5G'S NEXT TEST: TURNING INFRASTRUCTURE INTO REAL RETURNS | 16

₹100

www.voicendata.com

VOL 33 ISSUE 03 MARCH 2026

VOICE & DATA

Connecting the Digital World

CyberMedia

FROM PILOTS TO PLATFORMS: IIoT GROWS UP

Factory systems are evolving into a layered digital infrastructure where sensors, connectivity, edge computing and AI are driving real-time operational decisions.

"CUSTOMERS TODAY ARE BUYING OUTCOMES, NOT PRODUCTS"

ASHOK SHIVASHANKAR, Cisco India & South Asia

46

76 pages including cover

Special subscription offer on Page 56

Apeejay School

NOIDA (Established in 1981)

50+ Years of EXCELLENCE Since 1967 — APEEJAY EDUCATION

THE LEGACY OF 50+ YEARS OF EXCELLENCE CONTINUES

ADMISSIONS OPEN

Session 2026-27

Bal Vatika 1 to Class IX and XI

Age Criteria for Bal Vatika 1:
3+ years as on 31st March 2026

Attractive Scholarships Available

KEY HIGHLIGHTS

- One of the largest eco-friendly campus in Noida
- Fully air-conditioned classrooms
- Safe and secure environment with 24/7 CCTV surveillance
- Strong teacher-student connect and a caring school culture
- High parent engagement, fostering a supportive community
- Strong global outlook with a focus on international exposure

AWARDS & RECOGNITIONS

Ranked No. 1
in Noida **(Leaders Category)**
by the **Times School Survey 2025**
Bestowed with the esteemed
Dainik Jagran School Excellence Awards 2024-25

Outstanding Academic Achievements:

- Consistently brilliant results in CBSE
- Excellent performance in professional entrance exams
- Alumni excelling in prominent positions across diverse industries

For admission enquiry, please contact:

APEEJAY SCHOOL SECTOR -16A, FILM CITY, NOIDA - 201301

Contact Number: **+91-8527-570-570** | Website: **www.apeejay.edu/noida/** | Email: **skool.ms.nvd@apj.edu**

VOICE & DATA
CONNECTING THE DIGITAL WORLD

Website: www.voicendata.com

OUR OFFICES

GURGAON (CORPORATE OFFICE)
Cyber House
B-35 Sector-32, Gurgaon, Haryana – 122 003
Tel: 0124 - 4237517, Fax: 0124 - 2380694

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

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

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

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

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

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

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

March 2026

[CONTENTS]

COVER STORY 28

FROM PILOTS TO PLATFORMS: IIoT GROWS UP

Factory systems are evolving into a layered digital infrastructure where sensors, connectivity, edge computing and AI are driving real-time operational decisions.

[CONTENTS]

INDUSTRY SPEAK

08 Satellite IoT: Extending digital reach beyond fibre

10 Telecom platforms evolve from connectivity to engagement

13 AI's 2050 question: Who governs the algorithmic age

REPORT

20 Enterprise AI moves from pilots to infrastructure built for scale

23 Telecom becomes responsible AI's toughest governance test

26 Is 5G paving the road or blockingthe path to 6G

TECHNOLOGY

36 The invisible security moat in a connected world

40 Free-space optics open a new path for networks

42 India's data centres face the AI infrastructure shift

BROADBAND BYTES

16 5G's next test: Turning infrastructure into real returns

TV RAMACHANDRAN

INTERVIEW

46 "Customers today are buying outcomes, not products"

ASHOK SHIVASHANKAR

54 "Geopolitics may encourage domestic technology development"

ANDREW KITSON

FOCUS

50 Networks find their next foothold at the edge

USE CASE

58 BFSI security moves to AI-driven video infrastructure

COMMENTARY

62 MeitY's deepfake clampdown: short, sharp and suddenly real

66 Cyber insurance: The new backbone of India's digital resilience

STRATEGY

70 Telco capex walks a tightrope of returns

REGULARS

06 Voicemail 07 Opening Note 74 Postscript

[NEXT ISSUE]

FEBRUARY 2026

Scan QR Code & Subscribe now...

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

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

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

mail twitter Linkedin RSS Facebook

FEEDBACK
From Online Readers

Share your views at vndedit@cybermedia.co.in

For any query: ajaydh@cybermedia.co.in

FORM IV (See Rule)

Statement of ownership and other particulars about the newspaper VOICE&DATA to be published in the first issue every year after the last day of February.

