WHO PAYS FOR TRUST? UNPACKING DoT'S MNV FRAMEWORK | 10

₹100

www.voicendata.com

VOL 32 ISSUE 09 SEPTEMBER 2025

VOICE & DATA

Connecting the Digital World

CyberMedia

AI MEETS NETWORKS: SPARKS PREVENT FIRES

From blind date to foresight, AI and networks can now predict mishaps, prevent outages, and help operators stay ahead of the flames

"Light waves deliver security that radio waves cannot" 36

MARC FLESCHEN
Chairman, Light Communications Alliance

76 pages including cover

Special subscription offer on Page 62

Apeejay Institute of Mass Communication

Dwarka, New Delhi | Estd. in 2003 | AICTE Approved

50+ Years of EXCELLENCE Since 1967 — APEEJAY EDUCATION

Empowering Future Media Leaders with Expertise, Innovation, and Excellence!

ADMISSIONS OPEN 2025

PROGRAMMES OFFERED

FULL TIME 2 YEARS PROGRAM

- Management in Mass Communication

(CAT/MAT/XAT/GMAT/CMAT/ATMA Score Acceptable)

FULL-TIME 1 YEAR POST GRADUATE PROGRAMS*

- Television & Radio Journalism/Production
- Advertising & Marketing Communication
- Digital Media & Online Journalism
- Corporate Communication/ PR & Event Management
- Business & Financial Journalism

*Institute offers lateral entry option into 2nd year MA at Apeejay Stya University (UGC recognised) in accordance with UGC's choice based credit system.

PLACEMENTS IN TOP MEDIA HOUSES

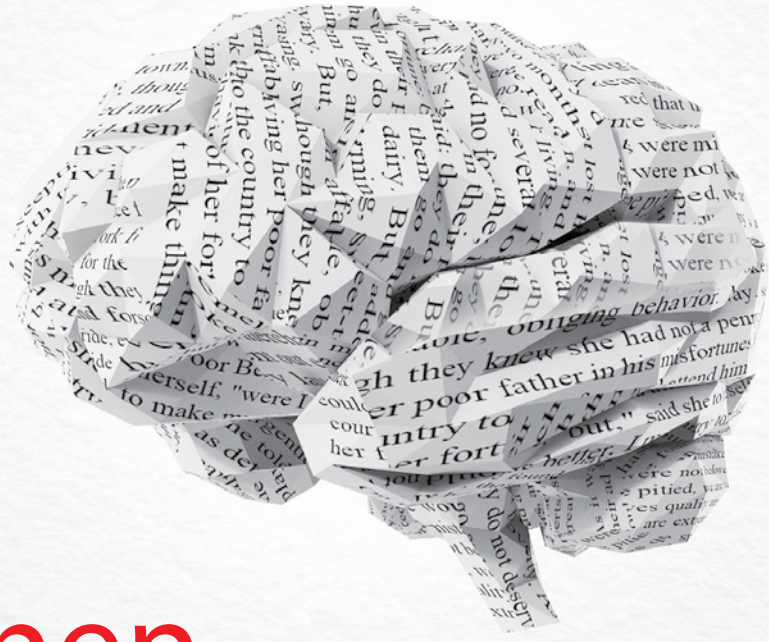
TIMES NOW, WUNDERMAN THOMPSON, newsX NEWS. NOT NOISE, Radio City A JAGRAN INITIATIVE, Edelman, inshorts stay informed, REPUBLIC TV, NEWS NATION, Network 18, TBWA\, McCain, 94.3 MY FM, ADFACTORS PR Knowledge-driven communications, Burson and many more

Excellent Placement Record across various media & entertainment platforms in over 100 reputed companies.

For more information, please contact us:

Apeejay Institute of Mass Communication
Institutional Area, Sector - 8, Dwarka, New Delhi - 110077
Admission Helpline: **+91-9910-222-777** | Email: **aimc.del@apj.edu**

Follow us on:



When print talks, the brain remembers.

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

Source: Study by TrueImpact (A Canadian neuromarketing firm)

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.

September 2025

[CONTENTS]

AI MEETS NETWORKS: SPARKS PREVENT FIRES

From blind date to foresight, AI and networks can now predict mishaps, prevent outages, and help operators stay ahead of the flames

MARC FLESCHEN
Chairman,
Light Communications Alliance

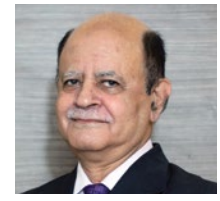
INDUSTRY SPEAK

NEWS ANALYSIS

COMMENTARY

OBITUARY/SUNIL RAJGURU

TELECOM TALK



USE CASE

TECHNOLOGY

REPORT

REGULARS

[NEXT ISSUE]

AUGUST 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

NEXT ISSUE

GREEN BY DESIGN

For any query: ajaydh@cybermedia.co.in

SHUBHENDU PARTH

[OPENING NOTE]

Hollow-core fibre could reshape telecom's physical layer

Inside a high-frequency trading floor, where nanoseconds delineate gain from loss, or across the fortified corridors of a command network, data must traverse vast distances swiftly and securely. Across much of the world, single-mode silica fibre has long served as the physical backbone of high-speed networks—a marvel in its time, but one now brushing against its physical limits.

The world now has its new contender: hollow-core fibre (HCF), which guides light not through glass, but through air.

Developed by researchers at the University of Southampton and Microsoft, the latest evolution—nested antiresonant nodeless fibre (DNANF)—has achieved a record-low attenuation of 0.091 dB/km at 1,550 nm. This surpasses the long-standing floor of conventional silica fibres, which rarely drops below 0.14 dB/km. By minimising leakage, surface scattering, and microbending losses, this design ushers in a new class of low-loss fibres suitable for both classical and quantum communication.

Technically, HCF marks a notable departure from photonic bandgap fibres and earlier Kagome-style designs. Unlike those, DNANF does not require intricate lattice arrangements to confine light. Instead, it relies on carefully nested tubes that support antiresonant guidance—simplifying fabrication while enhancing performance. Crucially, it avoids many nonlinear effects common in glass fibres, such as self-phase modulation and Raman scattering, making it ideal for high-power, long-distance links.

Conventional fibres use total internal reflection to contain light within a silica core. But silica, however refined, introduces dispersion, attenuation, and latency. In contrast, HCF uses air, where light travels nearly 50% faster. This translates to ~5 µs/km delay, compared to ~8.5 µs/km in solid-core fibres. In applications where low latency is sacrosanct—such as algorithmic trading, AI cluster synchronisation, and battlefield telemetry—this gain is not merely incremental; it is transformative.

Real-world deployments are already underway. Microsoft has integrated HCF into its Azure metro networks, enabling ultra-low-latency data paths. China Mobile reported 114.9 Tbit/s throughput across an HCF link between Shenzhen and Hong Kong. Relativity Networks, a US-based start-up, claims that HCF can extend inter-data-centre distances from 60 to 90 km without amplification—a potential boon for energy-constrained AI infrastructure.

HCF also presents distinct advantages for defence and secure communication networks. Its ability to transmit single-photon signals makes it a viable medium for quantum key distribution, offering future-proof encryption.

Its resilience to electromagnetic interference and reduced need for repeaters make it apt for long-range, low-visibility communication in high-threat and remote environments. The potential to deploy HCF in unrepeated subsea cables is also being explored, offering cost and reliability benefits by minimising the number of amplifiers required.

Yet, barriers remain. HCF is difficult to manufacture at scale, lacks industry-wide standards, and entails high cost. Nevertheless, its trajectory mirrors that of early fibre optics—once niche, now fundamental to global connectivity. To be clear, HCF will not supplant legacy fibre networks overnight. However, in domains where latency, reach, and signal fidelity are non-negotiable, it is poised to become not just a superior alternative but an indispensable one.

shubhendup@cybermedia.co.in

A voice of clarity, a life of quiet courage

Sunil Rajguru's words simplified complexity, his guidance shaped lives, and his quiet strength left an enduring mark on Indian journalism.

There are some people who become institutions within their own lifetime, not through grand gestures or loud proclamations, but through the quiet constancy of their presence. Sunil Rajguru was one such figure.

For colleagues, readers, and the many lives he touched, he was not merely an editor; he was an interpreter of complexity, a custodian of clarity, and above all, a companion on the journey of understanding a world that changes faster than words can capture.

On 1 September 2025, that steady voice was stilled. Sunil passed away at 14:30 IST, after a determined year-long struggle with cancer, leaving behind an irreplaceable void in the world of Indian technology journalism.

Sunil's career defied narrow labels. He could analyse the evolution of a chipset with the same ease with which he dissected a cricket match, reviewed a film, or conducted a spirited quiz.

A STORYTELLER WITH UNCOMMON COURAGE

What made Sunil singular was not simply his professional stature, but the extraordinary dignity with which he lived his final chapter. Even as his body fought a relentless illness, he refused to yield to despair. He worked on, breaking only for treatment, joining meetings with the same calm energy and conviction as if nothing in his world had changed.

When asked about his health, he would respond with a serene steadiness that reassured others more than himself: *"Dikkat to hai, per mai theek hun"* (Yes, there is a problem, but I am okay). His courage lay not in denial of pain but in his refusal to let it overshadow his purpose.

The poignancy of his last days is captured in one moment that one will never forget. On 7 August, he completed work on an edition of Dataquest. With deliberate grace, he lowered the screen of his laptop—a gesture uncharacteristic for a man who almost never shut it. "It is over," he said, quietly but firmly to his wife. That issue became his final bow, a legacy of commitment that will remain etched not just in print but in memory.

A LEGACY OF WARMTH AND WISDOM

Sunil's career defied narrow labels. He could analyse the evolution of a chipset with the same ease with which he dissected a cricket match, reviewed a film, or conducted a spirited quiz. His words carried both precision and playfulness, a rare combination that made him equally admired as a technology commentator and as a raconteur.

From his early days at Living Digital and IDC India to his stewardship of Dataquest and PCQuest, he built a reputation for making the difficult comprehensible, the abstract tangible, and the obscure accessible.

But it was his human qualities that left the more profound impression. Sunil was a mentor who never sought the title, yet shaped countless careers through a well-timed nudge, a word of encouragement, or the faith he placed in others. His laughter, gentle but infectious, could lift the weight of a newsroom's hardest day. His humility made him approachable; his generosity made him unforgettable.

He was never content to remain confined to the printed page. One of the early adopters of digital storytelling, he experimented with podcasts and video interviews, moderated discussions with wit, and anchored conferences with a balance of authority and warmth. He understood that journalism was not just about reporting but about building bridges between knowledge and people.

For his peers, he was more than a colleague; he was a reminder of what the profession could be at its best—curious without arrogance, rigorous without cynicism, serious about truth without ever losing a sense of humour.

AN UNFINISHED CONVERSATION

There is a haunting irony in losing a storyteller: every life he chronicled continues to live on, yet his own feels cut short, its narrative unfinished. And yet, in another sense, Sunil's story is still being written—in the memories of his colleagues, in the words he left behind, in the many voices he inspired to speak and to write.

His absence will be keenly felt in every meeting where his voice once steadied the room, in every page where his editorial hand brought order to chaos, in every conversation where his humour softened the hard edges of life. But his presence endures, woven into the fabric of the profession he loved so deeply.

Some lives are measured not in years but in the imprint they leave. Sunil Rajguru's life was one such, measured in clarity, generosity, and courage, quietly lived. He is survived by his mother, his wife, and his son, who carry forward his memory with love and pride. The screen of his laptop may have closed, but the story he told continues to echo, reminding us that true voices never really fall silent.

Who pays for trust? Unpacking DoT's MNV framework

India's MNV framework aims to fight fraud but may burden businesses and expose users to privacy risks in a rapidly digitising economy.

BY PUNEETH NAGARAJ & SHAILEJA VERMA

What began as a tool to bolster telecom cybersecurity may ultimately saddle businesses with compliance costs and expose users to privacy risks. The Department of Telecommunications proposed Mobile Number Verification (MNV) platform hints at a regulatory model where the private sector bears the brunt, while the financial and informational rewards accrue elsewhere.

Recently proposed amendments to the Telecommunications (Telecom Cyber Security) Rules, 2024 seek to regulate "telecom identification user entities" (TIUEs)—essentially any business that uses mobile numbers or other telecom identifiers to provide services or identify users.

Under the envisaged MNV framework, a TIUE may, either voluntarily or upon government direction, place a request to validate whether a mobile number provided by a user matches telecom service providers' (TSPs) databases. The goal: verify mobile number ownership. However, given the sweeping definition of a TIUE, the government could mandate even non-telecom entities to participate in the MNV platform. This raises concerns over regulatory overreach and significant privacy and financial implications for the broader digital ecosystem.

PRIVACY PROTECTION AND ITS BLIND SPOTS

The proposed cybersecurity amendments acknowledge the principle of 'purpose limitation' by stipulating that the MNV platform should only be used to validate users linked to a telecom identifier, and only for services tied to that identifier. However, they remain silent on the equally critical principle of 'data minimisation'. It is not yet clear whether the validation process will yield a simple binary response or also disclose additional personal information, such as the user's name or address.

This lack of clarity could result in the platform being misused by malicious actors seeking to mine or profile user data. The absence of mandated data minimisation, therefore, poses a substantial risk to user privacy.

DoT's proposed MNV system aims to validate users but may unlock a Pandora's box of privacy risks, financial strain, and regulatory overreach.

The amendments also require both TIUEs and TSPs to comply with the Digital Personal Data Protection Act, 2023. While this alignment is notable, there is little clarity on implementation. For instance, what happens if a user declines consent for a validation check initiated voluntarily by an online platform? This raises two critical questions: Can a digital service provider deny access if the user opts out of validation? And would such a refusal be used to draw adverse inferences, potentially affecting the user's access to services or their treatment on the platform?

WEIGHING THE FINANCIAL BURDEN ON BUSINESSES

Beyond privacy concerns, the MNV framework introduces a pay-per-verification model with fees ranging from Rs 1.50 to Rs 3 per request. While seemingly modest, these costs can quickly escalate if user verification is done at scale and frequency. For large digital platforms, this could mean a significant outlay—one likely to be passed on to consumers.

If this results in users losing access to free or freemium platforms, it could undermine the government's larger objective of promoting digital inclusion. Additionally, charging for what is positioned as a voluntary validation process may disincentivise participation, defeating the platform's core purpose of combating cyber fraud through broad uptake.

The revenue model appears designed to support the MNV platform's operational costs, with proceeds shared between the government and TSPs. Given the vast number of businesses that would fall under the TIUE category, this could translate into a substantial revenue stream. Yet, no oversight mechanisms are currently in place to govern the collection, distribution, or utilisation of these funds, raising questions around transparency and accountability.

A BROADER REGULATORY COMPARISON RAISES FLAGS

India's legal ecosystem already permits private entities to authenticate user credentials for a fee, but typically within clearly defined and regulated frameworks. The MNV platform, by contrast, lacks essential guardrails.

For example, under the Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023, KYC-user agencies pay between Rs 0.50 and Rs 5 per authentication request. TSPs that use e-KYC to obtain demographic data, for instance, are charged Re 1 per request.

Similarly, regulated entities in the banking, financial services, and insurance sector are permitted to verify a customer's PAN card through authorised agencies. This process includes a fixed, reasonable fee structure that allows entities to confirm a PAN's validity and match it with the individual's name and date of birth.

While the MNV platform mirrors this pay-per-verification structure, it departs significantly in two critical respects. First, Aadhaar and PAN authentication are limited to a narrow group of regulated entities performing compliance-specific roles. The MNV model, however, places no such threshold: any business can pay to validate mobile numbers, regardless of industry, function, or regulatory requirement. Second, whereas Aadhaar and PAN systems return only limited information, the scope of data disclosed via MNV remains undefined—raising alarms about potential data overreach.

The Draft National Telecom Policy, 2025, further reiterates the government's intent to introduce an MNV service "for providing a secure telecom space to other services sector entities like banking, insurance, social media, e-governance, etc., for prevention of misuse of telecom resources for cyber frauds".

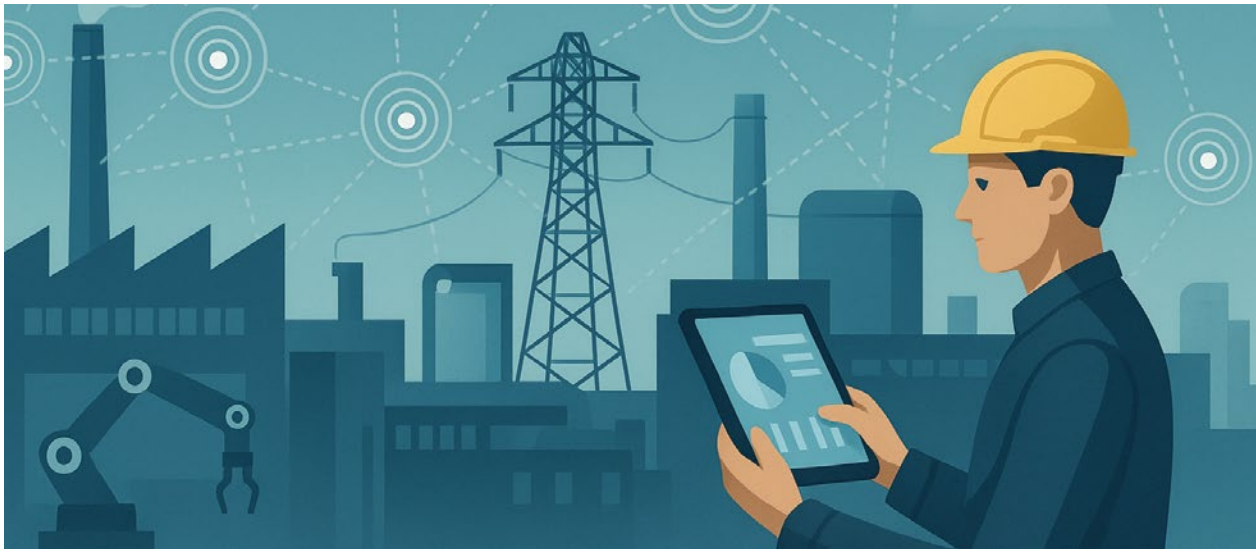
The aspiration to create a robust MNV framework is, in principle, commendable. However, its current design raises significant concerns, including financial setbacks for businesses, as well as far-reaching privacy issues for the average digital customer. This merits thoughtful reconsideration of the Proposed Cyber-Security Amendments before implementation.

Nagaraj is a Partner and Verma is a Senior Associate at Shardul Amarchand Mangaldas & Co. (The views expressed are those of the authors).

feedbackvnd@cybermedia.co.in

Quiet power: How mesh networks are powering industrial IoT

RF mesh networks are emerging as a resilient, decentralised backbone of industrial IoT, quietly powering factories, utilities, and infrastructure.



BY JANI VEHKALAHTI

Walk onto any modern factory floor today, and chances are you will not hear much discussion about the networks quietly keeping everything running behind the scenes.

While much of the conversation around infrastructure connectivity focuses on cloud platforms and AI-powered dashboards, the real enabler is operating silently in the background—reliable, unassuming, and essential. It is a wireless mesh network.

Over the past few years, mesh networking has moved from an emerging concept to a core layer of infrastructure, quietly transforming industries across the globe. And India is no exception.

WHY RF MESH MATTERS NOW?

Let us set the context. When we talk about Radio Frequency (RF) mesh communication, we are referring to the "last mile" of connectivity. RF mesh connects the actual devices, not replacing the Internet backbone, which continues to be delivered via fibre or cellular, but extending it. A single Internet connection can be shared with hundreds or even thousands of devices through an RF mesh.

In the case of cellular networks, one mobile operator subscription can serve hundreds of devices, dramatically increasing cost-efficiency.

Industrial environments, however, demand a different kind of connectivity. Traditional centralised infrastructure, such as Wi-Fi or cellular, often struggles in the harsh conditions of factory settings. Many industrial areas suffer from weak cellular coverage, and installing reliable Wi-Fi can be prohibitively complex and expensive. Metal walls, interference, and constantly evolving layouts create ongoing connectivity challenges.

Enter RF mesh networks based on the new NR+ standard, which completely rewrites that script. Instead of relying on a central hub, each device, or node, connects with its neighbours and relays data peer-to-peer, without the need for fixed infrastructure. Think of it like

> Smart meters in India show how RF mesh can connect millions of devices across geographies with reliability, scalability, and low cost.

a neighbourhood watch, where every house is both a resident and a signal repeater.

The result? A decentralised, self-healing network that adapts to its environment and eliminates downtime. It also offers the industry's fastest network recovery following power outages, far outperforming legacy standards.

In practical terms, this means data continues to flow even if a device goes offline or a machine is moved. For operations that run 24/7, that level of resilience is not just a benefit; it is a necessity.

REAL-WORLD BENEFITS OF RF MESH

Mesh networks have already proven their worth across a range of sectors. Take smart metering, for example. With millions of electricity meters scattered across diverse and often remote regions, India needs a connectivity solution that can reach even the smallest villages. RF mesh allows each meter to communicate with its neighbours, forming a multi-hop network that transports data across long distances without requiring infrastructure at every point.

