterprises cannot afford to leave this as a blind spot, especially as eSIMs, iSIMs, and AI-driven devices are redefining mobility, connectivity, and security. With employees' phones and IoT devices carrying corporate data, and eSIMs becoming the next node in the IoT chain, businesses must ask: has anything really changed with this new kind of SIM?

A lot, particularly in terms of convenience, flexibility, and mobility. As for security, that story is only getting more layered.

NO POCKET FOR PICKPOCKETS

We have all inserted that small chip at some point—the ubiquitous SIM, short for Subscriber Identity Module. It is the integrated circuit on mobile devices that stores essential data, such as the International Mobile Subscriber Identity, authentication keys, and subscriber credentials.

Until recently, these chips were physical, growing smaller as devices grew smarter. Then came eSIM—the embedded SIM—and now iSIM, or integrated SIM. The difference? These new versions live directly inside the device. No trays, no swapping, no lost chips. They are activated digitally and do not need physical handling, solving one of the biggest hassles of global mobility: managing multiple SIMs while roaming.

"eSIM and iSIM are both milestones in the evolution of SIM technology," explains Sachin Arora, Head of Connectivity and IoT, Giesecke+Devrient India. "An eSIM is a dedicated chip embedded in the device, whereas an iSIM is integrated directly into the device's System-on-Chip (SoC) alongside the processor and modem. This makes iSIM far more compact and efficient."

From a hardware standpoint, eSIMs already reduce the device footprint, but iSIM goes further—saving space, reducing power consumption, and simplifying manufacturing. That is crucial for wearables, industrial sensors, and compact IoT devices, Arora notes.

Shirsanka Saha, Consultant for eSIM, OTA, and IoT SIM compliance, explains the difference succinctly: "A physical SIM is a removable smart card with subscriber identity and authentication keys. An eSIM, or embedded Universal Integrated Circuit Card (eUICC), is a hardware element embedded in the device, but its SIM profile—the network credentials and carrier identity—is provisioned over the air. The eSIM profile is software-managed and cannot be manually swapped."

Replacing physical SIMs with embedded versions also gives device manufacturers more design flexibility. Rishi Padhi, Principal Research Analyst at Gartner, says, "It enables better control over form factor and component placement—for foldables, it enhances design; for wearables, it supports miniaturisation. The latest Apple iPhone 17 series gained over 250 mAh of battery capacity because the SIM tray space was redeployed for battery components."

The evolution is not limited to consumer electronics. Industrial IoT, smart utilities, connected cars, and logistics networks are adopting eSIM for its scalability and remote provisioning capabilities. It is a paradigm shift where connectivity itself becomes programmable.

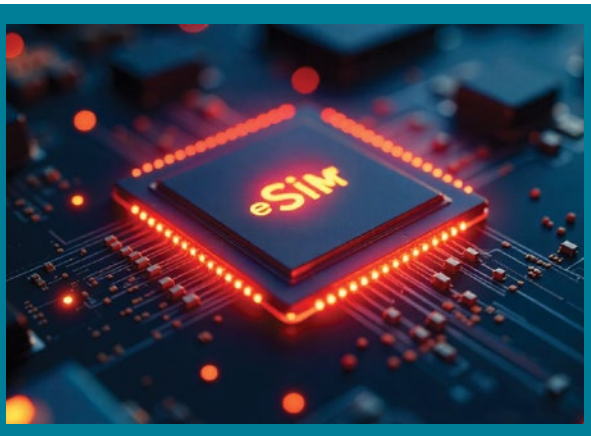
But flexibility raises an important question: Does it come at the cost of security?

BUILT-IN SECURITY: HARDER TO STEAL

Technically, eSIMs and iSIMs are much harder to steal or tamper with than physical SIMs. They employ advanced encryption protocols, hardware-level security, and remote provisioning systems designed as per GSMA standards such as SGP.22 (Consumer eSIM) and SGP.32 (IoT eSIM).

"Embedded, software-driven solutions like eSIM expand attack surfaces and risks—especially when users rush to connect at any cost."

CHOON HONG CHEE
Head, Consumer Channel – APAC, Kaspersky



THE HERO SIDE

- Secure over-the-air (OTA) provisioning and remote activation
- Tamper-resistant hardware with embedded cryptographic protection
- Multi-network flexibility without physical swapping or cloning
- AES and TLS encryption ensure strong device–carrier authentication
- Built-in security elements reduce fraud and traceability gaps
- Miniaturisation improves efficiency and limits physical vulnerabilities

They use Transport Layer Security and encryption algorithms such as the Advanced Encryption Standard, along with tamper-resistant Secure Elements. Public Key Infrastructure ensures strong identity verification between devices and carriers, while remote provisioning frameworks allow profiles to be downloaded, updated, or revoked securely.