1.	Place of Publication	:	New Delhi
2.	Periodicity of Publication	:	Monthly
3.	Printer's Name	:	Pradeep Gupta
	Whether Citizen of India	:	Yes
	Address	:	D-74, Panchsheel Enclave, New Delhi – 110 017
4.	Publisher's Name	:	Pradeep Gupta
	Whether Citizen of India	:	Yes
	Address	:	D-74, Panchsheel Enclave, New Delhi – 110 017
5.	Editor's Name	:	Shubhendu Parth
	Whether Citizen of India	:	Yes
	Address	:	203, Ashirwad Apartments, 74, I P Extension, Narwana Road, Delhi 110092
6.	Names & addresses of individuals who own the newspaper, and partners or shareholders holding more than one percent of the total paid-up capital	:	Cyber Media (India) Limited D-74, Panchsheel Enclave, New Delhi – 110 017

List of shareholders holding more than 1% of the paid up capital of the company as on 15th February 2026: Pradeep Gupta, Dhaval Gupta, Kriti Gupta, Mahendra Girdharilal.

I, Pradeep Gupta, hereby declare that the particulars given above are true to the best of my knowledge and belief.

Sd/-
Publisher

SHUBHENDU
PARTH

[OPENING NOTE]

When networks become the real defence shield

The first sign of an incoming missile is not an explosion. It is a signal.

A radar somewhere detects a faint track. Another sensor confirms it. A satellite observes the launch plume. Within milliseconds, encrypted packets travel through defence networks to command systems that calculate trajectory, speed and probable impact points. Before a human operator fully understands the threat, the network has already begun to respond.

In modern warfare, the defence shield does not begin with the interceptor missile. It begins with the network.

The ongoing US and Israeli vs. Iran conflict illustrates this shift clearly. Iranian missile and drone strikes across West Asia have targeted radar installations, early-warning sensors and communication infrastructure supporting adversary air-defence systems. Several high-value radar systems—the "eyes" of missile defence—have reportedly been damaged or degraded, while salvos combining drones and missiles have attempted to saturate interception systems.

These attacks were not random. They were aimed at the digital architecture that allows missile defence systems to function.

What Iran's strategy underscores is the distinction between kinetic defence and digital defence. The kinetic layer consists of interceptors such as Israel's Iron Dome, the US Patriot PAC-3 and the THAAD system, each designed to destroy incoming rockets, drones or ballistic missiles through high-speed interception. Yet these weapons are merely the visible edge of a deeper system.

Behind them lies the invisible architecture of integrated air and missile defence, the digital fulcrum of the modern defence shield. Long-range radars such as the AN/TPY-2 X-band system, airborne early-warning platforms and satellite sensors generate streams of tracking data. Through encrypted tactical data links, fibre backbones and satellite communications, these inputs are fused into a Single Integrated Air Picture—a constantly evolving map of the battlespace.

This fusion compresses what defence planners call the "sensor-to-shooter kill chain". Once a launch is detected, command systems calculate trajectory, assess intent and assign the most suitable interceptor battery. Even after launch, communication links remain active, transmitting mid-course guidance updates that enable interceptors to adjust their paths against manoeuvring targets.

Artificial intelligence (AI) increasingly provides the cognitive edge within this architecture. Modern attacks rely on saturation—swarms of drones and missiles launched together to overwhelm human decision cycles. AI-driven battle management systems orchestrate sensor fusion, filter false signals and prioritise threats within seconds. In such engagements, victory often hinges on latency measured in milliseconds.

Equally vital is resilience. Electronic warfare and cyber operations aim to jam radars, corrupt data streams or sever communication nodes. Break that digital spine, and the most sophisticated interceptor becomes little more than an expensive projectile waiting for instructions.

India witnessed the growing importance of such integration during Operation Sindoor in May 2025, when systems such as Akash, S-400 and the Akashteer command network formed a layered defensive grid capable of neutralising drone and missile threats with efficiency.

The lesson from today's *jang-e-asr,* the war of the present age, is unmistakable. Interceptors may deliver the final blow—the *zarb-e-akhir*—but networks, sensors and AI decide whether the *magen,* the shield, holds.

shubhendup@cybermedia.co.in

Satellite IoT: Extending digital reach beyond fibre

Satellite IoT is extending connectivity where terrestrial networks fall short, supporting urban infrastructure, aviation safety, and remote healthcare services.