While most RF mesh systems are limited in how many "hops" they can support, the NR+ standard introduces a virtually unlimited hop count. The result is better coverage, higher reliability, lower costs, and significantly reduced maintenance needs.

In manufacturing, similar benefits are emerging. Asset tracking, energy monitoring, and predictive maintenance all rely on sensors transmitting real-time or near-real-time data, and they need to do so reliably.

NR+ based RF mesh networks are purpose-built for these requirements. They scale effortlessly, maintain low latency, and provide the resilience industrial environments demand.

THE QUIET STRENGTH OF DECENTRALISATION

One reason mesh networking does not often make headlines is that it simply works. It does not require daily reboots. It does not need a complex configuration, and neither does it collapse when a single node fails.

That is the power of decentralised decision-making, much like how drivers on India's roads make split-second decisions based on their immediate surroundings. Now, imagine those cars were centrally controlled with delayed data. It would not work. Similarly, NR+ mesh enables each device to connect with over 50 other nodes in urban areas, ensuring multiple routes for data to travel.

By removing single points of failure, mesh networks distribute both data and responsibility. This reduces costs while increasing system security. If one node is compromised, the rest of the network continues functioning, isolating threats and protecting operations. In an era of growing cyber risks, that is a significant advantage.

INDIA'S EDGE WITH RF MESH ADOPTION

India will continue to be one of the biggest beneficiaries of RF mesh-based Industrial Internet of Things (IIoT). With a booming manufacturing sector, an increasing focus on smart infrastructure, and a diverse geography, RF mesh presents a low-barrier, high-reliability solution for connecting everything from factories in Tamil Nadu to water pumps in rural Punjab.

The industry is already seeing significant momentum, particularly in electricity distribution. Nearly 10 million smart meters have been deployed across India, with minimal support and without the need for complex integrations. And that is key, scaling IoT in India means keeping it simple.

There are existing solutions to help implement the latest RF mesh standard, ensuring simplicity and resilience. The system requires minimal planning, installs quickly, configures itself, and runs on standard hardware, using the unlicensed 865–868 MHz ISM spectrum.

The best technologies eventually fade into the background—like electricity, water, and the Internet. RF mesh is on the same path. It does not make noise, nor does it need to. When an entire factory floor talks to itself, stays connected, and runs without intervention, that is when the real revolution arrives—quiet, confident, connected.

The author is the SVP for Smart Grids with Wirepas.
feedbackvnd@cybermedia.co.in

Steel tape shortage: A missing link in India's telecom supply chain

A shortage of ECCS tape, the protective armour for fibre cables, threatens India's 5G rollouts, BharatNet progress, and BSNL revival plans.

BY DR JAIJIT BHATTACHARYA & MANOJ DINNE

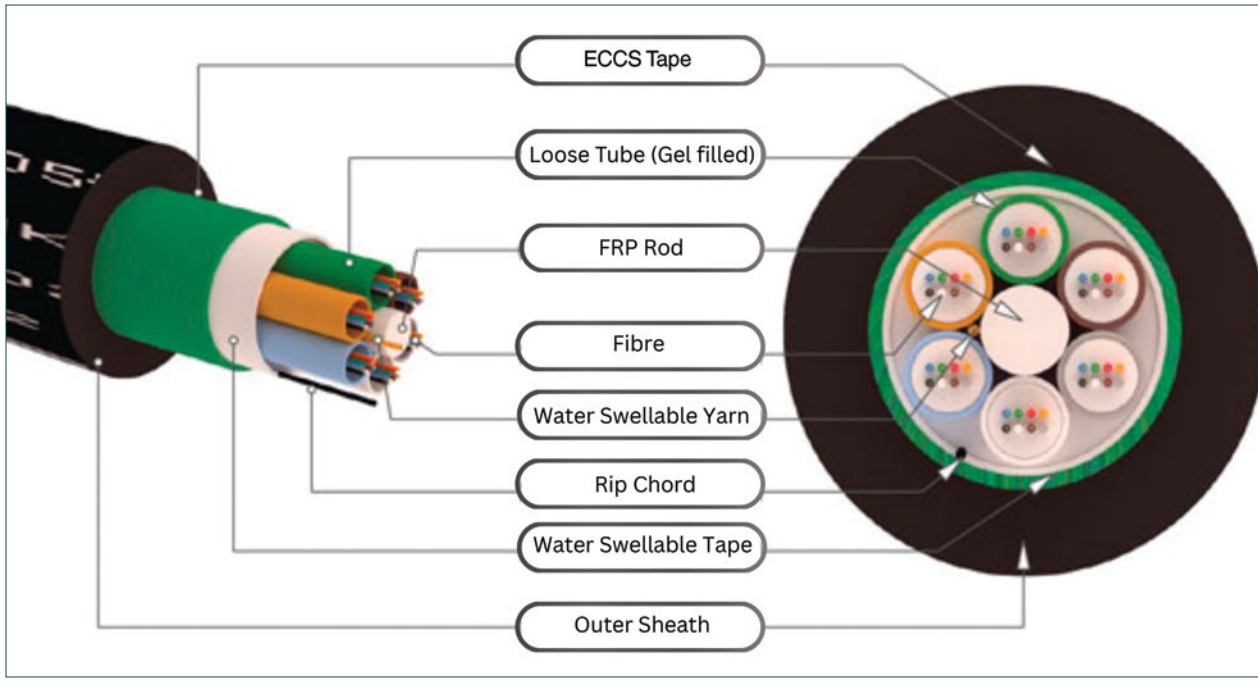
India's telecom infrastructure boom faces an unexpected constraint. As the telecom ecosystem players race to expand 5G networks, BharatNet connecting remote villages, and the revival plans of BSNL, a critical shortage has emerged: electro-chromium co-polymer coated steel (ECCS) tape; think of it as a body armour for the fibre.

This armoured tape is needed to rust-proof, strengthen and protect the Optic Fibre Cables (OFC) from corrosion, physical damage and moisture, making it an indispensable input in India's connectivity.

The current shortage stems from the intersection of quality improvement initiatives and supply chain realities. In January 2025, the Ministry of Steel implemented Quality Control Orders (QCO) requiring mandatory BIS licensing to enhance steel quality across the ecosystem. While logical for standard steel products, this framework creates complexities for specialised items like ECCS tape.

The challenge lies in ECCS tape's unique position: India lacks domestic production at scale, which means no established BIS standards exist for the product. Recognising such scenarios, the Ministry had established a specialised portal in October 2023, allowing importers to secure No-Objection Certificates (NOCs) for products without existing BIS specifications.

This workaround was effectively until December 2024, when NOC issuance ceased. Consignments that previously cleared through established exemption processes now face regulatory uncertainty, while industry domestic inventories have dwindled to weeks of supply.



> The ECCS tape shortage is more than a supply glitch—its a bottleneck that could slow down India's digital inclusion and 5G aspirations.

DEMAND-SUPPLY GAP WIDENS FOR STEEL TAPE

Demand supply gap data reveals the scale of the challenge. Industry projections indicate India will need over 11,000 metric tonnes of ECCS tape in the second half of 2026 alone, driven by massive infrastructure deployments across public and private networks.

Current order books paint an even starker picture. C-DEP's research revealed that between BharatNet's optical fibre cable requirements and private operators' 5G expansion plans, existing purchase orders translate into demand for more than 29,000 MT of ECCS tape in the next two to three years.

Domestic production capacity paints a stark picture. Even the country's leading steel producers do not make finished ECCS tape at scale, and the industry is still testing market feasibility. What is more, Indian steel presently lacks the necessary CACT or Component Approval Centre for Telecommunication certification, and with only two laminators currently certified, the supply situation remains further constrained.

While India can produce about 435 MT of raw steel coils per month (the base material for ECCS tape), actual conversion into finished ECCS tape is limited. These coils must be coated and laminated before they can be used to armour optical fibre cables.

Between January and June 2025, domestic makers supplied just over 1,000 MT of finished ECCS tape to the OFC industry, barely 22% of the requirement.

The shortfall will persist. For FY 2025–26, demand is projected at 18,000 MT, but domestic capacity can meet only around 5,000 MT. In other words, there will likely be a shortfall of 13,000 MT ECCS tape of the requirement in the next six months.

TELECOM ROLLOUTS FACE MOUNTING CHALLENGES

The supply constraint creates cascading effects throughout the telecommunications value chain. OFC cable manufacturers, like most other businesses, plan procurement months in advance, sequencing glass preforms, fibre drawing, colouring, stranding, jacketing, and armouring in tight cycles. If ECCS tape cannot be procured predictably, the domino effect will disrupt the entire supply chain, similar to how the rare earth magnet shortage impacted the Indian auto industry.

Public projects bear significant pressure. BharatNet's village connectivity mission and BSNL's fibre-to-the-home expansion, as well as 5G rollouts, represent multi-thousand-crore investments where delays could compound costs and extend deployment timelines, potentially affecting rural digital inclusion objectives.

So, what can India do?

In the near term, the Ministry can consider allowing imports of ECCS tape until domestic capacity is scaled up. The rationale here is compelling. First, ECCS tape is not yet covered by a BIS standard, and the NOC process previously provided was stopped in December 2024. Second, domestic production cannot meet current demand; even optimistic capacity additions will take time to commission and ramp. Third, certainty on ECCS availability will stabilise factory schedules and production planning, preventing cost escalation that ultimately lands on public budgets and consumers.

Parallelly, the Ministry of Steel could consider reopening the QCO portal for ECCS tape exemptions with clear criteria and validity periods and support the domestic ecosystem through targeted incentives so that India can achieve Atmanirbharta in ECCS tape production.

India needs to strike a balance between addressing the immediate supply constraints while building long-term industrial capacity. The telecommunications sector's continued expansion depends on solving such component-level challenges, making the ECCS shortage both a test of policy agility and an opportunity for strategic industrial development.

Bhattacharya is President and Dinne is Senior Policy Consultant at the Centre for Digital Economy Policy Research (C-DEP), a think tank focused on the digital economy, policy innovation, and technology governance.
feedbackvnd@cybermedia.co.in

CERT-In sets the rules for digital trust

The new audit guidelines shift cybersecurity from routine checks to a structured, risk-based framework for resilience and enterprise accountability.

BY JASPREET SINGH

The Indian Computer Emergency Response Team (CERT-In) has released the Comprehensive Cyber Security Audit Policy Guidelines (Version 1.0, July 2025)—a decisive move to strengthen the nation's digital security framework. Designed to introduce uniformity, clarity, and accountability, the guidelines aim to ensure that audits across government, critical infrastructure, and private enterprises become reliable benchmarks for risk reduction rather than routine exercises.

More than a technical document, the policy serves as a blueprint for organisations to measure, manage, and improve their cybersecurity posture in a structured and auditable way.

ESTABLISHING A UNIFIED AUDIT FRAMEWORK

The guidelines define a structured audit process that spans planning, scope definition, technical assessments, asset discovery, vulnerability scanning, and evidence gathering. They prescribe how findings must be categorised by severity and presented in standardised reports.

By setting a reproducible lifecycle, CERT-In ensures that audits move beyond a box-ticking approach. Each assessment is intended to deliver verifiable results that reduce tangible risks, elevating the audit process into a meaningful component of cyber resilience.

EXPANDING SCOPE ACROSS CRITICAL SECTORS

The framework applies to a broad spectrum of entities, including operators of critical infrastructure such as power grids, transport, and healthcare systems, along with financial institutions, IT service providers, data centres, cloud platforms, and government departments.

> The CERT-In framework makes audits transparent and traceable, ensuring every finding is classified, prioritised, and backed by verifiable evidence.

For many in regulated sectors, these guidelines will become the reference model for both internal and external audits. Even in the absence of a cyber incident, organisations will now be expected to demonstrate preparedness through structured compliance.

METHODOLOGY ANCHORED IN RISK PRIORITIES

Departing from fragmented checklist-driven audits, the new policy mandates the use of CERT-In-approved templates for planning, documentation, and evidence submission. Traceability is emphasised, with auditors required to show precisely how issues were discovered and classified.

Audits must be conducted by CERT-In empanelled professionals, ensuring quality and consistency in assessments. Every vulnerability or control gap must be ranked as critical, high, medium, or low, with corresponding timelines for mitigation. This risk-centric classification ensures that resources are channelled towards the most severe threats, including those that could lead to breaches, ransomware, or disruption of essential services.

The guidelines also extend their reach to emerging domains including cloud services, IoT, AI platforms, blockchain systems, and operational technology or industrial control systems. By addressing supply chain security and introducing scoring models such as CVSS combined with EPSS, the framework enables more accurate prioritisation of vulnerabilities most likely to be exploited.

WHY THE GUIDELINES ARE TIMELY TODAY

India's expanding digital footprint has been matched by an increase in state-sponsored attacks, ransomware campaigns, and cloud-based vulnerabilities. A standardised protocol for assessing and reporting risks was overdue.

The new guidelines fill this gap by offering a measurable, action-oriented framework that is consistent across sectors. They provide organisations with a structured way to prepare for compliance obligations, strengthen reporting to boards and regulators, and respond more effectively during crises.

IN BRIEF

- CERT-In's framework transforms audits into structured, reproducible exercises that set a new national benchmark for cyber resilience.
- The guidelines expand scope to cloud, IoT, AI, blockchain, OT/ICS, and supply chains, acknowledging risks beyond traditional IT systems.
- CVSS combined with EPSS moves audits from generic labels to risk-based prioritisation, focusing on vulnerabilities most likely to be exploited.
- Auditor independence eliminates conflicts of interest, ensuring findings are transparent, trustworthy, and free from organisational influence.
- By elevating audits from compliance to strategic tools, the guidelines reinforce security as a boardroom priority and a trust enabler.

Independence of auditors is another key feature, aimed at removing conflicts of interest and ensuring transparent, trustworthy findings. Stronger requirements for data handling—including storage in India, encryption, and secure disposal—underscore the recognition that protecting information is as critical as detecting flaws.

With expanded coverage to AI, IoT, and blockchain, the guidelines reflect a future-ready mindset where threats extend far beyond legacy IT.

FRAMEWORK ESSENTIALS

- **Standardised structure:** The guidelines transform audits from ad hoc reviews into structured exercises, introducing a national benchmark for quality, reproducibility, and consistency across organisations.
- **Expanded coverage:** Going beyond IT, the framework brings in emerging domains such as cloud, IoT, AI, blockchain, OT/ICS, and supply chains, acknowledging that vulnerabilities now lie across interconnected ecosystems.
- **Risk-based scoring:** The integration of CVSS with EPSS is a major shift, replacing generic "high/medium/low" labels with prioritisation rooted in actual exploit likelihood, ensuring that resources are deployed where risks are real and urgent.
- **Auditor independence:** By emphasising separation between auditors and auditees, the guidelines aim to eliminate conflicts of interest, reinforcing transparency and credibility in reporting.
- **Enterprise accountability:** The rules make it clear that while audits can validate, the ultimate responsibility for securing systems and addressing vulnerabilities rests with the enterprise itself.
- **Data stewardship:** Mandates on data storage in India, combined with requirements for encryption and secure disposal, highlight that protecting information is as important as detecting weaknesses.
- **Strategic value:** By elevating audits from check-box compliance to board-level strategic instruments, CERT-In has reframed them as tools for resilience, continuity, and long-term trust.

FROM COMPLIANCE TO DIGITAL RESILIENCE

For security teams, compliance officers, and IT heads, the guidelines demand immediate alignment of internal programmes with the new audit model. Organisations will need to map existing procedures against the CERT-In structure, train audit teams and vendors on updated requirements, and identify gaps in documentation and evidence readiness. Preparing for periodic audits by empanelled providers becomes an essential step.

More importantly, the emphasis shifts from detection to remediation. Organisations must demonstrate that vulnerabilities identified during audits are addressed, documented, and verified through testing. The framework insists that security ownership stays with the enterprise, while audits validate and benchmark performance.

The maturity of the policy lies in its elevation of audits from a compliance ritual to a strategic tool for resilience, continuity, and boardroom decision-making. Organisations that embrace the guidelines will find themselves better equipped to manage threats and strengthen trust among stakeholders.

Ultimately, the responsibility lies with leadership to adopt these measures in spirit, not just in letter. Cybersecurity today is a boardroom priority and a cornerstone of digital trust. CERT-In has provided the framework; it is now for enterprises to act decisively and build the secure digital ecosystem that India urgently requires.

The author is a Partner at Grant Thornton Bharat.

feedbackvnd@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

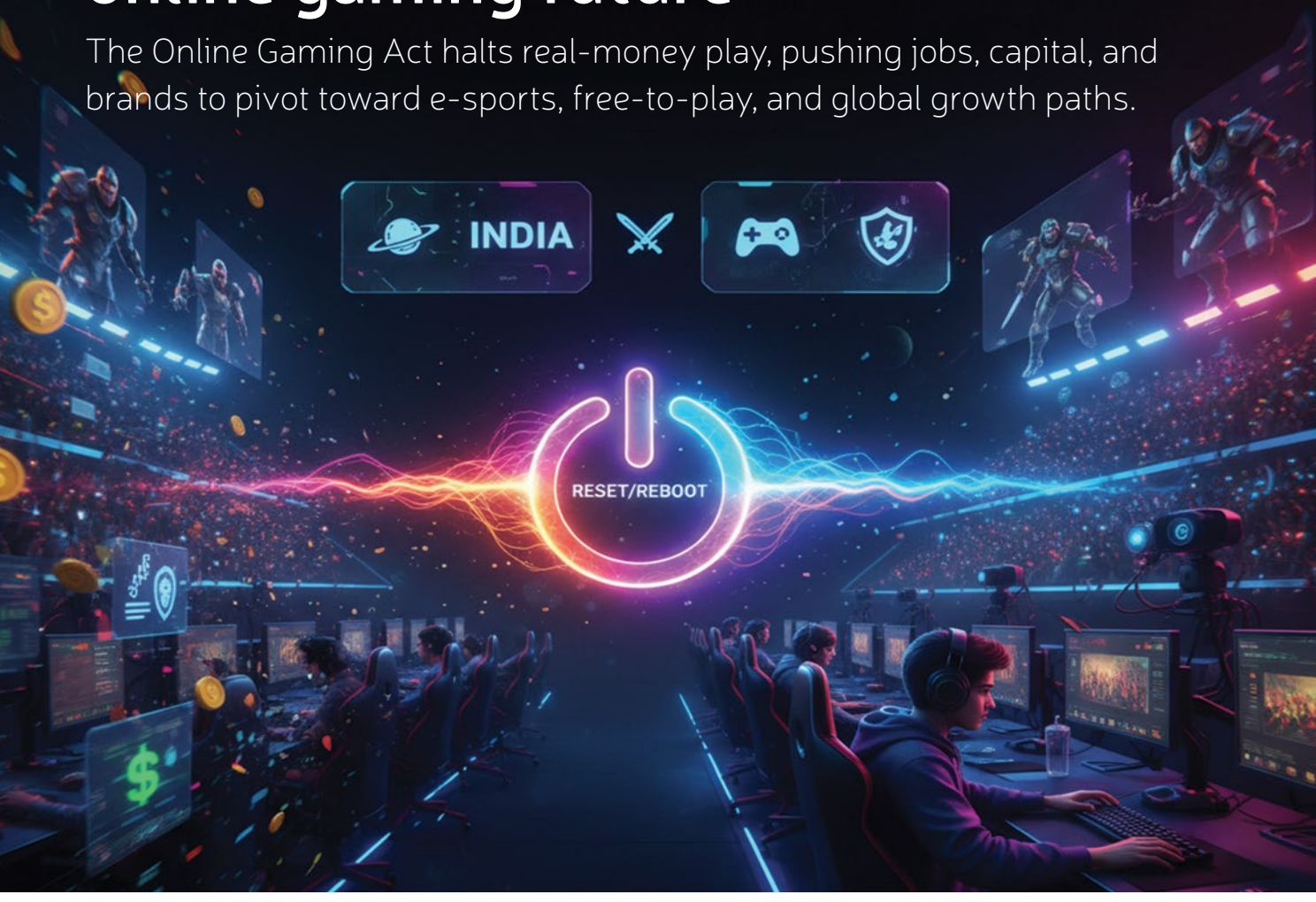
Ajay Dhoundiyal
Sr. Manager
ajaydh@cybermedia.co.in
+91 99535 40318

Scan the QR code for event registration and more information

[NEWS ANALYSIS]
ONLINE GAMING

Bet off the table: India rewrites online gaming future

The Online Gaming Act halts real-money play, pushing jobs, capital, and brands to pivot toward e-sports, free-to-play, and global growth paths.



BY JAIDEEP GHOSH

The passage of the Promotion and Regulation of Online Gaming Act, 2025, has sent a powerful regulatory shockwave through India's digital economy, effectively outlawing all real-money games (RMG) while simultaneously attempting to promote e-sports and social gaming. This is a fundamental restructuring of a sector that had drawn millions in venture capital, provided thousands of jobs, and created a new advertising category in India's sports economy.