Because eSIMs rely on digital authentication, they inherently reduce fraud. With encryption between the device and carrier, interception becomes almost impossible. Digital footprints make every activity traceable, improving network visibility for enterprises.

"Both eSIM and iSIM support remote SIM provisioning," Arora notes. "While eSIM uses a dedicated secure element, iSIM integrates the same functionality within the SoC. This maintains carrier-grade security while offering the scalability required for massive IoT adoption."

Padhi elaborates further: "The eUICC is tamper-resistant and permanently fused into the mainboard, providing stronger protection than removable SIMs. GSMA's Remote SIM Provisioning standards govern how profiles are securely managed and authenticated, establishing a robust, standardised defence layer."

Saha adds that digital provisioning also reduces supply chain vulnerabilities: "Physical SIMs can be intercepted or tampered with during shipment. eSIM provisioning is digital, minimising such risks. Enterprises can activate or deactivate eSIM profiles remotely, even across borders. Lost or compromised devices can be disabled instantly."

In large organisations, these capabilities translate into operational efficiency. Global firms can deploy hundreds of devices with pre-configured network profiles, update them over-the-air, and track compliance.

But as the locks evolve, the burglars do not quit—they get smarter.

NEW LOCKS, NEW HACKERS

Are eSIMs safer than their plastic predecessors? The answer is nuanced.

"The marketing narrative emphasises that eSIMs are more secure since they cannot be removed from stolen devices," Padhi says. "However, the risk shifts from

"OEMs must make strong security defaults—like MFA, SIM-change locks, and port-out protections—mandatory for all user accounts."

RISHI PADHI
Principal – Research, Gartner

physical theft to digital manipulation—cloning, spoofing, SIM swap attacks, and OTA backdoors."

Rahul Tandon, Senior VP, Connectivity Services, IDEMIA Secure Transactions, agrees: "The rise of eSIM and AI-rich devices redefines connectivity and convenience but also expands the threat landscape. It demands a future-ready trust framework to ensure long-term resilience."

Vivek Srivastava, Country Manager, Fortinet India and SAARC, adds: "Mobile devices have become pocket-sized computers. They must be secured so that they do not become an entry point for cybercriminals into enterprise systems."

Recent research from Security Explorations found vulnerabilities in certain eUICC implementations—linked to older Java Card flaws—that could be exploited to extract digital keys or install malicious OTA payloads. These require brief physical access but highlight potential weak spots in some vendor stacks.

SIM hijacking remains another persistent threat, where attackers trick carriers into transferring numbers to new profiles. Fake QR codes, eSIM data breaches at carrier endpoints, and even the throttling of eSIM profiles by unauthorised intermediaries have emerged as concerns.

Still, experts note that the encryption standards in eSIMs remain robust. Jim Handy, Semiconductor Analyst at Objective Analysis, reassures, "SIMs and eSIMs employ military-grade cryptography. Breaking these codes would need immense computing power, possibly quantum systems. As of now, AI or supercomputers cannot realistically breach them. The weakest link remains user negligence."

Choon Hong Chee, Head of Consumer Channel, APAC, Kaspersky, concurs as he says, "From a technical standpoint, eSIMs are more secure than physical SIMs. But that security depends on encryption, robust KYC, and user awareness. Greater convenience often comes with greater exposure."

THE VILLAIN SIDE

- Prone to malware, phishing, and social-engineering exploits
- Risk of OTA backdoors enabling silent data interception
- "Bricking" or disabling attacks that corrupt eSIM firmware
- Cloning, spoofing, or SIM-swap attacks via stolen certificates
- Throttling or hijacking of eSIM profiles by rogue operators
- Jurisdictional exposure through cross-border data routing

MORE SOFTWARE, MORE SOFT TARGETS

Would more convenience, flexibility, and AI-driven connectivity mean more fragility? Quite possibly.

Tandon warns: "These features improve the user experience but also expand the attack surface. As hardware gives way to software ecosystems, the trust layer must be

"Mobile security must guard the OS through sandboxing, permission controls, and app isolation to block unauthorised system access.."

VIVEK SRIVASTAVA
Country Manager, India & SAARC, Fortinet

stronger than ever. Without robust cryptography, trusted execution environments, and secure elements, software-only systems are open to exploitation."