BY SIDDHARTHA ABBURI

More than 1,002 million internet subscribers were reported in India by mid-2025, according to the most recent official data available. Yet significant gaps remain in consistent and reliable connectivity, especially in rural and remote regions where network infrastructure is weak or absent.

These connectivity gaps are not merely statistical figures; they encompass towns, transport corridors, coastlines, and disaster-prone areas that keep economies moving and communities safe, yet often fall outside the reach of dependable terrestrial networks.

As cities modernise and public services move deeper into digital platforms, the challenge is not only to build smarter technology but also to ensure it reaches everyone who needs it. This is where Satellite-enabled Internet of Things (Satellite-IoT) is beginning to make a tangible difference.

SMARTER CITIES BEYOND TERRESTRIAL NETWORKS

Urban intelligence runs on a constant flow of data. From managing traffic and water supply to balancing energy grids, waste collection, and environmental monitoring, thousands of sensors must work together in real time. Yet cities do not stop where fibre lines end. Industrial edges, transport routes, coastal stretches, and expanding peri-urban areas often lie outside reliable cellular coverage.

This is where Satellite-IoT quietly fills the gap. By allowing devices to connect directly via satellite, city teams gain visibility across their entire footprint. Water leaks can be flagged early, while air-quality and flood sensors continue reporting during extreme weather conditions. Remote substations or solar installations also remain monitored without costly network build-outs.

When disasters strike and ground networks fail, satellite-connected systems remain operational,

supporting faster response and recovery. Satellite-IoT, therefore, helps cities remain both smarter and more dependable when it matters most.

CONTINUOUS CONNECTIVITY FOR AVIATION SAFETY

Few environments demand reliability like aviation. Aircraft travel across oceans, deserts, and polar routes where traditional communication networks do not exist. Yet modern aviation depends on constant communication for navigation, surveillance, weather updates, and safety coordination. Satellite-IoT is increasingly becoming an important layer supporting aviation safety and efficiency.

Continuous aircraft tracking ensures that every flight remains visible, even across remote airspace. Satellite-enabled sensors monitor engine health, cabin conditions, and structural performance in real time. These capabilities support predictive maintenance and reduce the risk of in-flight failures. In air traffic management, such connectivity improves routing efficiency, reduces congestion, and enhances fuel utilisation.

Redundancy is another important advantage. Satellite links provide a dependable fallback when ground-based systems become unavailable, ensuring that communication does not become a single point of failure. As airspace grows busier and drones become more common, Satellite-IoT will play a key role in keeping skies safe and well managed.

CONNECTING HEALTHCARE BEYOND URBAN CENTRES

Perhaps the most transformative impact lies far from city centres and airports, in homes and communities that have historically lacked reliable access to healthcare. Remote diagnostics, connected medical devices, and telemedicine platforms all depend on stable connectivity. In many rural and underserved regions, that connectivity is often absent. Satellite-IoT changes this equation.

Health sensors can transmit patient data from villages, islands, and hilly terrain directly to doctors and diagnostic centres. Emergency response systems remain operational even when terrestrial networks are disrupted. Mobile health units, ambulances, and disaster-relief teams stay connected wherever they operate.

The result is not just improved access but also continuity of care. Early diagnosis, real-time monitoring of chronic conditions, and faster emergency intervention become possible regardless of geography. For communities that have long lived at the edge of healthcare systems, Satellite-IoT helps bring them into the broader digital health ecosystem.

TECHNOLOGY ADVANCES ENABLING SATELLITE IOT

Several technological developments are driving this shift. Low Earth Orbit (LEO) satellites offer lower latency and higher data speeds, making satellite connectivity more suitable for real-time IoT applications. Devices are also becoming smaller, more energy-efficient, and more affordable, allowing sensors to operate for years with minimal maintenance.

At the same time, hybrid networks that combine satellite, cellular, and Low-Power Wide-Area Network (LPWAN) connectivity can automatically select the most reliable available connection, helping ensure consistent coverage.

Governments are also recognising the strategic importance of resilient digital infrastructure. From smart city missions and aviation safety mandates to national digital health initiatives, policy frameworks are increasingly aligned with technologies that prioritise coverage, redundancy, and security.

BUILDING RESILIENT CONNECTIVITY INFRASTRUCTURE

At its core, Satellite-IoT is about trust. Trust that systems will function when they are needed most, that data will continue to flow even in challenging conditions, and that digital progress will not exclude those beyond traditional networks.