The ban, while presented as a step to foster a "healthy" ecosystem, creates a significant short-term social and economic cost. The Act has already been challenged in the courts, though most larger players seem reluctant to do so and instead intend to focus on a pivot strategy.

JOBS AT STAKE: HUMAN CAPITAL FALLOUT

The most immediate and tragic impact of the ban is on human capital. The prohibition could threaten over two lakh jobs across more than 400 startups. The affected functions—including operations, customer support, and marketing—are those directly tied to the now-defunct RMG business model.

India's gaming reboot could reshape jobs, capital, and sponsorships, but the ultimate impact depends on enforcement and sectoral pivots.

A significant portion of this talent pool is expected to migrate, including to the now-promoted e-sports and game development studios. However, many core skills of the RMG business are not directly transferable to meet the needs of e-sports and social gaming sectors. This creates a need for rapid reskilling in areas such as live ops, community management, and IP development.

Further, while the government aims to boost the creative economy and game development exports, this poses a substantial risk of "brain drain".

CAPITAL SHOCK AND INVESTOR RETREAT

Investors value predictability! This law marks one of the largest sudden value erosions of VC-backed assets in the Indian digital economy, comparable to earlier corrections in the edtech sector.

The RMG sector, with an estimated valuation of nearly USD 15 billion and having raised over USD 3 billion, is now facing massive capital losses and likely large write-offs. Nazara Technologies, the only publicly listed gaming company with exposure to RMG, saw its market capitalisation fall significantly.

For many RMG-focused investors, prospects for an IPO or strategic M&A have evaporated, creating a buyer's market for distressed assets. The immediate response from investors is a "cooldown" phase with a pause on follow-on rounds, as they focus on restructuring and damage control.

A sudden regulatory ban on a high-growth sector with significant VC backing also sends a negative signal about the broader investment climate.

Impact on sports sponsorship: The disappearance of this category will reshape sports marketing economics. Fantasy sports ventures Dream11 and My11Circle, together for example, were contributing nearly Rs 1,000 crore to Indian cricket, a significant portion of their revenue. The scramble by broadcasters, leagues, sports bodies, and ad agencies for new sponsors underscores the relationship that had developed between RMG and the sports ecosystem.

IN BRIEF

- Over two lakh jobs and 400+ startups face disruption, demanding urgent reskilling and talent migration.
- Nearly USD 15 billion in RMG value could erode, cooling investor appetite and sparking asset write-downs; recovery hinges on new sector pivots.
- Sports sponsorship losses may exceed Rs 1,000 crore, altering cricket economics if replacement brands step in slowly.
- AdTech, KYC, and fintech revenues are likely to contract, with the depth of impact tied to diversification speed.
- Public health risks may increase if demand shifts to illicit platforms, but the effectiveness of enforcement remains uncertain.
- E-sports, free-to-play, and exports may offer new growth, though scale and capital flows are still probabilistic.

> E-sports and free-to-play models may attract talent and capital, yet their ability to replace RMG revenues remains uncertain.

INDIA RMG SNAPSHOT

Company	Focus	Revenue (Rs Cr)*	Net Profit (Rs Cr)	Ad Spend (Rs Cr)	Valuation (Rs Cr)	Staff Impact#
Dream11	Fantasy Sports	6,200	400	1,200	60,000	5-10% layoffs
MPL	Fantasy Sports, Casual	2,800	-500	600	12,500	60% Layoffs
Games24x7	Rummy, Fantasy Sports	2,200	250	500	18,000	15–20% layoffs
Nazara Tech	Diversified Gaming, eSports	1,200	120	200	7,500	5–10% layoffs
Zupee	Ludo, Trivia, Skill Games	800	-300	150	5,500	30–35% layoffs
GamesKraft	Card games	3500	950			NA

**Revenues are estimated based on recently published data and are indicative.*
 # Staff impact figures are directional estimates reflecting possible adjustments post-regulation.

Impact on financial market: The law's effects extend far beyond the gaming platforms themselves. Financial institutions and fintechs now face the challenge of identifying and blocking payments to banned platforms while simultaneously ensuring user funds are safely withdrawn from domestic accounts, thereby increasing their process costs and risks of non-compliance.

Impact on the advertisement sector: The ban's ripple effects on the ad market are profound. This ban has led to an immediate oversupply of high-value programmatic ad slots and a drop in CPMs (cost per thousand impressions). AdTech firms need to diversify their client base, with a likely shift to e-commerce, BFSI, and D2C brands.

Additionally, companies providing services to the RMG sector, such as KYC vendors, anti-fraud firms, analytics providers, influencers, and other support services, may face a significant contraction in demand.

PUBLIC HEALTH AND BLACK-MARKET RISK

The law addresses legality, but not demand. Demand will inevitably find alternative channels. For millions of users, online gaming was not merely entertainment but a quasi-investment habit.

The government's rationale for the ban rests on mitigating the profound social and public health harms of online gaming, citing cases of addiction, financial ruin, and even suicide. When that "habitual user" is suddenly cut off from these platforms, the withdrawal symptoms can be severe.

With legitimate avenues closed, some users may be drawn to the very black market the law seeks to prevent, where offshore sites and underground networks offer a new fix. This shift exposes users to a higher risk of fraud and financial exploitation, with no legal recourse.

HOW THE WORLD HANDLES ONLINE GAMING

Online gaming regulation varies significantly across the world, driven by differing philosophies on consumer protection, public health, and economic development. While India has adopted a prohibition model for real-money gaming, other major markets, particularly in Europe and the United States, have opted for frameworks based on licensing, taxation, and controlled growth.

The European Union exemplifies sophisticated regulatory pluralism, with 27 of 31 countries adopting multi-licensing regimes that allow both private and publicly owned companies to operate. The UK's Gambling Commission, established under the Gambling Act 2005, requires rigorous licensing with strict compliance standards including age verification, anti-money laundering measures, and responsible gambling tools. The European e-sports scene is well-established, with monetisation from sponsorships, ticket sales, and merchandise.

The United States presents a complex patchwork where 35 states permit sports betting and six authorise

> Demand may drift underground, raising fraud and health risks, although outcomes will vary with user adaptation and regulatory control.

online gaming, each with distinct regulatory frameworks. States like New Jersey, Pennsylvania, and Michigan have generated substantial tax revenue through controlled licensing rather than prohibition.

Australia follows a hybrid approach, banning online casino-style gaming but allowing regulated sports betting. South Korea has taken a progressive stance on gaming regulation, with a strong focus on protecting users from predatory practices, while promoting non-speculative activities under the Game Industry Promotion Act.

All games distributed in South Korea, across all platforms, must be rated by the Game Rating and Administration Committee (GRAC). E-sports is a key focus of the government's Comprehensive Plan for the Promotion of the Game Industry (2024-2028).

Contrastingly, in Japan, gambling is generally a criminal offence and strictly prohibited online gambling if it involves the acquisition or loss of economic value through chance. The Japanese e-sports Union (JeSU) allows tournaments if third-party sponsors fund the prizes, and the entry fees are used solely to cover operational costs. China represents the most restrictive approach to online gaming regulation globally, implementing a comprehensive prohibition of all forms of real money gambling under its Criminal Law.

Licensing havens are also reforming, tightening AML and governance after years of lax oversight. These shifts highlight regulatory adaptability, as jurisdictions can transition between openness and restriction as risks evolve.

BEYOND RMG: INDIA'S NEW GROWTH ENGINES

The law has explicitly created a favourable environment for new areas. However, these currently generate a fraction of prior revenues and require different user acquisition economics.

The rise of the e-sports economy: By formally separating e-sports from gambling and betting, the Act has paved the way for institutional recognition and corporate investment. E-sports bodies like NODWIN Gaming anticipate a surge in investments, sponsorships, and career paths, with a projected market size exceeding USD 1 billion by 2033.

A Pivot to Free-to-Play (F2P) Playbook: The ban forces a pivot to F2P models, which can be monetised through in-app purchases and advertisements. This aligns with the global gaming market. This shift requires a focus on user engagement, community building, and product excellence, rather than aggressive marketing and user acquisition through cash bonuses.

Game Development and Export: With a large pool of displaced talent and a clear regulatory framework for non-RMG games, India can strengthen its position as a global hub for game development and outsourcing.

Launch RMG in other countries: This will require significant effort, along with local partnerships and capital, which could deter and delay operations in countries with a relatively flexible policy framework

For these opportunities to be fully realised, capital must follow the talent. Investors, having marked down their RMG portfolios, will need to reallocate capital to these new, more predictable verticals. The government, having set the rules, must now provide a stable, predictable policy environment—and perhaps targeted incentives—to support this strategic pivot.

India's approach will succeed only if enforcement is robust and accompanied by a transition framework for users, workers and the sports-marketing ecosystem. The ban will lead to a natural market reallocation of capital, talent, and user base. However, the speed of this reallocation is critical. The success of the law's "promotion" side hinges entirely on the ecosystem and the government's ability to act quickly.

The prohibition was the easy part; the promotion is the real, and far more complex, challenge.

The author is a former Partner at KPMG in India.
(Views are personal.)
feedbackvnd@cybermedia.co.in

[NEWS ANALYSIS]
SEMICONDUCTOR

Chip packaging evolves to support connected futures

As 5G, edge, and IoT scale globally, chip packaging plays a critical role in delivering low-latency, energy-efficient connectivity at both core and edge.

BY SHETAL MEHTA

The semiconductor industry is entering a phase of transition that highlights the complementary roles of legacy and advanced packaging technologies. For decades, established methods such as wire bonding and single-die packaging have supported large-scale electronics manufacturing, powering consumer products, communication systems, and industrial applications. These techniques continue to be widely used due to their cost-efficiency, reliability, and scalability across diverse devices.

Simultaneously, as devices demand smaller footprints, greater data throughput, and improved energy efficiency, the adoption of advanced packaging technologies is accelerating. This shift does not suggest the obsolescence of legacy packaging. Rather, the industry appears set for a period of coexistence, where mature solutions address established needs while advanced packaging supports emerging, high-performance applications.

LEGACY PACKAGING IN CONNECTED ECOSYSTEMS

Legacy packaging continues to serve the industry

> As networks densify and edge expands, packaging innovation becomes essential to meet latency and power demands across telecom systems

Legacy packaging powers the bulk of connected devices today—its role remains crucial to keep 5G and IoT deployments inclusive and affordable.

effectively at scale. Its established processes, proven yield, and ability to support high-volume production make it a dependable choice for manufacturers. Traditional computing, consumer electronics, and industrial systems still rely on these methods, where performance requirements are met without added design complexity or cost.

For many markets—especially those prioritising affordability, product longevity, and secure supply chains—legacy packaging remains integral. Instead of being phased out, it continues to provide a stable base that supports both incremental and advanced innovation.

ADVANCED PACKAGING POWERS DATA DEMANDS

Applications requiring higher integration, faster processing, and lower latency—such as autonomous vehicles, Artificial Intelligence (AI), 5G, and hyperscale computing—are exposing the limits of conventional techniques. Advanced packaging methods, including 2.5D integration, 3D stacking, and fan-out wafer-level packaging, offer solutions to these challenges.

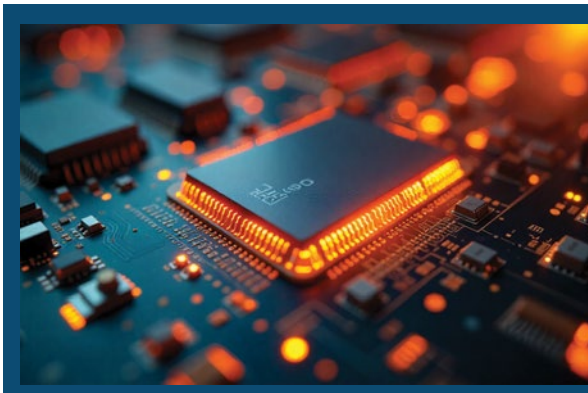
These technologies integrate multiple chips into a single package, reduce interconnect distances, and enhance power efficiency. However, their implementation is currently best suited for performance-intensive applications, while legacy packaging remains essential across broader, cost-sensitive device segments.

PACKAGING'S ROLE IN CONNECTIVITY SYSTEMS

Packaging has a direct influence on connectivity performance. Advanced packaging supports faster signal transmission, improved power efficiency, and stable operation in high-throughput environments—key for applications in 5G, cloud computing, and real-time IoT systems.

Nonetheless, not all connected devices demand these capabilities. Billions of devices globally continue to rely on legacy packaging for dependable and cost-effective connectivity, enabling inclusive and scalable digital ecosystems.

5G and edge computing demands: The global deployment of 5G networks is pushing performance requirements across both core and edge devices. Advanced packaging is proving beneficial for edge applications by supporting localised computing, which reduces latency and eases central processing



IN BRIEF

- Chip packaging shapes performance in 5G, cloud, and IoT by influencing latency, signal integrity, and system power efficiency.
- Advanced packaging supports high-bandwidth, real-time applications in telecom networks, from autonomous vehicles to mobile base stations.
- Legacy packaging remains vital for billions of connected devices that make up the foundation of telecom and industrial infrastructure.
- Dual-track packaging strategy enables scalability, from high-performance edge computing to cost-efficient network terminals and sensors.
- Evolving packaging helps operators manage power budgets and cooling in dense data environments supporting AI and next-gen connectivity.
- Future telecom growth depends on harmonising legacy reliability with advanced packaging's ability to meet dense integration demands.

> The future of connectivity depends not just on radio access, but on how chip packaging enables performance deep within devices and networks.

loads. This enables faster services in fields such as connected healthcare, industrial automation, and urban infrastructure.

Even so, the larger 5G infrastructure ecosystem continues to depend on legacy packaging for its supporting systems and devices, which require scale, reliability, and economic efficiency. Both technologies are needed to fulfil the full potential of 5G.

Enabling IoT at both ends of the spectrum: The Internet of Things is marked by its scale and diversity. Advanced packaging is essential for high-end IoT nodes that handle local analytics, offer low-power operation, and fit complex computing into compact forms. On the other hand, simple sensors and actuators—especially those deployed across agriculture, manufacturing, or supply chains—depend on legacy packaging for cost-effective mass deployment.

This dual approach is enabling broad-based IoT growth without compromising performance or affordability.

Supporting AI and data-centric workloads: AI workloads benefit from tighter integration between processing and memory. Advanced packaging helps reduce data transfer latency, improve compute throughput, and increase energy efficiency. This becomes crucial in use cases such as natural language processing, autonomous systems, and predictive analytics.

However, many AI workloads still run effectively on devices using legacy packaging—especially where real-time performance requirements are moderate. Together, both packaging approaches are shaping the evolving AI hardware ecosystem.

Balancing automotive system needs: In the automotive industry, safety, performance, and cost must be balanced carefully. Advanced packaging supports the complex, high-speed requirements of autonomous systems and in-vehicle communications. Simultaneously, legacy packaging is still used in subsystems such as infotainment, battery management, and power control where stability and maturity are essential.

This division allows manufacturers to manage costs while delivering innovation and safety in next-generation vehicles.

Environmental and operational considerations: With sustainability gaining prominence, packaging technologies are also being evaluated for their environmental and energy impact. Advanced packaging reduces energy consumption and improves thermal performance in data-heavy applications. Meanwhile, legacy packaging contributes through long-established, efficient processes that generate less waste in high-volume production.

Together, both approaches can support the industry's move towards lower emissions and reduced resource consumption.

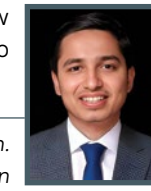
MANAGING TRANSITION AND COMPLEXITY

While advanced packaging introduces technical benefits, it also involves higher design complexity, increased cost, and demands new manufacturing capabilities. Legacy technologies continue to offer cost-effective, reliable alternatives, particularly for markets and applications where margins are tight or long-term reliability is prioritised.

To remain competitive, companies and countries will need to invest in both domains—preserving the strengths of legacy infrastructure while expanding capacity for advanced manufacturing.

Semiconductor packaging is not evolving through a replacement model but through mutual reinforcement. Advanced packaging will expand its role in high-performance computing, next-generation mobile networks, and AI-centric devices. Legacy packaging will continue to be crucial for scaled deployments in consumer, industrial, and infrastructure segments.

The future of the industry lies in how effectively it integrates both paradigms to serve a spectrum of market needs.



The author is a Co-Founder of Suchi Semicon.
feedbackvnd@cybermedia.co.in

The fragile shield: India's test of data resilience

As breaches multiply worldwide, India must reinforce its fragile shield of digital identity with stronger defences, resilience, and civic trust.

BY DAVID SEHYEON BAEK

In June 2024, Indonesia's Temporary National Data Centre (PDN 2) was targeted by a ransomware attack that encrypted over 200 public services. The attackers, using a LockBit 3.0 variant known as Brain Cipher, demanded a USD 8 million ransom. Immigration systems froze, healthcare subsidies were delayed, and school certificates could not be issued. For weeks, every day, services were inaccessible, and confidence in digital governance was shaken.

What unfolded in Jakarta should not be dismissed as a distant crisis. Similar failures have already surfaced across the world. In 2023, a government misconfiguration in Bangladesh exposed the personal details of more than 50 million citizens.

In the Netherlands in 2024, records of 63,000 police officers were leaked, putting those responsible for public safety at risk. In Finland in 2020, the breach

> Identity leaks are not abstract threats—once data enters the dark web, it becomes a permanent tool for fraud, coercion, and espionage.

> Civic lifelines like Aadhaar and UPI require the same resilience as power grids, with distributed architectures and rapid recovery plans.

of the Vastaamo psychotherapy centre led to patients being blackmailed with their most private confessions. Similarly, in the United States, the 2015 breach of the Office of Personnel Management compromised the security clearance files of 5.6 million federal employees, an intelligence windfall for adversaries.

INDIA'S IDENTITY EXPOSURES AT SCALE

India itself has not been spared. Several Aadhaar-related incidents have already revealed the dangers of managing identity at scale. In January 2018, reporters were able to purchase unauthorised credentials online for a nominal fee, which allowed them to query the Aadhaar database and retrieve names, addresses, photos, and phone numbers in plain text. That same year, poorly secured public-sector websites and APIs exposed data linked to more than 130 million citizens.

The problem has only grown.

On 9 October 2023, a Breach Forums user, calling themselves pwn0001, advertised what they claimed was an 815 million-record database of Aadhaar and passport details. The post listed fields such as names, phone numbers, Aadhaar numbers, passport numbers, addresses, districts, pincodes, and states, and even attached a sample of 100,000 records in plain text CSV format.

The advertisement described the dataset as 90GB, leaked in September 2023, and "never sold before." Researchers later confirmed that at least some of the samples contained valid Aadhaar numbers and citizen details.

The same claim resurfaced repeatedly. In early March 2024, another actor using the alias markflaus posted the same "815 million" Aadhaar and passport database. In late July 2025, a poster calling themselves joe-goldberg made a similar offer, followed by rofoy2984lu in early August 2025.

Not every post is authentic—some may be duplications or scams—but the repetition matters. Once even a portion

IN BRIEF

- Ransomware on Indonesia's PDN 2 froze vital services, showing how digital trust collapses when civic data is compromised.
- India's Aadhaar leaks, some allegedly in plain text, highlight systemic weaknesses in encryption and data handling.
- Repeat claims of 815 million Aadhaar records indicate that once breached, citizen data circulates endlessly across dark web channels.
- Breaches worldwide—from therapy notes to police files—demonstrate that data loss is now a systemic governance shock.
- Protecting civic platforms like Aadhaar and UPI needs continuity plans, breach disclosures, and proactive threat monitoring.
- Cyber hygiene must be taught universally, making secure practices as essential as literacy in safeguarding national identity.

> Trust in digital governance rests on security. Without it, national identity shifts from asset to liability in an interconnected world.

of such a dataset leaks, it circulates permanently across forums, torrents, and Telegram channels. Each new post becomes a test of whether oversight or missed vulnerabilities remain.

PLAIN TEXT DATA: A SYSTEMIC WEAKNESS

What is especially concerning is that much of the data appears in plain text. While UIDAI has consistently maintained that biometric data is encrypted, demographic and linked identity data have allegedly been stored or transmitted without strong encryption in some systems and third-party databases.

If Aadhaar numbers, addresses, and phone numbers had been correctly encrypted at rest, in transit, and in use, the leaked files would not have been directly readable. Instead, the samples being traded look like ordinary spreadsheets, line by line, making them immediately useful for fraud and identity theft.

This reality requires a change in mindset: defenders must assume breach. Threat actors are already probing, and some are already inside. Under this assumption, hygiene is no longer optional. Encryption by default, strict access controls, and continuous monitoring are essential guardrails that limit the damage even when attackers gain entry.

Taken together, global and Indian incidents demonstrate that data breaches are no longer limited to scattered leaks or stolen credit cards. They are systemic shocks. They damage governance, erode public trust, and tilt the balance of national security. In Indonesia, a ransomware infection paralysed state functions. In Finland, therapy notes became weapons of coercion. In Washington, personnel files turned into an espionage goldmine. And in India, Aadhaar-related exposures demonstrate that national identity can also become a national liability if its protection is weak.