Handy simplifies it further, "The biggest risk is not the technology—it is people. Password hygiene, access discipline, and common sense remain the best defences. AI simply magnifies the speed and scale of potential abuse."

AI also brings fresh risks like bias, data misuse, and adversarial attacks if not governed properly. Tandon highlights that IDEMIA integrates identity, device, and transaction-level protection using GSMA-certified eSIM management, continuous DDoS monitoring, and post-quantum cryptography to future-proof transactions.

Arora underlines the need for collaboration: "Operators must proactively engage policymakers to update privacy and data laws. Investments in secure-by-design architectures are essential."

Chee points to practical steps: "Our Kaspersky eSIM Store merges flexibility with security—allowing users to pre-activate plans, monitor usage, and avoid risky public hotspots."

Padhi notes how OEMs are also embedding trust at the silicon level: "Companies like Apple, Google, Qualcomm, and Samsung use proprietary Trusted Execution Environments such as Secure Enclave or Knox Vault. These create hardware roots of trust, anchoring encryption deep in silicon and extending it through the software stack."

Tandon adds that post-quantum cryptography will be vital to protect future eSIM transactions once quantum computing becomes mainstream.

Still, Padhi identifies a behavioural challenge. "Security opt-ins fail due to user fatigue. Protections should be the default, requiring users to opt out instead. It is a small policy change that can transform security across the board," he points out.

THE ENTERPRISE EQUATION

For enterprises, eSIMs are both a gift and a responsibility. They simplify global mobility, streamline provisioning, and integrate seamlessly into unified device management platforms such as Mobile Device Management and Unified Endpoint Management. Remote onboarding and instant activation reduce friction for distributed teams and IoT rollouts.

eSIMs also bring traceability—every activation, update, or deactivation leaves a digital record, making compliance audits easier. When combined with Zero Trust frameworks, they enhance visibility into every device connected to the corporate network.

But enterprises must also factor in the risk of rogue provisioning, compromised profiles, and insider misuse. Continuous monitoring, multi-factor authentication, and eSIM lifecycle management become critical pillars of enterprise security. With India's growing 5G infrastructure, these technologies will soon play a role in smart factories, connected cars, and Industry 4.0 ecosystems—each demanding secure, programmable connectivity.

EMBRACING FLEXIBILITY, GUARDING VIGILANCE

Security with eSIMs and iSIMs does not vanish; it evolves. The same tightrope — only higher, with stronger winds.

As Don once said, he may forget to greet his friends, but he never forgets to keep an eye on his enemies. That is exactly what enterprises must do: embrace the flexibility and intelligence of next-generation connectivity, but never turn their backs on the new-age hackers waiting in the dark.

The red diary may be gone, but the red pill remains.

pratimah@cybermedia.co.in

DATAQUEST 40+ YEARS THE BUSINESS OF INFOTECH

CyberMedia

DATAQUEST OCTOBER 2025 EDITION: THE GCC BOOM: INDIA'S JOURNEY FROM COST ARBITRAGE TO INNOVATION

ALSO READ MORE ON

- Bengaluru leads india's gcc story as karnataka builds future-ready talent - Priyank Kharge, Government of Karnataka
- Can GCCs Survive in the Deglobalization Era?
- Technology Vs. Cancer. Pound for Pound!
- Inside Wipro's Innovation Network: CTO Sandhya Arun on Ethics, AI-First Delivery
- Hitting 'Reset', Risking 'Reboot' – VMware's Bold Leap - Prashanth Shenoy, Broadcom

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

#ImpactingICTfor4Decades

For Subscription queries:
subscriptions@cybermedia.co.in
9289870545

Leverage Dataquest platform & network
Ajay Dhoundiyal | ajaydh@cybermedia.co.in | +91 99535 40318

Reimagining Earth through a living digital twin

A new geospatial alliance led by Aechelon seeks to build a real-time digital twin of Earth, merging satellite, radar, and AI for dynamic intelligence.

BY SHUBHENDU PARTH

California-based synthetic reality platform company Aechelon Technology has announced Project Orbion, an initiative to create a dynamic, real-time Digital Twin of Earth. Developed in partnership with Niantic Spatial, ICEYE, BlackSky, and Distance Technologies, the project aims to combine complementary technologies to build a platform that could eventually support both defence and civilian applications.