BUILDING RESILIENCE FOR CIVIC LIFELINES

Moving forward, India must rethink its approach. Data infrastructures like Aadhaar, UPI, DigiLocker, and GSTN are civic lifelines, no less critical than power grids or highways. Protecting them requires more than firewalls. It requires continuity planning so services can recover quickly under attack, mandatory breach disclosure so incidents are not hidden, and proactive intelligence to monitor dark web forums and Telegram channels where stolen credentials and phishing kits appear long before deployment.

Architecture matters as well. Estonia's reforms after its 2007 cyber assault show how distributing government data across secure nodes and backing up databases abroad reduces dependence on single points of failure. India can adapt similar models. Equally important is the human layer: many breaches begin with reused passwords, misconfigured servers, or poorly trained administrators. Cyber hygiene must become as basic a civic skill as literacy and numeracy, taught to students, officials, and kiosk operators alike.

Above all, data security is about trust. Citizens expect their identities, financial records, and medical histories to be safeguarded. When that trust is broken, the harm lingers long after systems are patched. Finns whose therapy notes were leaked, US officials whose background files were stolen, or Indians whose Aadhaar numbers now circulate online may never feel fully secure again.

Sovereignty in the twenty-first century is not defined only by territory or military might, but by control over data and the ability to defend it. The breaches of the past decade are not accidents; they are signals. For India, they serve as a lesson: data security is national security.

The choice is not whether breaches will happen—they already have. The choice is whether India will build the resilience, the intelligence, and the hygiene to withstand them. A digital future without secure data is fragile. Protecting it is not optional. It is essential.

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

AI MEETS NETWORKS: SPARKS PREVENT FIRES

From blind date to foresight, AI and networks can now predict mishaps, prevent outages, and help operators stay ahead of the flames

BY PRATIMA HARIGUNANI

What do firefighters ask Santa Claus? Ok, they are perhaps too grown-up for that, but if they were to make a wistful wish, what might they go for? No traffic jams? Possibly. Faster trucks? Certainly. No cats on the ledges? Definitely. Bigger hoses and buckets? Why not. Tougher blankets? Never hurts.

The answer, however, lies not in the smoke or the flames—but in the calm before the siren. It begins far ahead, even before the alarm bell rings or the call reaches the fire station. If firefighters could ask for something miraculous, it might be something deceptively simple yet notoriously hard to get—what if humans could detect a fire before the smoke spirals out of control?

This is precisely the sort of pre-emptive thinking now emerging in network operations rooms—across telecom operators, cloud providers, and data infrastructure teams. The question they are asking is no longer "What went wrong?" but "Can we know before it goes wrong?" The hope is that Artificial Intelligence (AI) may finally offer the predictive capability that decades of reactive network management could not.

AI INTELLIGENCE: AN OPERATOR'S FANTASY

The intelligence and real-time footwork that AI brings in can mean a whopping impact when translated into speed, precision and analytics in the realm of networks.

In the past, AI's role was mainly limited to analytics, decision support, and tasks such as fault prediction or capacity optimisation. But as Arvind Khurana, Regional Vice President and Country Head – Cloud and Network Services, Nokia India, captures it, today, AI is evolving to operate in real time, enabling autonomous, on-the-fly decision-making, powering capabilities like dynamic resource allocation, self-optimisation, and preventive assurance. "AI is essential for telecom operators as it forms the foundation of truly autonomous networks."

For telecom companies, the impact of this AI-driven approach is vital and extends beyond the network itself, concurs Jophy Varghese, APAC Head – System Integration and Country Manager – India Enterprise, Verizon. "Internally, it improves reliability and reduces operational costs. For customers, the same AI foundation enhances their experience through virtual assistants that troubleshoot issues and intelligent systems that

"AI reduces cost and boosts reliability for telecoms, while customers benefit from predictive routing, smart assistants, and quicker problem fixes."

JOPHY VARGHESE
APAC Head – SI & Country Manager – India Enterprise, Verizon

"AI is becoming the foundation of autonomous networks, enabling real-time decisions, dynamic allocation, self-optimisation, and assurance."

ARVIND KHURANA
Regional VP & Country Head – Cloud & Network Services, Nokia India

IN BRIEF

- AI is shifting networks from reactive firefighting to predictive foresight—spotting faults before sparks grow into disruptive outages.
- Digital twins give networks a second sight, enabling operators to model, validate, and prevent failures before they impact users.
- AI-powered sirens can auto-diagnose most critical faults, sharply reducing downtime and speeding recovery across large networks.
- Agentic NetOps brings autonomous AI agents that sense, decide, and act—cutting delays, boosting agility, and improving efficiency.
- Predictive AI lowers mean-time-to-resolution, ensuring operators stay ahead of outages and keep services consistently resilient.
- Success depends on robust data, skilled talent, and ethical guardrails to unlock AI's full potential in telecom networks.

route calls based on predicted complexity to resolve problems faster."

In fact, AI is rewriting the rulebook for networking, as Hon Kit Lam, Vice President – Hybrid Connectivity Services at Tata Communications, sees it. "It is turning static infrastructures into ever-smarter, self-adapting ecosystems. It automates complex processes, enhances real-time monitoring, and pre-emptively detects faults before they even reach our customers. The use of these technologies is helping shift from reactive fire-fighting to proactive, self-healing operations, particularly as isolating root causes and launching corrective measures is done without human intervention."

AI can proactively detect problems with impact assessment and provide automated root-cause analysis for immediate, decisive remediation, explains Manish Gangey, Executive President – Product Line Management, HFCL. "AI-based systems continuously learn from current and historical trends, enabling them to flag issues before they impact users."

Andrew Lerner, Vice President Analyst at Gartner, observes that AI is having, and will continue to have, a major impact on network infrastructure. "Their impacts range from short-term and cute to long-term and disruptive."

Let us expand how, and where exactly, AI is helping in preventing all the fires that networks were caught up in.

AI SIREN: FASTER AND SMARTER ALERTS

AI can be used to quickly detect network issues, personalise customer service and boost efficiency by automating support workflows, explains Lam. "For fault diagnosis, AI-powered programmes automatically analyse and correlate alarms across networks—including third-party networks—and even at the user end."

"This means that up to 85% of critical faults are automatically diagnosed, significantly reducing Mean Time

"AI is turning static networks into self-adapting systems, shifting operators from firefighting to proactive, self-healing operations."

HON KIT LAM
Vice President – Hybrid Connectivity Services, Tata Communications

To Recovery (MTTR) and ensuring a seamless customer experience. AI also enables predictive maintenance by identifying patterns that precede network failures, helping anticipate and address issues before they escalate," he says.

No wonder then, the power of AI—in context to networks—lies in more than one strength that it brings to the table. As Lerner breaks it down: "Typically, as it relates to network infrastructure, AI is packaged into a few different technologies: AI assistants, Digital Twins, and Agentic NetOps."

He unravels it further. "Network AI assistants are interactive digital tools backed by Generative AI (GenAI) and Machine Learning (ML) technologies that allow human users to communicate via conversational, natural language chat-interfaces. When built into network management consoles, network AI assistants provide actionable network insights and help with network operational tasks, improving administrator user experience, configuration, and operational efficiency. Today, these assistants are mostly 'cute' (i.e., nice to have), but they are evolving and eventually will become much more critical."

Varghese also points out that AI helps customer service agents by using generative AI to provide real-time recommendations. "By mastering AI for their own operations, these companies are better positioned to provide the robust, low-latency connectivity that other industries need for their own AI transformations, driving new revenue and future growth."

On the customer-service front, AI is powering advanced virtual assistants and sentiment analysis that personalise every interaction, avers Lam. "By drawing on account history, open incidents and behavioural data, these systems can greet users by name, provide tailored updates and guide them through self-help workflows—all before a ticket is created. Additionally, speech analytics helps gauge customer sentiment in real time, enabling proactive experience recovery when needed."

DIGITAL TWINS: NETWORK'S SECOND SIGHT

Consider how a twin changes the scenario completely—by seeing and alerting to things faster and better than ever before.

A network digital twin is a model of the behaviour of campus, Wide Area Network (WAN), or data centre network components, elaborates Lerner. "It is usually delivered as software and provides a model that can be used for validating the configuration, policies, or operations of a single network component or the entire network. It automatically synchronises with the production network. A network digital twin allows enterprises to validate configuration and security policies, as well as individual component operations or aggregation of components into a network."

Lerner contends that for IT leaders, a network digital twin allows faster testing and subsequent delivery of network changes, requiring fewer personnel resources and incurring lower costs by reducing system testing equipment needs. "We believe a network digital twin can improve delivery times for requests by 20% across the network."

With unified data, machine learning models analyse everything from traffic patterns to equipment health to forecast and prevent failures before they occur, Varghese adds. "This allows telecom companies to dynamically optimise network coverage, detect fraudulent activity, manage energy use and power tools that can answer plain-language questions about network performance."

There is more to AI than these ultra-powerful eyes and ears. AI also helps with new feet. And that is where we come to NetOps.

AGENTIC NETOPS: AUTONOMOUS AGILITY

NetOps can work as an entirely different kind of internal agility source—when combined with the astronomic speed and processing leaps of AI.

"Predictive AI spots anomalies early, cuts resolution times, and shifts teams from firefighting to proactive, foresight-driven decision-making."

MANISH GANGEY
Executive President – Product Line Management, HFCL

Agentic NetOps leverages goal-driven autonomous AI agents with capabilities such as memory, planning, sensing, tooling, and policy guardrails that have been granted rights by the organisation to operate network tasks and processes independently, Lerner indicates.

"AI agents work as a system to communicate autonomously with other AI agents to manage network infrastructure life cycle management with minimal to no human involvement. Agentic NetOps operates autonomously by minimising network operations personnel from being in the loop."

Lam adds that ultimately, this technology dynamically divides networks to control and contain threats and allocate resources most efficiently. "It is a combination of intelligence and agility that not only improves operational efficiency but also elevates the overall customer experience, making networks truly future-ready."

The impact translates into real-ground gains for operators. Lerner cites how AI agents can autonomously query other systems, tools, and other agents, make network changes, monitor network traffic, and use synthetic traffic injection to continuously analyse the network environment in real time and respond proactively to address issues. "They can improve network performance, efficiency, and response times by gathering data from multiple systems to make rapid decisions that cannot reasonably be achieved through traditional network operations."

Workflow automation is another area where AI delivers substantial value, Lam chimes in. "By having AI handle repetitive tasks, organisations can reduce response times from tens of minutes to near-instant, freeing expert teams to focus on strategic initiatives and innovation."

PREDICTIVE AI: FEWER NETWORK FIRES

All this predictive acuity means a great deal to telcos—as networks are the backbone of everything they do—and also of every place they fail.

Since Telcos operate at scale, a minor degradation can affect thousands of customers, Gangey underscores. "Predictive AI helps proactively identify user-impacting issues and bring down the mean-time-to-resolution. In particular, AI enables early detection of network anomalies by identifying patterns, deviations, or behavioural shifts, proactive coverage and capacity augmentation before user experience starts to degrade and transformation of operational teams from first responders to informed, ahead-of-time decision-makers."

Varghese sums up that advanced AI is transforming predictive network maintenance from a reactive to a highly proactive discipline. However, AI is only as good as the data it is built on, and we are on a journey to consolidate all our data into common platforms, he argues. "This will provide both cost savings because we will spend fewer resources moving and translating data; as well as operational benefits in having data from multiple domains in the same place, updating in near real time."

Manas R, Associate Vice President – Digital Engineering Expert, Aditi Consulting, underscored the challenge. "AI requires vast amounts of accurate, integrated data. Organisations need systems that can collect, analyse, and act on this data continuously. This demands not only the right tools but also the right talent and ethical frameworks."

He added that AI deployment often requires legacy systems to be updated, staff to be re-skilled, and new governance frameworks to be developed. "Without quality data and skilled people, even the smartest AI will fall short."

So, while the metaphorical cat may still climb the network ledge, operators are now better prepared—not to chase it, but to prevent it from climbing at all.

pratimah@cybermedia.co.in

CyberMedia

DOMINATE EVERY MARKET. BE A THOUGHT LEADER WITH CYBERMEDIA 365° GTM STRATEGY

Orchestrate a flawless market reach with CyberMedia comprehensive Go-To-Market strategy.

#GTMwithCyberMedia

Leave no stone unturned. Reach your target market with our strategic 365° Go-To-Market (GTM) approach. We orchestrate a seamless Thought Leadership Campaign, ensuring your reach across decision makers across strategic and functional verticals.

- Comprehensive coverage across CyberMedia brands
- Unique & innovative content experience in technology & innovation
- Focussed on Sustainability, Reliability and 40+ years of market leadership.

We don't just create campaigns; we craft cohesive experiences. Our GTM strategy integrates all touchpoints – from targeted CXO connects to Data-Driven measurable results.

Redefine your market presence with innovation and Out of the Box approach.

For further information, write to
Ajay Dhoundiyal, Sr. Manager,
ajaydh@cybermedia.co.in, +91 99535 40318

"Light waves deliver security that radio waves cannot"

What makes Light Fidelity (Li-Fi) the next big contender in connectivity? Is it the use of lasers, access to an unregulated light spectrum, EMI immunity, wall-level privacy, freedom from spectrum scarcity, or the absence of interference?

The answer is all this and more—though challenges remain around indoor obstructions, LED infrastructure, and hardware requirements. At the centre of this conversation is the Light Communication Alliance (LCA), which brings together the largest Li-Fi manufacturers and industry partners.

Its Chairman, ***Marc Fleschen,*** *in interaction with* ***Pratima Harigunani,*** *shares his perspectives on Li-Fi's current status, the questions still to be addressed, and how the LCA is shaping the technology's future. Excerpts:*

How would you define Light Communication for a non-technical audience?

Light Communication (LC), encompassing technologies such as Li-Fi and Optical Camera Communication, represents a profound shift in connectivity. By harnessing the expansive, unlicensed light spectrum for data transmission, LC offers a sustainable solution to the pressures on traditional radio frequency (RF) networks. It addresses spectrum scarcity, inherent security vulnerabilities, and increasing ICT energy consumption.

How does Li-Fi compare with Wi-Fi and existing wireless systems?

LC offers advantages in data speed, military-grade security, immunity to electromagnetic interference (EMI), and spectrum efficiency. The objective is not to replace Wi-Fi but to complement it—deploying LC where its unique strengths provide maximum value. Together, they form heterogeneous, converged networks with better performance, stronger security, and higher sustainability.

What improvements does Li-Fi bring in terms of speed and bandwidth?

Li-Fi can deliver several gigabits per second for commercial applications. Laboratory demonstrations have shown access points aggregating 2 Terabits per second (Tbps) using Vertical Surface Emitting Lasers (VCSELs) in a Multiple Input Multiple Output (MIMO) configuration, with energy consumption under 2 Watts. That translates to energy efficiency close to 1 pJ/bit—a requirement of 6G. This throughput is enabled by lasers and the reusability of the visible and infrared spectrum, unlike the congested and licensed RF spectrum.

What advantages does Li-Fi offer in terms of security and privacy?

A standout feature of Li-Fi is physical-layer security. Light waves do not penetrate walls, so signals are confined within a room or defined space. This makes interception extremely difficult and is often described as 'military-grade security'. What some see as a limitation actually makes Li-Fi ideal for high-security or sensitive applications, including Fixed Wireless Access (FWA) configurations.

What are the enterprise use cases and latency benefits?

Li-Fi is designed to integrate with the Internet of Things, enabling advanced Industry 4.0 use cases. It supports massive device connectivity, ultra-low latency, and secure machine-to-machine communications. This makes it well-suited for industrial control, mission-critical processes, gaming, or video conferencing—applications where responsiveness and reliability are non-negotiable.

How does Li-Fi contribute to sustainability goals?

It promises significant reductions in energy consumption, directly contributing to CO_2 emission reduction targets and supporting the transition to a greener digital future.

What are the main limitations or barriers to adoption?

The first challenge is line of sight. Walls or obstructions block signals, which limits pervasive coverage but simultaneously enhances security and interference immunity.

Second, environmental factors play a role. Outdoors, Free-Space Optical Communication (FSO) can be disrupted

MARC FLESCHEN
Chairman, Light Communications Alliance

> Li-Fi uses light waves to deliver multi-gigabit speeds while confining signals within walls, ensuring both ultra-efficiency and military-grade security.

by fog, rain, or dust. Indoors, strong ambient light can affect signals, though modern systems adapt well.

Finally, infrastructure is key. Adoption requires Li-Fi-enabled LEDs or VCSEL lighting and compatible hardware at the device end. Unlike Wi-Fi, which is ubiquitous, Li-Fi will need careful rollout of compatible equipment.

How do Li-Fi and Wi-Fi complement each other in practice?

Wi-Fi offers broad mobility and shared resources, while Li-Fi delivers secure, high-speed, dedicated links in confined spaces. Combined, they ensure seamless coverage. Wi-Fi can provide surface-level connectivity and mobility, while Li-Fi supports FWA and in-building density. This complementarity will shape new network architectures.

What is the strategic perspective of the Light Communication Alliance?

The long-term potential of Light Communication Technology (LCT) lies in convergence. It is not about one technology dominating, but about combining wired and wireless optics for end-to-end sustainable solutions. Wired optics deliver stability and capacity, while wireless optics provide flexible, secure access. Together, they optimise performance, reduce energy use, and adapt to diverse vertical markets.

How will Li-Fi co-exist with 5G and 6G networks?

Li-Fi and 5G/6G together create robust networks that combine RF with visible light or infrared (IR). In Industry 4.0, Li-Fi FWA supports secure, high-rate machine communications, while 5G/6G ensure mobility and broader coverage. This synergy creates holistic, future-ready infrastructures.

What role do channel models, reflecting surfaces, and infrared play in Li-Fi development?

Channel models are essential for network optimisation. They combine line-of-sight and non-line-of-sight scenarios to plan deployments. Optical Intelligent Reflecting Surfaces (IRSs), such as metasurfaces, can redirect light waves to extend coverage, reduce error rates, and improve link reliability indoors.

Infra-red (IR) is also key. Li-Fi uses both visible light (350–700 nm) and IR (800–1000 nm). Typically, IR supports upstream traffic, while visible or IR serves downstream. VCSEL-based IR sources are energy efficient and particularly useful in environments dominated by ambient light.

What is the mandate of the LCA, and how critical are its industry members?

The Light Communication Alliance is a global community of industry leaders, researchers, and innovators committed to advancing light communication. Collaboration is critical because no single player can build this ecosystem alone.

Major telecom players like Nokia and Liberty Global bring strong industry validation. Their work in 5G, 6G, and O-RAN strengthens the case for Li-Fi, while their involvement in the LCA ensures alignment with global standards. Their presence provides the weight needed for interoperability and large-scale deployment.

How is Li-Fi being standardised, and what progress has been made?

Standardisation is pivotal. The IEEE 802.11bb standard, ratified in June 2023, marks a breakthrough. It positions Li-Fi as a complementary technology within the Wi-Fi ecosystem, ensuring interoperability with existing wireless infrastructures.

The standard covers both the physical and medium access control layers for operation over the infrared band (800–1000 nm). It supports bidirectional data transfer from 10 Mb/s to 9.6 Gb/s and ensures compatibility across solid-state light sources with varying bandwidths.

This framework paves the way for mass adoption. By integrating optical antennas into devices alongside Wi-Fi protocols, 802.11bb attracts interest from semiconductor firms and handset manufacturers. Once chipsets are embedded in consumer devices, Li-Fi will move from pilots to widespread deployment.

To read the full interview, please visit the dqindia.com website.

pratimah@cybermedia.co.in

LT GEN DR SP KOCHHAR

SECURITY AND COMPETITION: BALANCING THE TELECOM ACT

The Telecom Act 2023 strengthens security and consumer trust, but gaps in competition, OTT parity, and licensing stability raise new challenges.

In an era defined by hyper-connectivity, digital dependence touches every facet of life and business in India. Against this backdrop, the introduction of the Telecommunications Act, 2023, marked a pivotal legislative moment, meant to modernise the legal framework that governs an industry central to India's digital ambitions. Yet, even with a refreshed framework, certain provisions have triggered deeper conversations around how the Act addresses national security, licensing and equitable competition.

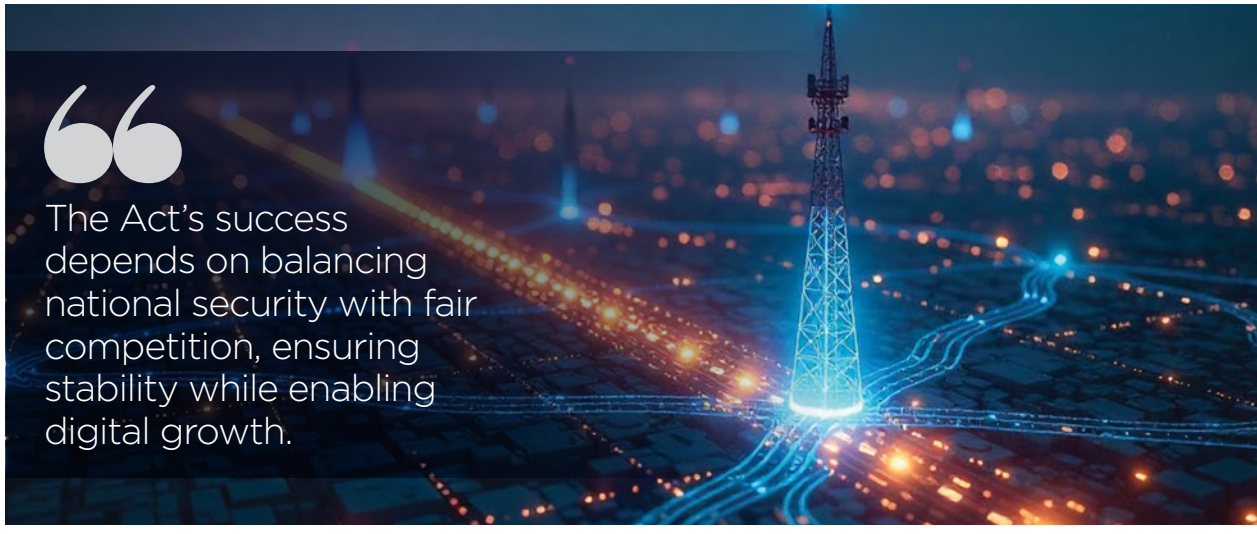
Between 2021 and 2023, India's telecom sector experienced a surge that exposed the limitations of its legacy regulations. Gross revenue climbed from Rs 3.33 trillion in FY2022-23 to Rs 3.36 trillion in FY2023-24, while total telephone subscribers grew from 1.17 billion to 1.19 billion in the same period.

Broadband subscriptions increased by 9% to 924 million, and the Number of Internet users rose 8.3% to 954 million. Data consumption exploded by nearly 22%, driven by rapid smartphone adoption and 5G rollouts. Foreign investments and strong user growth pointed to an industry in transformation. Yet, these dynamic trends underscored the urgent need for a modern, flexible telecom law to govern emerging technologies, consumer habits and sectoral expansion.

The need for a new telecom law was clear. The previous Indian Telegraph Act (1885) and Wireless Telegraphy Act (1933) were not equipped for a landscape disrupted by data, satellite Internet, Over-the-Top (OTT) platforms and the Internet of Things. Thus came the Telecommunications Act, 2023, built on the principles of inclusion, security, growth and responsiveness to the changing technological environment.

NATIONAL SECURITY AND COMPLIANCE COSTS

Section 20 (2) of the Telecom Act empowers the government to suspend the transmission of messages,



The Telecom Act brings stronger safeguards and modern rules, but security costs and compliance overlap worry industry stakeholders.

IN BRIEF

- The Telecom Act 2023 modernises governance but raises challenges in balancing national security and industry competitiveness.
- Security powers strengthen resilience, but excessive compliance without cost-sharing could burden telecom operators.
- Shifting from contracts to authorisations creates uncertainty for investors and fails to resolve AGR revenue disputes.
- Uneven spectrum pricing for satellite versus terrestrial operators threatens fair competition and digital sovereignty.
- OTT platforms escape regulation, creating a competitive imbalance and adding security risks to India's networks.
- Consumer safeguards and Right-of-Way reforms offer positives, but practical implementation remains critical.

intercept communications and impose controls for national security and public order. Such powers are certainly not new; legacy laws also permitted similar interventions. The sector acknowledges that in a world of escalating cyber threats and borderless digital risks, proactive national security measures are vital for safeguarding citizens and critical infrastructure.

However, telecom service providers (TSPs) already comply with overlapping obligations regarding security mandates from various security agencies. Hence, there should not be any additional or avoidable compliance burden on TSPs that imposes unnecessary costs on the industry. Furthermore, it is important to envisage and implement a cost-sharing mechanism between TSPs and LEAs or user government departments to meet the security requirements.

Moreover, the Act restricts the authorisation of Internet shutdowns to the central government, thereby ensuring continued, uninterrupted and seamless telecom connectivity for all citizens. While some industry voices advocate for ongoing clarity in procedural safeguards and technical standards to preserve user trust and privacy, there is a broad recognition that robust security measures are foundational for a resilient and truly digital India.

LICENSING OVERHAUL AND AGR UNCERTAINTIES

One of the Act's most challenging reforms is the overhaul of the licensing regime. The new service authorisations plan to replace time-tested contractual license agreements between telecom operators and the Department of Telecommunications (DoT) with a government-issued authorisation process. Side-lining this contractual stability could introduce regulatory uncertainty, undermine investor confidence and deter long-term capital commitment. These arrangements have driven enormous investment and expansion in the sector over three decades.

Additionally, the calculation of Adjusted Gross Revenue (AGR), which is critical for determining government levies and dues, remains inadequately addressed. The industry has repeatedly advocated for revenues from licensed telecom activities to be considered as a part of AGR. This reform was unfortunately omitted even in the later TRAI recommendations tied to the Act.

SATELLITE SPECTRUM AND DIGITAL SOVEREIGNTY

The government has introduced security measures such as mandatory localisation of key network functions within India, geo-fencing to restrict cross-border data flow and prohibited the decryption of Indian data outside the country to mitigate risks.

Nonetheless, disparities in pricing and obligations between satellite and terrestrial operators, along with worries about foreign control over sensitive

> Unequal treatment of satellite operators and OTT platforms risks distorting competition in India's digital economy.

communications, highlight vulnerabilities in India's security framework.

A balanced, transparent spectrum policy is essential to ensure satellite connectivity supports, rather than undermines India's digital sovereignty and national defence.

OTT EXCLUSION AND NATIONAL SECURITY RISKS

Beyond spectrum and authorisation reforms, a pressing concern is the exclusion of app-based communication services from the regulatory framework. Despite offering similar critical services, these platforms operate outside licensing norms, unlike telecom operators who must meet stringent compliance and security obligations. This disparity creates regulatory arbitrage, undermines fair competition and raises national security concerns.

The sector is already under financial pressure from high spectrum fees and legacy dues, limiting investments in infrastructure. Meanwhile, App based communication services handle a large share of communication traffic without contributing to network upkeep, further straining operator revenues.

Additionally, the absence of oversight over app-based communication services creates security vulnerabilities. While licensed telcos adhere to strict interception and data protection rules, unregulated services can become entry points for cyber threats. Addressing this gap through balanced regulation is essential to safeguard the integrity and resilience of India's telecom networks.

CONSUMER PROTECTION AND INFRA REFORMS

Despite these concerns, the Act does introduce forward-looking features, particularly in consumer data protection and infrastructure development.

The Act introduces vital consumer protection and anti-spam measures to address the growing threat of cyberattacks such as data breaches and ransomware, which pose risks to national security and public safety. It mandates prior user consent for commercial messaging, enforces the maintenance of Do Not Disturb (DND) registers, and strengthens grievance redressal mechanisms to shield consumers from unsolicited communications and spam.

Alongside these, the Act enforces robust data localisation requirements and enhances privacy safeguards, aligning with global standards and India's vision to set new benchmarks in data privacy. These measures ensure that user data remains secure from unauthorised access and misuse, thereby fostering greater consumer trust and confidence, critical foundations for realising Digital India's aspirations.

Building on this momentum, the Act also simplifies Right-of-Way procedures, allowing telecom operators streamlined access to public and private lands for deploying vital infrastructure such as cables and towers. This modernisation reduces duplication of efforts and cuts costs, expediting network expansion. All that remains here is the uniform and effective implementation by local authorities to fully unlock their potential in accelerating digital infrastructure growth.

BALANCING STABILITY WITH DIGITAL AMBITION

As India marches towards becoming a digitally empowered society, the Telecom Act is both an enabler and a catalyst for change. It attempts to modernise India's telecom governance, with strong steps toward consumer protection, infrastructure ease and digital sovereignty. But as implementation unfolds, key concerns remain.

To truly deliver on its promise, the Act must retain the contractual stability that has long guided industry investment. Spectrum allocation, especially for satellite and enterprise use, must be equitable to avoid scarcity for core operators. Crucially, regulatory parity with OTT communication platforms is essential to ensure both fair competition and national security.

While the Telecommunications Act, 2023, is a critical step forward, clear, consistent policies and a level playing field are essential to align it to the digital future that the country and its people deserve.

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

[USE CASE]
CLOUD

GPU cloud: Retail's new engine of relevance

Retailers must shift from basic personalisation to hyper-relevance, using GPU cloud to deliver fast, scalable, and privacy-first experiences.

BY NARENDRA SEN

Personalisation in modern retail is a must-have and not a nice-to-have any more. It is table stakes and not a competitive edge a business has over another. Retail platforms of today are expected to understand their consumer instantly—from curated recommendations to predictive search. The key question is no longer whether businesses can personalise, but how to personalise for consumers.

To retain customers, businesses must customise quickly, at scale, and with precision. This is where the graphics processing unit (GPU) cloud comes in—the silent powerhouse enabling the next generation of intelligent, hyper-relevant retail experiences.

THE SHIFT TO HYPER RELEVANCE

A decade ago, personalisation meant addressing customers by name in an email. Today, it is about predicting what they want or need even before they can type it. This shift to hyper relevance requires real-time analysis of context, intent, and behaviour—all delivered in milliseconds.

It is not simply about enhancing user experience but also a test of a platform's infrastructure readiness and AI maturity. Businesses are turning to GPU cloud infrastructure to process massive volumes of behavioural data in real time.

Purpose-built GPUs, unlike CPUs, enable lightning-fast model inference, powering hyper-personalised experiences at scale. A GPU-powered backend ensures AI keeps up with customer expectations—whether serving millions of recommendations or dynamically adjusting pricing and promotions.

SPEED EQUALS REVENUE IN RETAIL

In retail, milliseconds matter. A delay as small as 100 milliseconds can result in a significant drop in conversion rates. Platforms must interpret behaviour instantly and respond with intelligent suggestions to keep customers engaged and purchasing.

Speed equals revenue in retail, with even a slight delay of just 100 milliseconds leading to a significant drop in conversion rates.

Platforms must interpret behaviour instantly and respond with intelligent suggestions to ensure customers stay, shop, and buy.

GPU cloud enables sub-second inference, transforming personalisation into a real-time advantage. A GPU-driven platform maintains AI responsiveness, user experience stickiness, and lower cart abandonment rates.

GPUS FUEL RETAIL AI INNOVATION

Traditional CPU-based systems, while reliable for core operations, fall short when handling high-speed inference, multi-modal data, and real-time learning. Personalisation at the hyper-relevance level cannot run on autopilot, as powerful AI models such as deep learning networks demand immense processing capacity.

While both CPUs and GPUs play their roles, CPUs are what keep the lights on by managing core operations, such as transactions, databases, and web servers. GPUs, on the other hand, are what light the fire. All the heavy lifting, such as image recognition, natural language processing, recommendation engines and generative AI, in short, all modern AI workloads are taken up by GPUs.

CPUs maintain the foundation, but GPU-powered cloud fuels the intelligence and agility required for hyper-personalised experiences. Crucially, GPU cloud platforms scale AI workloads for millions of users, instantly and cost-effectively.

REAL-WORLD AI USE CASES IN INDIA

The use of GPU cloud is already prevalent among Indian retailers, helping them transform the shopping experience for their customers. Image recognition models are being trained and accelerated on GPU infrastructure to power visual search and instant discovery. Live clickstream data is fed into AI models running on a GPU cloud, enabling real-time recommendations.

Retailers are also using GPU-powered models to forecast demand by location, helping optimise inventory and fulfil ultra-fast deliveries.

There has been a heightened focus on data governance and security since the introduction of India's Digital Personal Data Protection (DPDP) Act. While consumers want customised experiences and personalised recommendations, there is also an emphasis on privacy.

GPU cloud providers are rising to the occasion with sovereign and secure environments allowing retailers to train and deploy proprietary AI models on their own datasets in compliant and encrypted enclaves.

The result: personalisation that is both privacy-first and powerful.

PERSONALISATION REIMAGINED

The integration of generative AI is fuelling creativity and automation in retail. Content can be tailored to target multiple demographics by having multiple AI-generated descriptions for a single product to attract urban buyers, heritage enthusiasts or even to optimise SEO. It can be created and deployed instantly.

GPU clouds running LLMs are enabling conversational assistants for virtual shopping that can now handle more nuanced requests such as, "Find a shirt that is office-appropriate for Mumbai weather."

This is not just automation but a reimagination of personalisation at scale.

SCALE: NOT OPTIONAL BUT A STRATEGY

Retailers across the board today need a compute strategy that aligns with their AI ambitions. The strategy needs to be adaptive and intelligent. This step will determine a retail company's ability to deliver relevance instantly, at scale and without compromising on data ethics or performance, making GPU cloud a strategic imperative.

Investing in GPU cloud today is not just a technical upgrade; it is how retailers future-proof their platforms to deliver experiences that are fast, flexible, and trustworthy. In the race for relevance, infrastructure is no longer backstage; it is the main act.

TThe author is the Founder and CEO of NeevCloud.
feedbackvnd@cybermedia.co.in

Modernising OTT for a hyper-connected audience

OTT platforms are evolving with microservices, AI-driven content workflows, and smart CDNs to deliver seamless experiences at a global scale.

BY SARVANRAJA NADAR

With digital entertainment now being consumed on devices, in time zones, and across geographical regions, over-the-top (OTT) services have evolved from mere video-streaming solutions to sophisticated technology platforms. The core architecture of OTT infrastructure is being reimagined end-to-end in reaction to increasing viewer expectations and demands during live events or global releases.

Three key pillars fueling this change are: integrated content lifecycle management, elastic cloud infrastructure on a microservices foundation, and cognitive content delivery networks (CDNs) optimising Quality of Experience (QoE).

FROM MONOLITHS TO MICROSERVICES IN OTT

The legacy monolithic architectures, once a standard in OTT, are now falling short when it comes to concurrency and performance expectations of today. In a monolithic architecture, the components of an application are strongly coupled together, making them hard to scale selectively. Any increase in user activity—whether log-in, playback, or payments—compels the whole system to scale, which leads to resource inefficiencies and higher costs in infrastructure.

Microservices-based designs address this challenge by compartmentalising OTT applications into separate services—such as login, content display,

> Microservices enable OTT apps to scale login, playback, or payments independently, resulting in efficiency without resource wastage.

recommendations, advertising, and subscription flows. Each can scale independently as needed. A sample is a login service that would need to scale rapidly during a popular live event, while content recommendation services would require less frequent scaling.

This design pattern is being merged with ease by modern-day cloud platforms, where microservices run in lightweight containers or pods. These can be automatically scaled based on real-time usage patterns, ensuring resources are utilised to their optimum. OTT players like Netflix and JioHotstar have successfully implemented this pattern.

MANAGING CONTENT LIFECYCLE WITH AI

The success of OTT is largely dependent on content, but it is the agility of content that sets leaders apart. Ingesting, processing, curating, tagging, and publishing media of different kinds geographically and across platforms—while ensuring compliance and localisation—is a gargantuan task without an integrated system.

A central, Artificial Intelligence or AI-powered content lifecycle management platform helps OTT players streamline this complex process. Whether it is auto-creating multilingual subtitles, moderating content appropriateness in sensitive geos, or tagging metadata to facilitate discovery and recommendation—automation is the operative word.

For instance, when delivering European content to Indian or Middle Eastern markets, it could be AI-dubbed, subtitled, or even content-moderated based on local laws. Instead of processing all these steps manually, modern-day platforms have adopted a one-touch model in which adding a piece of content with regional publishing rules automatically triggers respective processing pipelines.

They also use integrated content platforms that enable them to oversee rights handling, geo-fencing, parent ratings, and optimising publishing workflows across franchises from one point of control. Not only does it lower operational costs, but it also reduces time-to-market and guarantees consistent quality across markets.

SMART CDNS FOR QUALITY OF EXPERIENCE

As OTT consumption extends across devices from smartphones to smart TVs, providing a consistent and high-quality viewing experience is crucial. Quality of Experience (QoE) is now as valuable as the content itself. OTT players are increasingly using smart CDNs and AI-driven technologies to optimise streaming. Content-aware encoding makes it possible to encode bandwidth efficiently without visually degrading.

For example, AI can decode high-definition video from standard-definition content on edge devices to provide better playback quality on devices that use less data.

Real-time monitoring tools track critical performance metrics, including content start time, buffering, and API response time. These statistics enable platforms to change CDNs dynamically during times of high usage, a strategy used by providers like Amazon Prime and Hulu. YouTube responds to network and device conditions using adaptive bitrate streaming at the edge for continuous playback.

With the optimisation of CDN routes and dynamic content delivery optimisation based on user location, device capability, and network speeds, platforms can offer rich experiences of watching even in times of heavy traffic.

REDEFINING OTT PLATFORMS FOR THE FUTURE

OTT platform transformation goes beyond backend optimisation. It is an intrinsic redefinition of entertainment production, management, and consumption in a world of hyper-connectivity. By replacing monolithic microservices architecture, consolidating content operations, and using AI for QoE optimisation, leading OTT players are creating digital platforms that are intelligent, scalable, and future-proof.

In a universe where user attention is the most valuable currency, the ability to deliver seamless, personalised, and world-class streaming experiences will be the winners of the next OTT era. It is not about getting content delivered—it is about designing delight, at scale. 😍

The author is the OTT Practice Head at Tata Elxsi.
feedbackvnd@cybermedia.co.in

Fibre or 5G? Convergence may be the real superhero

Fibre brings stability and 5G adds reach, but convergence offers enterprises the most resilient path to future-ready connectivity.

BY PRATIMA HARIGUNANI

Superman flies at astonishing speeds across the sky and has X-ray vision. Spiderman, by contrast, spins webs from his wrists but manoeuvres deftly across any landscape. Superman can hear sounds from miles away in space. Spiderman is no less powerful, with his 'spidey-sense'. Both save the day – and sometimes a stranded cat on the 40th floor. Each has a weakness too – Kryptonite or ethyl chloride, a red sun or water.

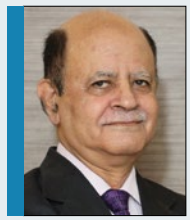
Preferences often depend on whether we live in a DC or Marvel universe. Choosing between them is not easy. A similar dilemma confronts enterprises today: whether to rely on 5G or fibre for connectivity. Spectrum or physical networks – both bring superhero-like strengths. The way forward, experts argue, may lie in convergence, where 5G's reach is reinforced by fibre's reliability, with each technology leveraged for its unique advantage.

John Strand, CEO of Strand Consult, frames the debate in enterprise terms. "What we are talking about is fibre vs. 5G MBB vs. 5G FWA. The question is which infrastructure can service corporate or enterprise customers best. Different customers have different needs. In some areas, fibre competes with 5G. In others, fibre supplements 5G. In many cases, they will co-exist side by side."

Before considering convergence, it is worth weighing their strengths separately.

5G: THE SKY HERO OF CONNECTIVITY

In terms of scalability and reach, 5G is often the first



"Private 5G is no shortcut: spectrum, equipment, and expertise add heavy capex that many enterprises cannot shoulder alone."

LT GEN DR SP KOCHHAR
Director General, COAI

choice. Spectrum-based solutions such as 4G and 5G private networks offer flexibility for mobile or remote devices across industrial sites, according to Sachin Arora, Head of Connectivity and IoT at Giesecke+Devrient, India.

From a return-on-investment perspective, 5G enables faster value realisation where laying fibre is cost-prohibitive or geographically difficult, said Stan Gray, SVP IoT Broadband and High Cat Vertical Sales, Telit Cinterion. "Its wireless nature reduces upfront infrastructure investment and accelerates deployment, particularly for dispersed operations. Fibre, on the other hand, often has a longer lifespan and lower operational costs once installed, which makes it highly efficient in fixed environments."

Gray added that 5G offers mobility, rapid deployment, and the ability to support devices at scale, particularly in IoT and edge computing.

Recent industry trends reinforce this preference. Strand cited that since Telia rebranded as Norlys in May 2025, even within its fibre footprint, Norlys has prioritised 5G mobile broadband (MBB) over fibre. Fibre-only brands such as Hiper have also launched 5G MBB. Telenor, over the past two years, has consistently promoted 5G MBB to end customers before fibre. Strand said he expects the decline in fixed broadband subscriptions to have accelerated in 2025, given rising fibre BSA wholesale prices and sustained competitive pressure.

Strand believes this shift in the Danish market is driven more by economics than customer demand. "The rise in fibre wholesale prices, combined with intense competition, has left many ISPs financially strained. Service providers that own mobile networks lean towards more profitable 5G offerings."