The idea is not simply to map the world but to reimagine how it might be seen, understood, and acted upon. Aechelon describes Orbion as a "living synthesis" of satellite imagery, radar intelligence, video photogrammetry, and AI—reconstructed into a three-dimensional view of Earth that would remain in motion, complete with live weather and physics.

The ambition is to move beyond static mapping towards a dynamic model that responds in real time to the changing conditions of the planet.

GPS LIMITATIONS: A TRIGGER FOR PROJECT ORBION

Since its deployment in 1995, the Global Positioning System (GPS) has been the backbone of navigation, from smartphones to aeroplanes to shipping. But GPS was built for a different era. Its accuracy is limited by environmental factors such as weather and urban density, and its updates are never truly real-time.

As Michael Wollersheim, analytical director at ICEYE, explained: "Once you have a fragment of data, it starts to degrade immediately." This delay may be acceptable for everyday navigation but not for high-

> Project Orbion signals a shift from static mapping to continuous planetary awareness, fusing geospatial and AI intelligence in real time.

stakes environments—such as disaster zones, military operations, or autonomous systems requiring split-second precision.

Project Orbion, according to Aechelon, is designed to address these gaps by offering a model that could reflect the Earth as it is in the present moment, not as it was minutes or hours earlier. In many ways, it is an attempt to build what GPS cannot: a digital twin that is dynamic, detailed, and globally accessible.

TECH USE: AI, RADAR SATELLITES, GEOSPATIAL DATA

Each partner brings a critical piece of technology to the table. Aechelon, known for its defence simulation systems, plans to integrate its Synthetic Reality platform to fuse multiple data streams into photorealistic global environments. ICEYE would add radar satellites capable of imaging through clouds, smoke, and darkness, a feature that could prove vital for responding to wildfires, floods, or combat operations obscured by weather.

Similarly, Niantic Spatial brings its geospatial reconstruction expertise and intends to integrate its forthcoming Visual Positioning System (VPS), designed to deliver centimetre-level localisation in GPS-denied environments. This would allow emergency teams operating in crisis or electronic warfare zones to navigate with precision.

Given that Project Orbion would generate vast amounts of information, BlackSky's role is to manage the scale of incoming data. Its AI-driven architecture is intended to filter and analyse large volumes of imagery, converting raw feeds into actionable insights. Distance Technologies, meanwhile, is developing 3D light-field displays that could render this complex intelligence into intuitive visuals, supporting training, battlefield operations, and augmented reality.

In short, the five companies aim to combine their respective strengths to build a planetary map that is not only accurate but also usable under the most demanding conditions.

DEFENCE, DISASTER RESPONSE AND ENTERPRISE APPLICATIONS

While defence is a key focus, Project Orbion is being designed for broader use. In conflict situations, the platform could enable near real-time tracking of troop movements and battlefield conditions. In peacetime, it may help improve disaster management, global shipping operations, and urban planning. By fusing "ground truth" data with AI, Orbion may eventually train both human operators and autonomous systems with a level of precision that is not possible today.

Aechelon Co-Founder and CTO Nacho Sanz-Pastor underlined how the initiative builds on the company's history of simulation technologies. "The challenge has always been keeping pace with changes in the physical world and training humans and autonomous systems with realistic worldwide information. Project Orbion addresses applications that until now were just in the realm of science fiction."

Niantic Spatial CTO Brian McClendon pointed to potential benefits for emergency services: "Geospatial understanding unlocks a new level of situational awareness that allows teams to plan and execute missions with greater confidence and safety."

In fact, the companies aim to expand the concept of digital twin, primarily associated with manufacturing and urban design, to encompass the entire planet. By merging ground-truth intelligence with AI-enabled processing, the project aspires to provide a continuously updated operational picture. For the defence sector, this could mean faster, more reliable mission planning and enhanced command capabilities. For enterprises, it may open the door to safer logistics, smarter infrastructure development, and more advanced risk management.

The ambition is clear: to establish a new global benchmark for geospatial intelligence and to move beyond the static limits of GPS. Whether Orbion achieves this will depend on how effectively its technologies are integrated, scaled, and sustained in practice.

shubhendup@cybermedia.co.in

NASA laser test proves deep space data transfer tech

NASA's Optical Communications demo shows lasers can beam data across deep space, opening new possibilities for Mars and beyond.

NASA's Deep Space Optical Communications (DSOC) demonstration has completed a nearly two-year-long experiment, validating the use of laser-based data transmission over interplanetary distances.

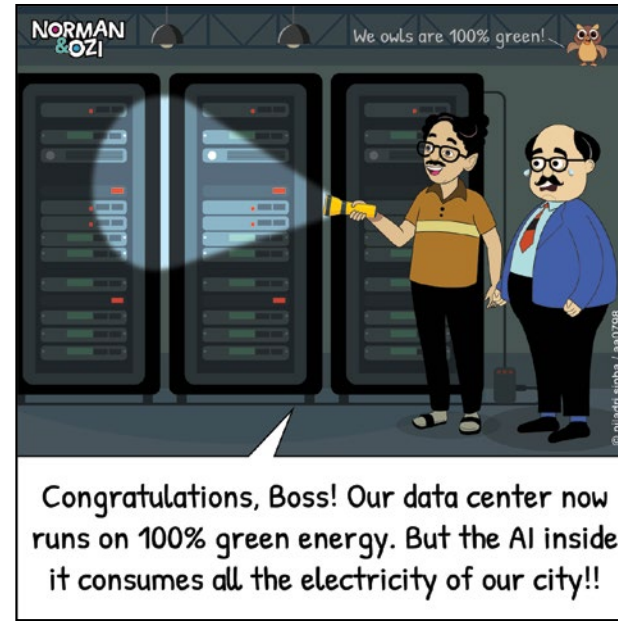
Launched aboard the Psyche mission in 2023, DSOC completed its 65th and final test pass by successfully sending and receiving laser signals over 218 million miles. The system established a link with the Psyche spacecraft just one month after launch and consistently transmitted data, achieving rates comparable to household broadband.

The project achieved a milestone on 11 December 2023 by streaming ultra-high-definition video from over 19 million miles at 267 megabits per second. It also set a new record in optical communication on 3 December 2024 by downlinking data from 307 million miles away. Across the demonstration, ground terminals received 13.6 terabits of data.

Managed by NASA's Jet Propulsion Laboratory, DSOC includes a flight laser transceiver on Psyche and two Earth-based ground stations. A 3-kilowatt uplink laser from the Table Mountain Facility guided Psyche's transceiver, allowing it to direct signals back to Earth with precise targeting — critical due to the vast distances and motion of both spacecraft and planet.

The Palomar Observatory served as the primary downlink station, using a 200-inch telescope to detect weak signals. A high-efficiency detector array decoded the data from faint photons. The system also tested a hybrid radio-optical antenna at the Deep Space Network's Goldstone complex and experimented with "arraying" techniques using multiple telescopes to increase signal reliability.

The DSOC demonstration is part of a broader initiative by NASA's Space Technology Mission Directorate and the Space Communications and Navigation program to prepare for data-intensive missions to the Moon and Mars.



PCQUEST

CyberMedia

PCQUEST OCTOBER 25 EDITION - "CLICK, BUILD, REPEAT": THE RISE OF CITIZEN DEVELOPERS

ALSO READ MORE ON

- Who codes the coder now?
- The new blueprint of enterprise tech
- From pilot to production: The untold truth of enterprise GenAI
- 8 best Free AI video generator tools you can actually use in 2025
- Inclusive by design: How tech is reshaping accessibility
- Securing the Future of AI Infrastructure
- REVIEWS: HMD T21 tablet
- BenQ RD320U
- OnePlus Nord Buds 3r

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

RNI No. 59233/94. Published on 1st of every month. DL(s)17/3114/2021-23. Licensed to Post WPP. U(SE)62/2020
Posting Date: 13&14 of every month. Posted at Lodi Road HPO.
Advance Payment Facility Customer ID # 3000052248. Voice&Data Magazine Post DL (DS)-58/MP/2023-24-25

APEEJAY SCHOOL

Mahavir Marg, Jalandhar | Estd. In 1968

50+ Years of EXCELLENCE Since 1967 — APEEJAY EDUCATION

THE LEGACY OF 50+ YEARS OF EXCELLENCE CONTINUES

ADMISSIONS OPEN 2026-27

NURSERY TO IX & XI

Follow us on:

APEEJAY EDUCATION

Quality Education from Pre-Nursery to Doctoral level

5,000+ Educators & Staff Members

26 Educational institutions across the country

40,000+ Students

Apeejay School, Mahavir Marg, Jalandhar, Punjab–144001

KEY HIGHLIGHTS

- Value-based Holistic Education
- Curriculum aligned with NEP 2020
- State-of-the-art infrastructure
- Safe & Secure Campus
- Outstanding Results in CBSE and Competitive Exams

Admission Helpline:
+91-181-2453608 | 9311446232
Email:
skool.ms.jln@apj.edu