Cost comparisons further strengthen the case for 5G. Fibre installation, particularly underground, can be expensive due to excavation and labour requirements. A report by Global Market Insights notes that laying fibre

IN BRIEF

- 5G delivers speed, mobility, and scale, making it attractive for IoT and edge cases where fibre rollout is costly or impractical.
- Fibre ensures stability, ultra-low latency, and interference immunity, ideal for mission-critical workloads and industrial operations.
- Private 5G networks require higher capex, spectrum, and skilled resources, making TSP partnerships essential for long-term efficiency.
- Fibre's mature ecosystem offers reliability, while 5G's dynamic ecosystem requires careful interoperability and security checks.
- FTTH Council says convergence can save up to 96% in rollout costs and avoid the 2–3.5× penalty of late fibre deployment for 5G.
- Hybrid fibre backbones with 5G mobility layers are emerging as the preferred connectivity model for global enterprises.

"Fibre's wired security is strong but still vulnerable to cuts, while 5G must lean on encryption, SIM authentication, and zero-trust."

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

optic cables underground can cost up to USD 144,000 per mile in urban areas, factoring in trenching, permits, and restoration. Maintenance challenges, such as breaks and weather-related damage, add further costs. In such contexts, 5G becomes a more attractive option.

FIBRE: THE SKYSCRAPER HERO OF NETWORKS

Fibre remains the gold standard for fixed locations demanding high bandwidth and consistent performance, such as core factory operations, Arora explained.

Latency is another advantage. "Fibre provides ultra-low latency and exceptional reliability, making it suitable for mission-critical workloads. While 5G also delivers near real-time responsiveness, wireless overhead can slightly affect latency," he said.

Gray highlighted the fibre's unmatched stability, extremely high bandwidth, and immunity to spectrum interference. "It is ideal for fixed, high-demand locations where capacity is predictable."

Unused fibre capacity is often cited as a drawback. Gray explained that this usually results from over-provisioning or delayed adoption. While it represents sunk capital, it also offers a buffer for future demand. "The greater short-term risks lie with 5G, especially around security, interoperability, and early deployment challenges," he said.

On security, fibre's wired nature makes it less vulnerable to interception, though physical damage remains a risk. By contrast, 5G requires encryption, SIM-based authentication, and zero-trust design principles to counter its larger attack surface. "Enterprises must embed security from day one," Arora said.

HARNESSING THE POWER OF BOTH WORLDS

The best outcomes often lie in convergence. Just as comic book universes sometimes create hybrid heroes, enterprises can combine fibre and 5G for balance.

"Enterprises should evaluate scalability, latency, and security when choosing between spectrum-based and fibre-based connectivity," said Arora. "The decision should reflect operational needs, mobility, and performance requirements."

Gray pointed out the scalability trade-off. "5G excels in connecting millions of IoT devices, while fibre scales more in terms of bandwidth per connection. Urban enterprises may find fibre more accessible, while rural regions may leapfrog directly to 5G."

Cost also weighs heavily. Lt Gen Dr SP Kochhar, Director General of the COAI, recently argued that private 5G networks entail significant capital expenditures (Capex) for equipment, spectrum, security, and skilled personnel. He said enterprises setting up private networks independently could face unexpected financial and operational burdens.

Strand cited Danish retail pricing to illustrate the swing: in some areas, fibre broadband is DKK 419/month while

"5G lowers upfront costs and speeds deployment, yet fibre proves its worth with longevity and efficiency in fixed environments."

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

"Fibre and 5G are not an either-or choice; sometimes they clash, sometimes they complement, but more often they end up side by side."

JOHN STRAND
CEO, Strand Consult

5G MBB is DKK 249/month; in others, fibre is DKK 319/month against 5G MBB at DKK 249/month. Where fibre pricing is sharper, the uptake balance shifts accordingly.

Vendor ecosystems also influence choices. Fibre has a mature, proven ecosystem with well-defined service-level agreements. 5G, though more dynamic, involves collaboration across telcos, cloud providers, and equipment vendors. This brings innovation but requires careful checks on interoperability and security, Gray said.

Kochhar added that enterprises often underestimate the operational challenge. Unlike telecom service providers (TSPs), most enterprises lack the expertise and scale to manage networks effectively. "With continuous evolution of both technology and ecosystem, frequent upgrades will be necessary, and TSPs are best placed to anticipate and implement them," he said.

Regulation and geography add further complexity. Fibre deployments often face right-of-way and zoning hurdles, while 5G depends on spectrum licensing, which varies across markets. Geography often dictates outcomes: dense urban centres justify fibre's Capex, while remote or mobile-heavy areas benefit from 5G.

A FORK IN THE ROAD OR ON THE ENTERPRISE PLATE

When weighing fibre against 5G, enterprises should view them not as substitutes but as complementary solutions, Gray argued. "The decision is less about choosing one over the other and more about aligning each with business needs. A manufacturing plant may benefit from fibre's reliability, while a logistics network tracking thousands of moving assets may need 5G."

Hybrid architectures that combine fibre backbones with 5G mobility layers are gaining traction. A study by the Fibre to the Home (FTTH) Council highlights the value of reusing existing fibre networks to support future 5G rollouts. Reusing FTTH infrastructure can reduce 5G network costs by up to 22%.

According to FTTH Council Europe's paper on optimising FTTH networks for convergence, high-band 5G (24–40 GHz) can deliver very high capacity but struggles with building penetration and attenuates quickly over distance. That reality necessitates dense small-cell deployments anchored on fibre backhaul.

Vincent Garnier, Director General, FTTH Council Europe, noted that 5G requires high antenna density, which in turn demands a fibre transport network. "The FTTH Council has been exploring synergies between FTTH and 5G deployments," he said.

The FTTH Council also notes that without early convergence, fibre built later for 5G can cost 2–3.5× more. Conversely, an optimally converged FTTH-and-5G design can remove roughly 65–96% of the cost of a standalone fibre network for 5G.

Strand said it is wrong to frame the issue as 5G vs fibre. "Many fibre players are extending fibre with 5G fixed wireless access (FWA) to lower broadband rollout costs. In countries such as India, 5G FWA is widely viewed as a cost-effective way to extend high-speed Internet access, and it is seeing strong uptake in the USA, Brazil and large parts of Africa."

Security remains central to any decision. Gray cautioned that 5G IoT deployments must embed resilience into design, with strong collaboration across vendors, operators, and device makers.

The choice between fibre and 5G, therefore, is not binary. Capex vs latency, reach vs security, control vs bandwidth – these are trade-offs. The solution lies in designing for flexibility and convergence. For enterprises, it may not be a question of Superman or Spiderman, but of Batman: defined not by powers but by decisions. As Batman said, "It is not who I am underneath, but what I do that defines me."

pratimah@cybermedia.co.in

Lost in translation? Edge AI finds the right voice

Speech-to-speech translation is moving from cloud to edge, bringing faster, private, and more natural conversations across languages.

BY RAJESH SUBRAMANIAM

Imagine landing in Tokyo, walking into a cafe, and confidently ordering in English, only to hear your voice echo back in perfect Japanese, complete with your own tone and cadence. No awkward pauses. No robotic inflexion. Just fluid, human-like conversation. This is not science fiction. It is the new frontier of speech-to-speech translation (S2ST), powered by AI and edge computing.

Behind this seemingly straightforward conversation lie decades of technical advancements, strategic shifts in hardware design, and an increasing demand for effortless global communication.

Let us see how we arrived here and what is next.

THE EVOLUTION OF S2ST: FROM FRANKENSTEIN TO FLUENT

In its early stages, speech translation was a patchwork of three stand-alone technologies: Automatic Speech Recognition (ASR) to translate voice into text, Machine

> Voice-first communication is emerging as the new standard, where speed, accuracy, and emotion define the future of multilingual dialogue.

AI-powered devices are shifting translation from a convenience to a necessity, reshaping global business, travel, and human connection.

Translation (MT) to change the language, and Text-to-Speech (TTS) to recite the output. Each one was impressive in isolation, but together, they fell short, as minor errors added up, creating jumbled outputs, while lags disrupted the flow of natural conversation.

Then came neural machine translation. With deep learning, AI began to understand context, tone, and even emotion. Meta's SeamlessM4T and Google's SimulTron are standout developments, translating speech directly from one language to another—preserving not only meaning but also melody. However, these systems required immense computing power—until the cloud entered the scene.

CLOUD POWER: FIRST BREAKTHROUGH AND ITS LIMITATIONS

Technology behemoths such as Google, Microsoft, and Alibaba launched APIs that enabled multilingual apps to be plug-and-play. However, S2ST in the cloud had its limitations: it was dependent on Internet connectivity, which usually introduced additional delay (latency), and raised serious concerns about data privacy.

This puts people in need of a solution that would have cloud-level intelligence without the cloud.

Step forward, and enter Edge AI.

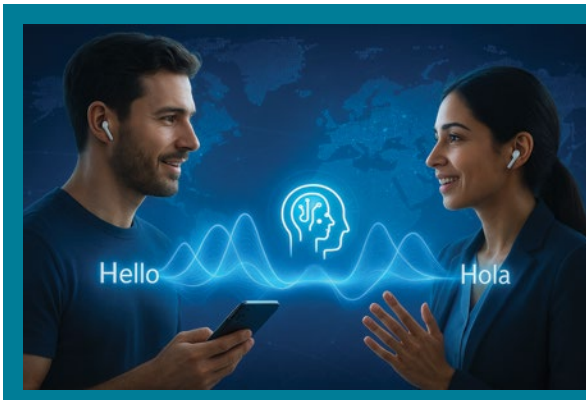
EDGE AI: REAL-TIME, RIGHT WHERE YOU ARE

Edge computing brought the AI "brain" closer to home—onto one's phone, smartwatch, and even the earbuds. Thanks to chips like Apple's Neural Engine and Google's Tensor, devices can now perform real-time translation offline.

Google's Pixel offers offline translation in its Live Translate and Interpreter Mode, while Apple's Translate app supports this for select languages. These algorithms work at lightning speed, processing input every 40 milliseconds, enabling real-time speech without pinging the cloud.

But this evolution is not just about speed—it is about control. Data remains local. Words no longer need to travel across the globe and return with a lag. In regions with weak connectivity—remote towns, disaster zones, or even 35,000 feet in the air—edge-powered translation ensures conversations continue uninterrupted.

For example, at a cafe in Paris, a Korean tourist orders coffee using the phone's offline Live Translate feature. As she speaks Korean, the Pixel instantly translates it into fluent French for the barista—without Internet access. When the barista responds, the phone translates back in



IN BRIEF

- Early speech translation relied on ASR, MT, and TTS, but errors, lags, and robotic tones disrupted natural conversations.
- Neural models brought fluency, tone, and emotion, yet dependence on the cloud caused latency, privacy issues, and uneven access.
- Edge AI enables offline, real-time translation on phones, earbuds, and wearables, making cross-language dialogue seamless.
- Latency challenges are tackled with consensus-based strategies, stream ASR, and faster TTS, cutting response times sharply.
- Smart translation hardware—earbuds, devices, and AI-driven phones—is fuelling rapid growth in global multilingual markets.
- Next-gen tools like emotion-aware synthesis, hybrid systems, and smart glasses will redefine voice-first communication.

> Edge AI ensures secure, real-time speech translation, enabling inclusive conversations even in remote regions with weak connectivity.

real time. No awkward pauses, no language barrier—just seamless, natural conversation over a cappuccino.

So, one may ask who wins the race between Edge and Cloud?

In a test of 8,400+ users and 6,300+ servers, 58% of customers hit edge servers in under 10 milliseconds, versus just 29% for cloud servers. In under-resourced areas such as Africa and Oceania, edge computing showed 90% lower latency than cloud. Even in highly connected regions like North America and Europe, Edge remains the winner.

FIXING LATENCY IN REAL-TIME TRANSLATION

Latency, which is the lag between speaking and hearing a translation, is the weakness of real-time translation. Reducing it is critical to deliver smooth user experiences. To address this, scientists have come up with different strategies. One is the 'Wait-k strategy', which waits until a predetermined number of words arrive. While the translation is accurate, it is a bit slow. A more dynamic strategy is "consensus-based" translation, which triggers output as soon as the model gains enough confidence.

Meanwhile, stream-based ASR now processes audio in small chunks, rather than waiting for complete sentences, which cuts translation time by up to four seconds (though it requires ~18% more computing power). On the flip side, TTS in speech-to-speech systems has learned to speak on the fly, even before a sentence is complete. While this can sometimes cause awkward phrasing, smart techniques like pseudo-lookahead help keep the speech natural and trim response time even further.

SMART HARDWARE: EARS THAT LISTEN, CHIPS THAT TALK

Real-time translation is no longer limited to apps—it now lives in specialised devices, earbuds, and smartphones, each built for different needs. Dedicated tools like the Vasco V4 offer always-on global connectivity and OCR for seamless travel use. Wearables, such as Timekettle earbuds, enable natural conversations with low-latency translation, while smartphones with on-device AI, like Google's SimulTron, excel in offline or noisy settings. Together, these smart hardware solutions are making multilingual communication more effortless, everywhere.

Industry reports indicate that the S2ST market is expected to double from USD 454.4 million in 2024 to USD 881.7 million by 2033, and the real-time translation industry is projected to reach USD 1.8 billion by 2025.

Globalisation and localisation are no longer purely strategic choices; they are now having tangible impacts, with some sources indicating a 3x ROI or higher. This is especially true in the healthcare and public sectors, where real-time translation ensures equitable access. In finance and law, localised AI upholds data sovereignty, trust, and compliance. Meanwhile, e-commerce giants are increasingly describing their products in different languages to expand sales internationally, customising content for every region. By 2025, 30% of all new gadgets will come with built-in translation features, driving both interaction and commerce across cultures.

THE FUTURE: SMART GLASSES, EMOTION-AWARE TRANSLATION

S2ST is evolving beyond earbuds and phones. Hybrid systems with human editors, emotion-aware speech synthesis, and AI-powered smart glasses are setting new standards. The Asia-Pacific region, led by India and Japan, is expected to dominate the market by 2030, particularly in multilingual e-commerce and healthcare.

Startups like DeepL are also reshaping the market, competing with Big Tech through niche precision in legal and technical translation.

The future of communication is not text-based but voice-first. Whether in a boardroom, hospital, airport, or classroom, real-time multilingual conversation is quickly becoming table stakes. With edge AI, that conversation is now fast, secure, and personal. Today, technology is not just translating words, it is translating human experience, in real time.

So, the next time you step into a cafe in Tokyo, do not be surprised if the only thing lost in translation... is nothing at all.

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

DATAQUEST 40+ YEARS THE BUSINESS OF INFOTECH

CyberMedia

DATAQUEST SEPTEMBER 2025 EDITION: THE HUMAN–MACHINE RENAISSANCE BLENDING EFFICIENCY WITH EMPATHY

ALSO READ MORE ON

- Indian factories and automation: The 'everything bagel' is here
- Why context, not just data, will define the future of AI in finance - Jayanth Saimani, Intuit
- Intelligent Drones for Industry 5.0 - Agnishwar Jayaprakash, Garuda Aerospace
- In the Age of AI, What It Really Means to Be a Software Professiona - Dr. Pavankumar Gurazada, Great Learning
- Cloud Sovereignty: Feature. Bug. Feature. Repeat!
- Pharma's industry 5.0 moment: Human + Machine, smarter together - Braj Panda, Dr. Reddy's

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

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

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

[COMMENTARY]
QUANTUM

Building India's quantum backbone with QKD

India's push for QKD networks is reshaping security, demanding policy clarity, legal reform, and early adoption to protect national infrastructure.

BY GAURAV SAHAY

For a country like India, with its vast and sensitive infrastructure across governance, defence, and financial sectors, the development of a quantum communication backbone is not just an aspirational goal but a national imperative. Drawing lessons from the recent and ongoing Operation Sindhoor, quantum key distribution (QKD) has emerged as a critical frontier in securing communications.

Quantum technology provides a secure communication solution that is resistant to attacks, including those from future quantum computers. India's early steps in this direction, through institutional engagement and pilot initiatives, reflect both the strategic significance and the complex regulatory ecosystem within which such technologies must operate.

The value of quantum-secured communication lies in its ability to redefine data protection and national security frameworks. For India, it represents a formidable enhancement of confidentiality and integrity across its information ecosystem. The potential for adversarial states or actors to compromise existing encryption protocols poses an imminent risk to the nation's digital sovereignty. QKD directly mitigates this risk by raising the security threshold to a level that cannot be breached without detection.

POLICY FRAMEWORKS FOR A QUANTUM SHIFT

Integrating QKD into India's critical infrastructure would significantly reduce reliance on legacy encryption protocols that are vulnerable to foreseeable advances in computing. This technological shift aligns with

> Integrating QKD into India's critical systems is more than technology—it is a sovereign imperative for digital security and resilience.

national cyber and data protection policies, as well as the objectives of the Defence Cyber Agency and other security stakeholders.

From a regulatory perspective, QKD deployment may require new legislative provisions or amendments to existing laws. These would need to address quantum-safe protocols, lawful interception thresholds, and standards for validation, certification, and liability. Its integration into defence, space, and public service systems thus goes beyond technological progress—it is a sovereign imperative to secure India's communication architecture against escalating geopolitical, technological, and cyber threats.

India has already recognised this potential, with multiple pilot projects demonstrating the viability of QKD networks. Agencies such as C-DOT, DRDO, and ISRO are spearheading these efforts. However, full-scale commercialisation remains a multifaceted challenge that requires harmonisation of technology readiness, legal frameworks, and market incentives.

Currently, India's legal and policy structures are not adequately tailored to regulate or facilitate quantum communication. Critical questions remain around data sovereignty, export control of quantum equipment, certification protocols, and lawful interception in quantum networks. While the Digital Personal Data Protection Act, 2023, covers general data protection principles, it does not yet address the specificities of quantum-safe systems.

Moreover, the deployment of QKD networks in government and defence contexts will require distinct legal treatment compared with commercial applications. Protocols must be developed for standardisation, interoperability, and liability in cases of breach or malfunction. This could involve amendments to existing laws or the establishment of a dedicated legal framework for quantum technologies. International cooperation, especially in harmonising standards and export controls through multilateral forums such as the Wassenaar Arrangement, will also influence India's policy approach.

FINANCIAL SECTOR AS THE FIRST MOVER

The financial sector presents a compelling case for early adoption of QKD. Banks, stock exchanges, and payment gateways manage vast volumes of confidential and time-sensitive data. With the advent of quantum computing, the threat to public-key cryptography—on which current financial infrastructure depends—is no longer hypothetical. Institutions such as the Reserve Bank of India and the Securities and Exchange Board of India must proactively assess quantum risk and incorporate QKD-based solutions into their cybersecurity frameworks. This will necessitate sector-specific plans, compliance mechanisms, and legislative amendments.

The commercialisation of QKD in India will depend on multiple factors. A clear national roadmap, as outlined in the National Mission on Quantum Technologies and Applications (NM-QTA), must be accelerated with strong public–private partnerships. Policy must establish time-bound goals for trials, ecosystem development, indigenous hardware development, and talent creation. Regulations must be forward-looking to avoid retrospective compliance challenges. Investments from startups and academia should be supported with tax incentives, procurement mandates, and balanced intellectual property reforms.

Integration of QKD into existing telecommunication infrastructure, particularly BharatNet and the 5G backbone, could catalyse deployment at scale. This would not only secure India's digital infrastructure but also generate opportunities for export-led innovation. However, issues such as cross-border data flows, cybersecurity audits, and third-party vendor obligations will need to be reassessed in light of quantum-enabled systems.

India's journey towards building a QKD-powered backbone is now at a decisive juncture. While pilot projects are promising, the commercial and strategic value of QKD can only be realised through a legally robust and forward-looking policy framework. This will require coordination among science, industry, law, and security agencies. By embracing anticipatory governance, accountability, and international alignment, India can secure its digital sovereignty and establish itself as a global leader in the quantum revolution.

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

[COMMENTARY]
GEOPOLITICS

Security by design: Defence, aerospace and derivative hedges

Combat-proven platforms, civil aviation muscle and market hedges form a tri-layer shield that stabilises capital and dampens geopolitical shocks today.

BY NITIN SINGH

Defence production and exports serve not only as economic assets but as political risk management instruments. Countries that can export defence technologies increase their diplomatic influence. When countries are combat-tested, their defence products gain global traction, insulating them through export diplomacy. For instance, during the 2024–25 Israel–Iran conflict, Israel's effective use of Iron Dome and David's Sling systems led to a surge in export interest from Germany, the Czech Republic, and Gulf states.

Similarly, India's Operation Sindoor in May 2025 showcased the operational maturity of the indigenously developed BrahMos cruise missiles and Tejas fighters, spurring export interest across Southeast Asia and Africa.

Such sales build political alignment, and importing nations become stakeholders in the exporter's political stability. Defence deals increasingly include co-production and long-term training contracts, which anchor bilateral relations beyond transactional terms. This pattern has been evident in the India–Philippines BrahMos deals and the Israel–Germany Arrow 3 contracts, which emerged following regional instability.

AEROSPACE AS POLITICAL RISK SHIELD

The aerospace sector has helped nations to immunise

> Export diplomacy works because buyers inherit doctrine, training and supply chains—an umbilical that makes political estrangement costly and unlikely.

> Aerospace is the quiet guarantor: satellites, MRO, and lift give states room to manoeuvre when sanctions bite or borders harden, and alliances remain intact.

IN BRIEF

- Defence exports act as a form of political risk insurance, expanding leverage and shaping long-term alignments between sellers and buyers.
- Combat-proven systems drive demand—Iron Dome, David's Sling, Tejas, and BrahMos have garnered interest, shifting buyers toward validated suppliers.
- Deals now bundle co-production, training, and long-term maintenance, creating lock-ins that tie security postures and policy choices together.
- Dual-use fleets, space systems, and India's GIFT City leasing drive autonomy and reduce logistical chokepoints.
- Short, high-intensity conflicts with quick de-escalation make arms exports instruments of deterrence and political insurance.
- Markets matter too: futures, options and immunisation tactics stabilise cash flows and balance sheets during geopolitical shocks.

themselves against political risk. For example, aerospace influences political risk through dual-use exports, space-based systems, and regional aviation dominance.

Israel's precision airstrikes using F-35I Adirs and loitering UAVs during the 2025 Iran conflict reinforced its stature as a high-tech aerospace exporter. This led to accelerated defence procurement talks with Romania, Finland, and India to acquire or license UAV and missile tech.

Aerospace exports help establish long-term maintenance contracts, training programmes, and supply chains that lock in bilateral dependencies. A robust domestic civil aviation ecosystem enhances connectivity and economic integration, thereby reducing political fragmentation.

India's push to develop aircraft leasing in GIFT City is aimed at reducing reliance on foreign OEMs like Boeing and Airbus after recent political blockades. Civil aviation also provides dual-use capability: during crises, commercial fleets can be mobilised to move troops and evacuate civilians. This adaptability reduces the country's exposure to external logistical choke points.

Countries are constrained to adopt a model of conflict characterised by short-duration, high-intensity engagements followed by rapid de-escalation, which represents a new equilibrium of nuclear-backed, limited war in South Asia. These events highlight a trend where arms exports are not just commercial exchanges, but tools of political insurance that immunise buyers and sellers against future political risks.

DEFENCE EXPORTS AS POLITICAL HEDGES

Defence importers increasingly prefer platforms that have proven effective in live combat, as demonstrated by Israel's Iron Dome and India's precision airstrikes. Such systems are seen as low-risk acquisitions, reducing uncertainty in operational performance and political alignment. For example, after the April 2025 missile exchange between Israel and Iran, Germany and Finland began procurement talks for Israeli missile shields.

India's rapid retaliation during Operation Sindoor drew interest from Southeast Asian and African nations seeking

> Derivatives turn volatility into a known cost; when missiles fly, hedged treasuries keep projects funded and nerves steady—financing stays on course.

medium-range cruise missiles, UAVs, and electronic warfare systems. This represents a diversification from traditional suppliers, such as the US and Russia, toward other defence exporters with recent battlefield validation.

Exporting defence systems creates lock-in effects, where long-term contracts for maintenance and spare parts become vectors of dependency. Eventually, even a country with divergent ideologies may form a collaboration with the government that supplies defence systems, reducing the likelihood of diplomatic opposition and thereby reducing political risk between these two countries.

Defence sales are increasingly bundled with intelligence-sharing and surveillance technologies, which further embed exporters more deeply into the buyer's security. This shift is evident in India–Israel, Israel–Balkans, and Russia–India defence alignments, where defence deals have led to cooperative political stances that may result in reduced political risk in the region.

DERIVATIVES FOR POLITICAL RISK

In the current political climate, effective immunisation against political risk requires a cross-sectoral approach that brings together financial, defence, and aerospace capabilities. These domains are no longer isolated policy silos. Instead, they seem to form insurance mechanisms that collectively maintain political autonomy and resilience.

The increasing complexity of global threats, sanctions, commodity shocks, missile warfare, and trade disruptions requires strategies that work at both the political and business levels. Financial instruments, such as commodity futures, credit default swaps, and interest rate swaps, enable firms to hedge against political risk.

In the context of political risk, financial derivatives such as oil futures and options on metals serve as a hedging instrument. These instruments enable firms to factor in political risk before disruptions occur. They are speculative in nature but are supported by quantitative justification.

The pricing of these derivatives adjusts to perceived political risk. For example, during the Israel–Iran escalation and the Russia–Ukraine war, oil and gas futures markets had volatility spikes due to localised political risk. Recent studies have shown that political shocks create "jump risks" in commodity prices, making derivative contracts essential for hedging positions.

Hedging strategies range from natural hedging to financial instruments like futures, forwards, and options. Immunisation strategies, particularly in fixed-income portfolios, ensure that changes in interest rates caused by political risk do not affect the value of liabilities and assets. These instruments stabilise capital flows and protect balance sheets in times of uncertainty, as seen in studies that link derivatives markets to political risk.

Simultaneously, combat-proven defence systems, specifically those used in recent conflicts such as the Israel–Iran missile exchange and India's Operation Sindoor, serve a dual purpose: they deter hostile actors and create long-term export relationships that lock in diplomatic alignment. Aerospace capabilities complete the triad. Satellite surveillance, dual-use aircraft fleets, and maintenance ecosystems support national integration and crisis response.

Countries like India are developing indigenous aerospace ecosystems for passenger aviation and ISR, reducing reliance on foreign OEMs and safeguarding sovereignty over critical airspace infrastructure. Taken together, the approach has three layers: financial hedging, defence deterrence, and aerospace resilience.

Studies indicate that these three layers form the foundation of a political risk immunisation architecture. This perspective treats political risk not as an exogenous threat but as a manageable, forecastable, and even negotiable element of global strategy.

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

Transcending the noise with tech-powered interactions

Technology helps businesses cut through digital clutter, creating trusted, seamless interactions that build loyalty and lasting customer value.

BY SHARAT SINHA

In today's hyper-connected world, the digital revolution has transformed how businesses communicate with customers. With trust at a premium and attention spans at a minimum, strong customer engagement is now the backbone of loyalty, retention, and business growth.

Customers expect fast, efficient, and personalised support. Yet, the digital landscape is saturated with the battle for customer attention being fierce, making it imperative for businesses of today to reimagine how they interact with their customers.

The solution? Leveraging technology to deliver seamless, personalised experiences that not only cut through the clutter but also make every customer interaction count.

> Clear and trusted communication builds confidence from the first contact, helping brands stand apart in a crowded digital marketplace.

> Businesses that leverage caller ID, AI, and real-time insights transform ordinary interactions into memorable customer experiences.

IN BRIEF

- AI, data, and automation enable personalised offers and proactive solutions, turning every interaction into a loyalty opportunity.
- Advanced caller ID ensures customers see a trusted business name, boosting engagement and reducing the risk of calls being ignored.
- Omnichannel platforms unify voice, SMS, email, and chat, ensuring consistent brand messaging and seamless customer journeys.
- Unified platforms bring consistency across channels, aligning communication strategies and strengthening brand recognition.
- Emerging tech such as AI, ML, and real-time analytics will create context-aware, dynamic engagement for the next generation.

HARNESSING TECHNOLOGY FOR CUSTOMER ENGAGEMENT

Using new technology helps businesses connect with customers more smoothly and quickly. Tools like automation, personalised messages, and working across phone, email, and chat make customer service better and set new expectations. With data, AI, and cloud tools, companies can make sure every conversation fits what the customer needs and wants.

Businesses that prioritise engagement turn their customers into powerful brand advocates. However, the prevalence of spam calls and impersonal outreach has eroded trust in business communications. To cut through the noise, companies must leverage technology to deliver authentic, value-driven interactions at every touchpoint.

One such innovative approach is the use of advanced caller identification solutions. When customers see a trusted, clearly displayed business name on their incoming calls—rather than an unknown number or generic label—they are far more likely to answer and engage. This simple yet powerful feature not only boosts call answer rates but also reinforces brand credibility and trust.

BREAKING THROUGH THE CLUTTER TO SHINE

The digital space is crowded, even as calls by brands are rampant, making customers more cautious than ever. Many ignore legitimate calls from essential services simply because they cannot verify the caller's identity. This trend not only affects customer experience but also hampers business efficiency and growth.

One of the most effective innovations to solve this challenge is advanced caller identification. When customers see a trusted, clearly displayed business name on incoming calls—rather than an unknown number or generic label—they are far more likely to answer and engage. This simple feature boosts call answer rates and reinforces brand credibility and trust as customers are no longer left guessing about the legitimacy of incoming calls.

MAKING EVERY CUSTOMER INTERACTION COUNT

Every customer interaction offers a chance to build trust and create differentiation, and technology can help businesses maximise these opportunities. Advanced tools, such as AI-driven analytics and real-time data processing, enable organisations to personalise offers, anticipate customer needs, and proactively resolve concerns, thereby strengthening connections at every stage.

Displaying a recognisable business name on outgoing calls further enhances caller identity, reassuring

> The future of engagement lies in innovative communication tools that ensure companies rise above the noise and remain customers' first choice.

customers and reducing the risk of being mistaken for spam while creating a strong first impression.

Similarly, unified communication platforms also ensure omnichannel consistency across voice, SMS, email, and chat, delivering a seamless and reinforced brand experience. In addition, data-driven insights and real-time analytics empower businesses to refine engagement strategies, identify trends, and address emerging customer requirements proactively.

BUILDING A STRONGER BOND OF CUSTOMER TRUST

Trust is the foundation of every successful customer relationship. In today's digital landscape, establishing trust can be challenging—yet it is more important than ever. Customers seek out businesses that demonstrate transparency and authenticity, and technology offers powerful tools to reinforce these qualities throughout every interaction.

By utilising advanced caller identification and verification systems, companies can display a verified business name at the point of contact. This simple, technology-driven step reassures customers that they are engaging with a legitimate organisation, not a potential scammer. In a crowded marketplace, this clarity enables businesses to stand out and convey professionalism from the very first interaction.

A well-crafted brand name, enhanced by digital verification, becomes more than just a label—it transforms into a trust signal. When customers recognise a verified brand on their screens, it serves as a mental shortcut that reduces perceived risk and builds confidence. Technology not only safeguards the customer experience but also deepens trust, leading to more positive brand perceptions and stronger, lasting relationships.

TRANSFORMING ENGAGEMENT INTO BUSINESS VALUE

Customer engagement is no longer a luxury, but a strategic imperative that directly translates into tangible business value. By leveraging technology and data-driven insights, companies can transform every customer interaction into an opportunity to build lasting relationships, foster trust, and drive measurable results.

Robust engagement strategies ensure engaged customers who are more likely to remain loyal, spend more, and advocate for your brand, delivering a premium in share of wallet, profitability, and revenue compared to average customers. An omnichannel approach for seamless, personalised experiences ensures that customers feel recognised and valued at every touchpoint, reinforcing brand loyalty and encouraging repeat business.

Businesses that prioritise engagement see significant increases in cross-sell and upsell revenue, reduced churn, and lower acquisition costs, unlocking new levels of efficiency and profitability. Moreover, every positive interaction contributes to higher customer lifetime value and strengthens your competitive edge in crowded markets.

THE FUTURE OF CUSTOMER INTERACTION

As technology continues to evolve, the possibilities for enhancing customer interaction are virtually limitless. Technology needs to be at the heart of every business's customer engagement strategy. The integration of artificial intelligence, machine learning, and advanced analytics is enabling enterprises to deliver even more personalised, context-aware experiences. From predictive engagement to real-time issue resolution, these innovations are setting new benchmarks for customer experience excellence.

Digital name displays and caller identification technologies are just the beginning. In the future, we can expect to see even more dynamic and interactive solutions that further blur the lines between physical and digital communication.

As the digital landscape continues to evolve, the businesses that prioritise customer engagement and embrace innovative communication tools will be the ones that thrive. Transcending the noise is not just about being heard; it is about being remembered, trusted, and chosen—again and again.

The author is the Director and CEO of Airtel Business.

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.

Rising orbit: Startups power India's new space journey

India's space sector shifts from state-led missions to public–private partnerships, with startups driving agility, innovation, and global competitiveness.

BY PUNAM SINGH

For decades, the global space narrative was largely a duopoly, dominated first by the United States and then the Soviet Union, with Europe and a rising China slowly entering the arena. India, through its Indian Space Research Organisation (ISRO), carved a distinct niche—launching satellites and interplanetary probes with precision and frugality. But while ISRO led these missions with remarkable efficiency, the effort was almost entirely state-driven.

That is changing.

India's space sector is undergoing a fundamental transformation. What was once a public-led domain

"The PPP model allows both sectors to complement each other and create outcomes that neither could achieve alone."

AWAIS AHMED
Founder & CEO, Pixxel

"India's space startup ecosystem is thriving as policies and IN-SPACe reforms lower entry barriers, open satellite data, and spur collaboration."

KRISHANU ACHARYA
Co-Founder & CEO, Suhora Technologies

is now being restructured through a focused public–private partnership (PPP) model. The shift is strategic and deliberate, aimed not just at internal expansion but at repositioning India in the global space economy.

FROM MONOPOLY TO MULTI-STAKEHOLDER SPACE

ISRO has long been the singular force in Indian space—designing, building, launching, and operating missions. Its milestones, including the Chandrayaan series and the Mars Orbiter Mission (Mangalyaan), showcased Indian ingenuity. However, as the global space economy expands—driven by commercial innovation—India has recognised that a single government agency, however capable, cannot capture the full scope of emerging opportunities.

Reforms began taking shape after 2014, culminating in the Indian Space Policy 2023. This policy formally empowered the private sector, moving it from the role of contractor to that of co-creator and independent operator. The objective is to grow India's space economy to USD 44 billion by 2033 and capture an 8% share of the global market.

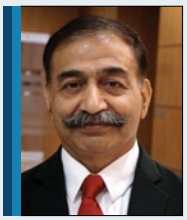
Enabling this is a model built on government facilitation, regulatory clarity, and trust in enterprise. Key institutions include the Indian National Space Promotion and Authorisation Centre (IN-SPACe), which streamlines regulations and grants private access to ISRO's infrastructure, and NewSpace India Limited (NSIL), ISRO's commercial arm that handles technology transfers and launch services. Together, they are converting decades of state-led knowledge into a platform for private innovation.

THE RS 1,200 CRORE PPP BREAKTHROUGH DEAL

If there is one story that encapsulates this seismic shift, it is the recent Rs 1,200 crore (approximately USD 137 million) Earth Observation (EO) satellite constellation project. Awarded by IN-SPACe to a consortium led by Bengaluru-based Pixxel.

IN BRIEF

- India's space sector is shifting from state-led to public–private partnerships for global competitiveness.
- The Rs 1,200 crore Pixxel-led Earth Observation satellite constellation project signals private confidence in space commerce.
- IN-SPACe and NSIL have helped ease regulations, enabling startups to access ISRO facilities and infrastructure.
- Private firms are bringing in agility, capital, and customer focus, complementing ISRO's technical expertise.
- Startups like Agnikul and Skyroot are expanding into indigenous launch capabilities under PPP models.
- With 300+ startups, India's ecosystem is emerging as a global space-tech innovation hub.



"Agility and ingenuity of startups fuel faster cycles and global competitiveness—something government R&D cannot fully replicate."

LT GEN AK BHATT (RETD)
Director General, Indian Space Association

What stood out was the 'zero-bid' proposal by the Pixxel-led consortium, which included PierSight Space, Satsure Analytics India, and Dhruva Space. Jointly, the companies proposed to fully fund the project without seeking government financing. This move reflects a strong belief in the long-term commercial viability of India's space sector.

Awais Ahmed, Founder and CEO of Pixxel, described it as a structural shift. "This PPP marks a fundamental change in India's space sector. It shows we are ready to compete globally in both technology and business models," he said.

The 12-satellite constellation is expected to include a mix of high-resolution, multispectral, hyperspectral, and Synthetic Aperture Radar (SAR) payloads. The aim is not only to capture high-quality data but also to strengthen data sovereignty—building indigenous capabilities in the growing global geospatial intelligence market.

WHAT PRIVATE PLAYERS BRING TO THE TABLE

The shift towards private participation is grounded in a clear recognition of what these players bring—agility, risk tolerance, and a sharp customer focus.

"Private industry brings speed, flexibility, and access to capital," said Ahmed. "ISRO remains the scientific and technical backbone, but startups can assume commercial risks, quickly iterate, and build customer-centric products. The PPP model allows both sectors to complement each other and create outcomes that neither could achieve alone."

Krishanu Acharya, CEO and Co-Founder of Suhora Technologies, agreed. "India's space startup ecosystem is thriving, thanks to enabling policies and regulatory support from IN-SPACe. Recent changes have lowered entry barriers, opened access to satellite data, and fostered collaboration."

Suhora is building advanced Earth observation solutions with global relevance. According to Acharya, the ease of doing business has improved, and India is becoming a hub for space-tech entrepreneurship. "Agile startups can now transform their vision into reality and contribute meaningfully to national space goals," he said.

EXPANDING REACH BEYOND SATELLITE VENTURES

This transformation is not limited to Earth observation. India's private sector is rapidly diversifying, pushing into areas once exclusively reserved for national agencies. We are seeing the emergence of indigenous launch capabilities.

Companies like Agnikul Cosmos and Skyroot Aerospace are not just dreaming of rockets; they have signed framework agreements with IN-SPACe, accessing ISRO facilities, and are developing their own launch vehicles. NSIL is even exploring the production of ISRO's heavy-lift launcher, the LVM3, under a PPP model.

Lt Gen AK Bhatt (retd), Director General of Indian Space Association (ISpA), believes this is crucial for India's global standing. "Their agility, customer-centric approach, and technological ingenuity accelerate development cycles and fuel competitiveness against international giants, something a government R&D organisation, by its very structure, cannot fully replicate," he said.

The future of India's space sector is no longer a solo journey. With over 300 space startups now active, a clear policy direction in place, and institutional frameworks enabling access, the ecosystem is becoming both vibrant and globally competitive.

ISRO's legacy laid the foundation, but it is the private sector—agile, innovative, and willing to take risks—that is now propelling India to new heights. Once viewed as supporting actors, private firms are increasingly taking centre stage.

punams@cybermedia.co.in

Rewiring AI infrastructure from core to edge

As GenAI shifts from pilots to production, enterprises must rethink infrastructure strategy to meet performance, cost, and compliance demands.

BY SHUBHENDU PARTH

Nearly 80% of Chief Information Officers (CIOs) in the Asia–Pacific region are expected to adopt edge services from cloud providers by 2027 to meet the performance and compliance needs of generative AI (GenAI) workloads, according to new IDC research commissioned by Akamai Technologies.

The research paper, "The Edge Evolution: Powering Success from Core to Edge," highlights how the rising adoption of AI is prompting APAC enterprises to reevaluate their digital infrastructure. It finds that centralised cloud models alone are no longer adequate to support the speed, scale, and regulatory requirements of AI inferencing.

According to the IDC Worldwide Edge Spending Guide, public-cloud services at the edge are forecast to grow at a compound annual growth rate of 17% through 2028, with spending expected to reach USD 29 billion.

EDGE SERVICES GAIN MOMENTUM ACROSS APAC

The report reveals that 31% of surveyed enterprises in APAC have already moved GenAI applications into production, while 64% are still in the testing phase. This growing momentum is putting strain on conventional cloud architectures and driving the shift to more distributed models.

Key infrastructure challenges include multi-cloud complexity (49%), changing compliance requirements, which are expected to impact 50% of the A1000 by 2025, unpredictable cloud costs (24%), and latency-related performance issues. These gaps are pushing organisations to integrate edge computing into their infrastructure plans.

> India's geographic spread and uneven network quality make edge infrastructure critical for lowering latency and managing costs.

Adoption rates vary across the region. In China, 37% of enterprises have GenAI in production, with another 61% in testing. Most of them—96%—rely on public-cloud infrastructure-as-a-service (IaaS). Japan is slower in deployment but is investing in AI, IoT, and disconnected environments. Meanwhile, countries in ASEAN are taking an edge-first approach to support decentralised operations.

INDIA BUILDS EDGE TO SUPPORT GENAI GROWTH

In India, the focus is on expanding edge infrastructure beyond metro cities to manage costs and improve performance. Around 92% of enterprises in the country believe GenAI has already disrupted or will disrupt their operations in the next 18 months. Over half (56%) identify AI workloads as the primary driver for changes to their infrastructure.

While 16% of Indian enterprises have GenAI in production, 82% are still in pilot stages. Among adopters, 91% plan to use public-cloud IaaS for AI training and inferencing. Cost concerns and a shortage of skilled professionals are driving the demand for affordable and AI-ready infrastructure.

Similarly, Edge IT spending is expected to rise among Indian enterprises in 2025. The need to deliver GenAI services closer to customers and remote sites is resulting in new edge data centres in tier-2 and tier-3 cities. These support use cases in IoT, surveillance, content delivery, and real-time insights across sectors such as financial services, healthcare, retail, telecom, and digital-native businesses.

India's geographic spread and uneven network quality, however, remain a concern. Locating compute closer to data sources is seen as a way to reduce connectivity costs and address performance issues caused by unreliable links.

"As GenAI transitions from experimentation to deployment, organisations must rethink where and how their infrastructure operates," said Daphne Chung, Research Director at IDC Asia–Pacific.

Parimal Pandya, Senior Vice-President and Managing Director, Asia–Pacific at Akamai Technologies, said the findings show that businesses are shifting to edge-first models to handle the demands of modern AI workloads.

INFRASTRUCTURE PRIORITIES FOR ENTERPRISES

The report recommends that enterprises align infrastructure plans with business goals. This includes assessing current estates, identifying workload needs, evaluating cloud providers, and updating plans as the business evolves. A centralised management experience across platforms is advised to improve governance, security, and compliance, while avoiding vendor lock-in.

IDC suggests that workload placement is a critical first step. Enterprises should keep training activities on centralised or dedicated infrastructure and shift latency-sensitive inferencing and data pre-processing to the edge to meet data sovereignty and performance needs.

The report advises enterprises to adopt edge orchestration and open standards to manage distributed compute environments. It also stresses the importance of integrating security and data governance into edge deployments.

Key security practices include zero-trust architecture, encryption, real-time monitoring, and a secure-by-design approach. Data-management strategies should cover data lifecycle, sovereignty, and governance, with AI and machine learning used to automate analytics and maintain integrity.

Automation is recommended to simplify deployment and manage hybrid and multi-cloud operations. Cost management should be treated as an ongoing process. IDC advocates for FinOps practices to track usage, uncover savings, and optimise resource allocation. This should be supported by analytics tools and GenAI-powered insights.

For India, IDC recommends partnerships that enable cost-effective compute and storage, alongside strategies to lower egress charges. Enterprises are urged to modernise infrastructure from core to edge with a focus on portability, operational simplicity, security, and latency.

shubhendup@cybermedia.co.in

Charting telecom's path to a trusted digital future

At COAI Dialogues 2025, trust, policy, and infrastructure converge to shape India's telecom roadmap for an inclusive, secure digital future.

BY PUNAM SINGH

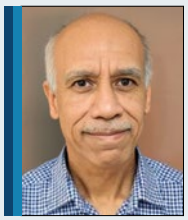
India's ambitious journey towards a fully digital economy took a decisive step forward at the COAI Dialogues 2025. The event, marked by strategic conversations among industry leaders, regulators, and technology experts, underlined a shared national vision: to realise Viksit Bharat 2047 through inclusive digital infrastructure, trusted connectivity, and forward-looking regulation.

Organised by the Cellular Operators Association of India (COAI), in collaboration with Voice&Data, the day-long conference went beyond ceremonial speeches. It created a forum for problem-solving, calling for robust cross-sector partnerships and citizen engagement. From spectrum challenges to AI risks, from rural broadband to the promise of 6G, the Dialogues reflected the depth of India's telecom transformation.

FROM DIALOGUE TO ACTION: A NEW MODEL OF ENGAGEMENT

The conference opened with a traditional lamp-lighting ceremony led by Lt Gen Dr SP Kochhar, Director General of COAI, setting the tone for a participative format focused on outcomes. Kochhar reiterated that the COAI Dialogues were structured not to end in platitudes but to generate actionable insights. The inaugural edition had earlier flagged grey areas requiring deeper exploration; the 2025 edition aimed to convert those into strategic blueprints.

Rahul Vatts, Vice Chairperson of COAI and Chief Regulatory Officer at Bharti Airtel, described telecom as the spine of India's digital story, enabling not just connectivity but national resilience. He flagged the need for trust-based digital ecosystems, pointing to rising



"Trust, safety, and inclusion must guide the telecom sector to build a resilient and equitable digital future that serves every Indian."

RITU RANJAN MITTAR
Member, Telecom Regulatory Authority of India

cyber threats and urging collective responsibility across sectors. His call underscored telecom's dual role as infrastructure and enabler.

GSMA's Asia Pacific Head, Julian Gorman, framed the larger global implications, highlighting how India's digital trust frameworks could guide emerging economies. He called for a "whole-of-government, whole-of-industry" approach, encouraging open standards and harmonised governance.

REGULATORY SIGNALS: TIME FOR AN INCLUSIVE FUTURE

Speaking at the forum, the chief guest and Member of TRAI, Ritu Ranjan Mittar, reflected on how recent policy and regulatory developments are reshaping the telecom landscape. He cited milestones such as the enactment of the new Telecommunication Act, the draft National Telecom Policy, and TRAI's initiatives to build trust through measures like SMS tagging and a trusted calling series for banks.

"While India has achieved remarkable progress, including the fastest 5G rollout globally and surpassing 1.2 billion mobile connections," Mittar reminded the audience that true digital inclusion goes beyond statistics. "The real measure of success," he said, "lies in reaching the last customer."

He even suggested exploring innovative schemes, such as making second-hand devices affordable, to ensure that no citizen is excluded from the digital revolution. Mittar also highlighted the new challenges emerging with AI-enabled devices, emphasising the need to anticipate risks and strengthen safeguards.

On the infrastructure side, he called for urgent focus on backhaul spectrum and interconnect regulations, essential for ensuring network resilience and service quality as traffic surges.

He concluded with a clear message: trust, safety, and inclusion must remain the guiding principles of India's telecom journey. Only by embedding these values into regulation, technology, and industry practices can the sector sustain its momentum and build a digital future that serves every Indian.

CHARTING THE ROAD TO DIGITAL INDIA 2030

Sandeep Saxena, Head of Technology and Solutions, Nokia India, laid out an ambitious roadmap for the next

"When the customer feels secure, it becomes a self-sustaining asset that generates long-term value across the entire digital ecosystem."

RAHUL VATTS

Vice Chairperson, COAI & Chief Regulatory Officer, Bharti Airtel

decade. He pointed to India's significant progress—with 99% district-level and 95% village-level broadband coverage and 640 million UPI transactions daily—as a base for future goals.

By 2030, India targets to achieve 80% broadband penetration across the country, expand the broadband user base to 100 million, and deploy 100 million public hotspots. Saxena explained that this vision would be driven by seamless connectivity across geographies and devices, AI-enabled networks capable of sensing and acting autonomously, the deep integration of telecom with public, private, and hybrid cloud systems, and the proliferation of smart, AI-powered devices, such as wearables and immersive computing tools.

He acknowledged that these goals face roadblocks such as affordability, terrain, and sustainability. However, he argued that only sustained collaboration between government, industry, and tech innovators could translate ambition into nationwide impact.

BALANCING INNOVATION AND SECURITY: A TELECOM TIGHTROPE

A key panel moderated by GSMA's Senior Director for Advocacy and Industry Engagement, Debashish Chakraborty, debated how to strike a balance between rapid digital innovation and citizen protection. Sanjeev K Sharma, DDG at the Department of Telecommunications (DoT), warned that without strict controls, scams could erode the foundation of the digital economy. He emphasised the need for skills development and local manufacturing.

Vatts shared how AI analytics were already flagging irregular behaviour across India's 14 billion daily calls with 99.9% accuracy. He highlighted the centrality of user trust: "If the customer feels secure, it becomes a self-sustaining asset," he said.

Ravi Gandhi, President and Chief Regulatory Officer, Reliance Retail and Reliance Jio proposed stricter platform governance and a national database of digital fraudsters. Nokia's VP for Government Relations (APAC), Vibha Mehra, praised India's citizen-led reporting model, noting that over 470,000 people had flagged suspicious calls, enabling action against 3.7 million numbers.

The panel, including Vodafone Idea Chief Regulatory and Corporate Affairs Officer Ambika Khurana, converged on one message: India's telecom sector cannot innovate

"Connectivity is no longer merely a concept; it forms the foundation of India's digital transformation and future economic resilience."

SANDEEP SAXENA
Head – Technology and Solutions, Nokia India

without embedding trust, and achieving Viksit Bharat 2047 would require joint stewardship of security, speed, and affordability.

6G, SATELLITES, AND PRIVATE NETWORKS

In another high-stakes panel moderated by journalist Rajiv Makhni, experts explored how India can prepare for future telecom frontiers.

Vodafone Idea's Chief Technology Officer Jagbir Singh, Bharti Airtel's Chief Technology Officer Randeep Sekhon, and Ciena Communications India's Senior Director of Sales Digvijay Sharma assessed the viability of 6G, satellite networks, and private 5G. The panellists were sceptical about the immediate value of 6G, citing unclear use cases and ecosystem immaturity.

However, satellite communications earned high marks for their ability to bridge India's digital divide. Projects by Starlink, OneWeb, and Amazon's Kuiper were seen as practical tools for education, healthcare, and rural enterprises. Meanwhile, private 5G networks emerged as a realistic opportunity for high-performance sectors such as manufacturing and logistics.

The key takeaway: India's telecom policy must not chase hype but focus on near-term, high-impact deployments.

THE SPECTRUM PUZZLE: A BARRIER TO DIGITAL GROWTH?

Jagbir Singh, in his keynote during the session, drew attention to spectrum management issues that could stall India's digital progress. He flagged fragmented governance, high pricing, and the absence of a unified national database.

Unlike previous transitions where spectrum refarming was possible, the shift to 5G was complicated by fresh allocations with no continuity. Singh urged coordinated spectrum management across ministries like DoT, ISRO, and Defence, and called for rational pricing.

He also emphasised that satellite and terrestrial networks must be developed in tandem to reach unserved areas and prepare for 6G. Singh identified three urgent priorities: the need for spectrum pricing to be rationalised and brought in line with global benchmarks, the creation of a unified and transparent national spectrum database, and the development of a coherent framework to integrate terrestrial and satellite networks in preparation for 6G.

Singh's remarks reinforced the urgent need for reform in resource governance if India hopes to lead in digital infrastructure.

BUILDING A RESILIENT NATIONAL DIGITAL BACKBONE

A panel comprising officials from TRAI, DoT, and telecom companies, such as Bharti Airtel and Vodafone, discussed the scale of investments fueling India's digital economy. With public funds via Digital Bharat Nidhi and private contributions from telecom giants, India is investing heavily in core infrastructure.

"The digital economy may falter if scams and fraud increase; securing the entire infrastructure is critical to ensure continued public trust."

SANJEEV K SHARMA
Deputy Director General (AI & DIU), DoT

"Spectrum is the lifeblood of telecom. Without rational pricing and unified governance, India may fall behind in the race for digital progress."

JAGBIR SINGH
Chief Technology Officer, Vodafone Idea

Speakers noted that financial investment alone won't suffice. The sector now requires rationalised policies, timely support, and sustainability-led technologies. Every investment must be assessed not just for its reach but also for its impact on inclusion, service quality, and long-term resilience.

Vodafone Idea Executive Vice President for Regulatory and Corporate Affairs Sanjeev Arora and TRAI Principal Advisor D Manoj agreed that timely regulatory clearances and inter-agency coordination are essential for maintaining rollout momentum.

THE BHARATIYA PROJECT: BRIDGING THE RURAL GAP

Niraj Verma, Secretary of the Department of Justice and former head of the Digital Bharat Nidhi, spotlighted the stark rural connectivity gaps: over 14,000 villages remain unconnected by 4G. While half are in progress, the rest require new initiatives, possibly involving satellite tech.

Verma described the Bharatiya Project—a shared digital infrastructure model involving multiple operators and performance-linked contracts. The focus is not merely on laying fibre, but also on ensuring it is utilised for governance, education, and economic activity. He emphasised that success would depend on how these networks are used—whether to deliver e-governance at the Gram Panchayat and block levels, expand access to citizen-centric platforms in healthcare, education and agriculture, or connect rural entrepreneurs, artisans and non-profits to national marketplaces like the ONDC.

Verma also shared that the government was in dialogue with ISPs to lease dark fibre on non-discriminatory terms, especially for industrial corridors. The approach, described as "book-building," involves advance engagement with stakeholders to align infrastructure rollout with anticipated demand.

He pointed out that the government's approach aims to move from output (infrastructure) to outcome (usage), creating a model that other developing nations could emulate.

INCLUSIVE BROADBAND: BEYOND URBAN METRICS

A closing session titled "The Future of Inclusive Broadband Connectivity" underscored that coverage alone is not enough. Panellists included Neeraj Kumar, DDG with National Broadband Mission; Dharmendra Khajuria, Head Network Partner, Bharti Airtel; Akshat Mohindra, Account Leader – Government and PSU Business, Ciena India; and Dinesh Shiv, Head – India Telecom Compliance and Regulatory, Zoom Communication.

Moderated by Prof Brejesh Lall of IIT Delhi, the speakers argued that the new benchmark must be meaningful connectivity. They highlighted the importance of expanding fibre-to-the-home, ensuring connectivity for schools, health centres and panchayats, and increasing infrastructure sharing—especially ducts and fibre routes—to build a cost-efficient, sustainable model for broadband expansion.

The panellists warned against relying solely on urban metrics for success, emphasising that the sector's true test lies in delivering similar service quality in rural India, enabling equitable access to public services and economic opportunity.

Vikram Tiwathia, Deputy Director General, COAI, wrapped up by reiterating the need for collective action. He thanked participants, partners, and policy-makers for transforming the platform into a forum for forward-thinking collaboration.

The event's consistent message was clear: Viksit Bharat 2047 is not just about technological leadership. It is about embedding trust, fostering inclusion, and creating partnerships that put citizens at the centre of India's digital revolution.

punams@cybermedia.co.in

EOS unveils high-energy laser to counter drone attack

Apollo, scalable up to 150 kW, combines precision targeting and cost-efficient firepower to defeat drones and disrupt coordinated attacks.

Australian defence technology firm Electro Optic Systems (EOS) has unveiled its high-energy laser weapon, Apollo, a system scalable up to 150 kW and built to defeat small to medium-sized drones while disrupting their sensors to counter coordinated swarm attacks.

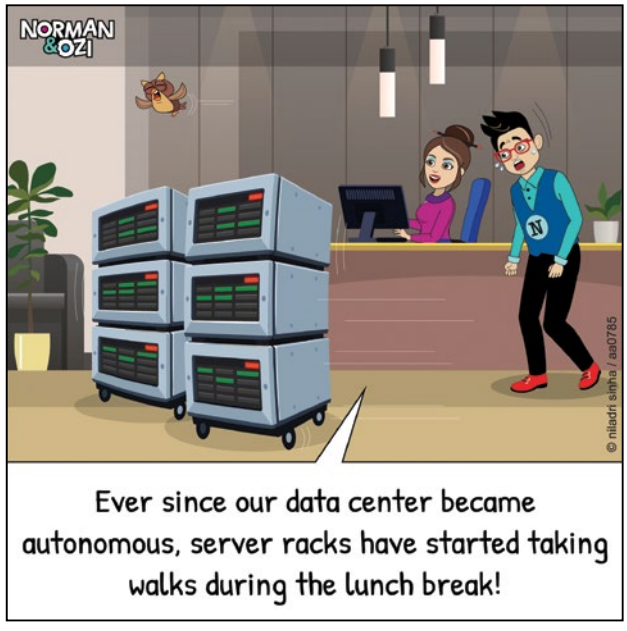
At 100 kW, Apollo can disable more than 20 drones per minute at typical swarm engagement distances. EOS said the system counters UAS manoeuvres such as rapid rotation, thermal isolation, and reflective coatings, which are increasingly used to evade defences. Its high slew rate and reduced dwell time between targets allow rapid retargeting, giving it the ability to track and neutralise multiple fast-moving threats.

The system also targets loitering drones beyond 10 km, which are often used to coordinate swarm attacks. By disabling their sensors, Apollo disrupts the flow of targeting data to strike platforms.

With external electrical supply and cooling, Apollo provides unlimited shots. When operating independently, its internal magazine supports more than 200 kills. EOS emphasised that while missile-based defences cost hundreds of thousands of dollars per shot, the cost of a laser engagement is limited to electricity, making sustained defence against swarms economically viable.

Packaged in a 20-foot ISO container, Apollo is designed for mobility, camouflage, and rapid deployment. Crews can set it up in under two hours, enabling both fixed-site protection and expeditionary use. The system delivers 360-degree coverage, with hard kills at up to 1.86 miles (3 km) and optical sensor denial at up to 9.32 miles (15 km).

Apollo integrates with NATO-standard command-and-control and air defence networks, enabling adoption in existing layered systems. EOS Group Chief Executive Dr Andreas Schwer said high-energy laser weapons were becoming essential to address the rapid growth of drone warfare.



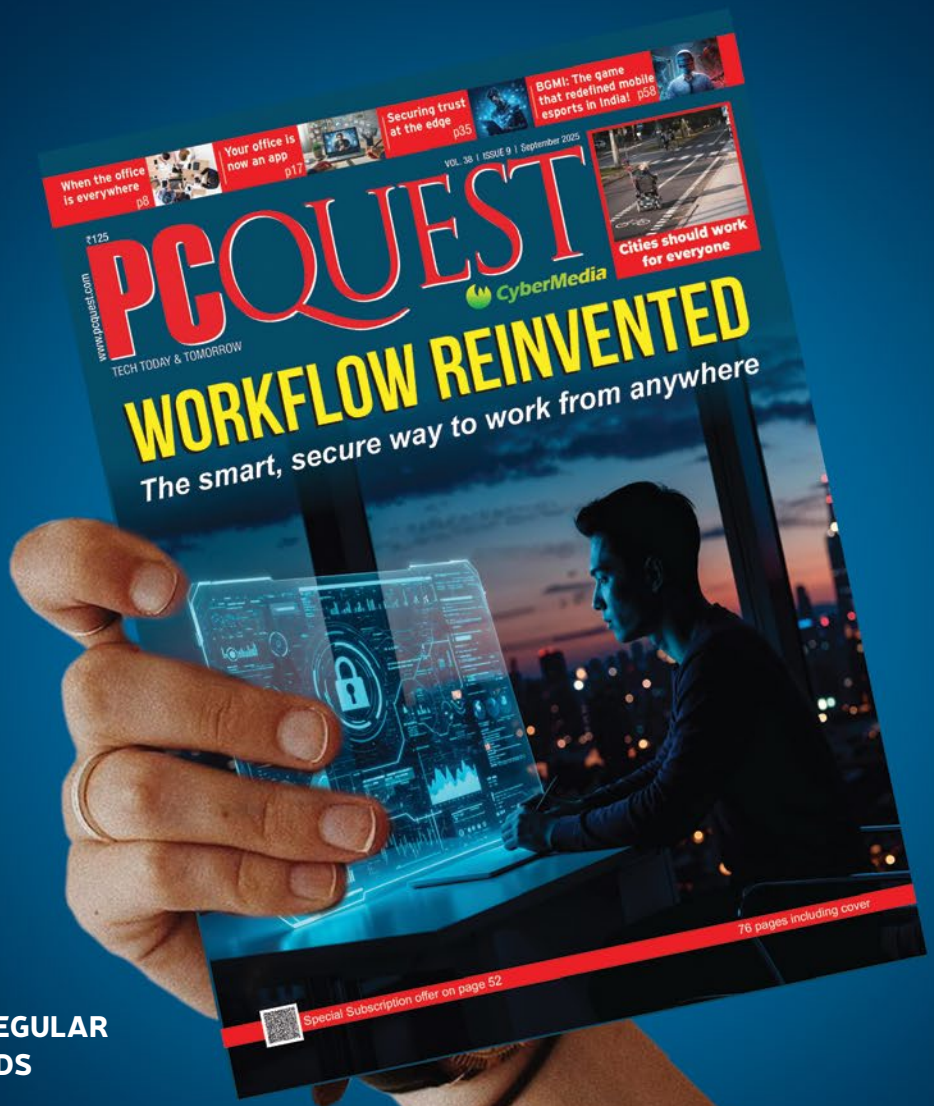
PCQUEST
TECH TODAY & TOMORROW

CyberMedia

PCQUEST SEPTEMEBR '25 EDITION - WORKFLOW REINVENTED: THE SMART, SECURE WAY TO WORK FROM ANYWHERE

ALSO READ MORE ON

- Your office is now an app
- When data flows, defense scales
- AI in security Oversight or overdependence?
- Smart warehouses, smarter deliveries: The rise of AI-driven logistics
- Rewiring the future How Oben Electric is reshaping India's EV motorcycle?
- REVIEWS: OnePlus Nord 5 | Tata Tiago.EV | Jitendra EV Yunik



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

Rama Mandi, Jalandhar - Estd. 2001

50+ Years of EXCELLENCE Since 1967 APEEJAY EDUCATION

Your Child's Journey to a Promising Future Starts Here

ADMISSIONS OPEN FOR SESSION 2026-27

NURSERY to IX

KEY HIGHLIGHTS

- State-of-the-art Infrastructure with tech-enabled classrooms
- Value-based holistic development
- Thematic curriculum aligned with NEP 2020
- Art Integration and honing of artistic skills
- Focus on play-based, activity-based and enquiry-based learning
- Outstanding CBSE results and selection in leading competitive exams

For admission related queries, please contact us:

Apeejay School, Hoshiarpur Road, Rama Mandi Jalandhar, Punjab – 144007

91-8872020402 **https://www.apeejay.edu/hoshiarpur/**

skool.rmd.jln@apeejay.edu

Follow Us On:

Scan To Apply