As cities expand, airspace becomes more congested, and healthcare becomes more decentralised, the need for reliable connectivity will continue to grow. Satellite-IoT does not replace terrestrial networks but strengthens them, extending intelligence to the edges and resilience to the core.

The next phase of digital growth will be defined not only by how quickly systems operate in ideal conditions but also by how reliably they perform in real-world environments. For a nation moving toward the vision of Viksit Bharat, such reliability forms an essential foundation.

The author is a Director of Avantel.
feedbackvnd@cybermedia.co.in

Telecom platforms evolve from connectivity to engagement

As enterprises seek deeper digital engagement, telecom networks and messaging platforms are evolving into intelligent layers enabling contextual interaction.

BY ASHUTOSH AGRAWAL

The telecom industry is undergoing a profound transformation. What once revolved around coverage and tariffs is now increasingly driven by experiences—how seamless, relevant, and intuitive every interaction feels. Customers expect conversations, not just connectivity. As a result, telecom operators and enterprises are shifting from infrastructure-led models to experience-led communication frameworks designed for a digital-first world.

Modern communication journeys are evolving rapidly as enterprises seek to move beyond transactional messaging towards contextual and conversational engagement. This shift reflects a broader change in how organisations view communication infrastructure: not merely as a delivery mechanism for messages, but as an intelligent layer that enables meaningful interaction between businesses and their customers.

CUSTOMERS RESHAPE THE COMMUNICATION PLAYBOOK

Customer expectations have accelerated far beyond what traditional messaging systems were designed to support. A payment reminder or delivery update is no

> Enterprises are rethinking telecom infrastructure as a platform for interactive customer journeys rather than a simple channel for alerts and updates.

RCS messaging is transforming the mobile inbox into an interactive interface where customers can explore services, respond instantly and complete actions.

IN BRIEF

- Telecom is shifting from connectivity and tariffs toward experience-led communication models that prioritise seamless customer interaction.
- Enterprises are replacing fragmented messaging tools with integrated platforms that enable contextual and personalised communication journeys.
- Technologies such as RCS enable app-like experiences in messaging inboxes with interactive media, suggested replies and guided workflows.
- Messaging channels such as WhatsApp Business allow enterprises to provide conversational service, alerts and support within familiar apps.
- CPaaS platforms integrate voice, SMS, messaging apps and email into programmable workflows that orchestrate multichannel journeys.
- Cloud numbering services enable global enterprises to maintain local identities across markets while managing communication centrally.

longer an isolated message; it forms part of a broader interaction that may span several channels and touchpoints. Customers expect these interactions to be personalised, contextual, and effortless.

To respond to these expectations, enterprises are increasingly moving away from fragmented messaging tools toward integrated communication platforms. Such platforms enable organisations to orchestrate interactions across channels while maintaining consistency and relevance. The objective is to deliver communication experiences that match the pace and style customers prefer for engaging.

RCS BRINGS INTERACTIVITY TO MESSAGING INBOXES

Rich Communication Services (RCS) is emerging as a significant evolution of traditional SMS. By transforming the standard messaging inbox into a more interactive environment, RCS enables enterprises to deliver app-like experiences directly within a messaging interface.

Instead of simple text alerts, organisations can deliver high-resolution media, interactive buttons, suggested replies, and guided transactional journeys within a single conversation thread. On compatible Android devices, RCS is integrated directly into native messaging clients, allowing users to interact with businesses without installing additional applications.

Another key feature of RCS is its support for persistent conversational journeys, enabling ongoing interactions that can extend beyond a single notification. Enterprises can embed catalogues, service flows, and other interactive elements within these conversations, creating richer engagement experiences that resemble in-app interactions.

MESSAGING PLATFORMS EXPAND ENGAGEMENT OPTIONS

Messaging platforms such as WhatsApp Business have also become central to enterprise communication strategies. With billions of users already familiar

> Cloud numbering services help enterprises establish local identities across countries while managing global communication centrally without physical infrastructure.

with these platforms, they offer a convenient and conversational environment for customer engagement.

Enterprises increasingly use such channels to provide customer support, deliver updates and alerts, and manage service interactions. Automated conversational flows, often supported by chatbots, allow organisations to respond quickly while also escalating complex issues to live agents when required. Personalised alerts and reminders can be delivered within the same conversational thread, creating a unified communication experience.

Because customers already use these platforms in their everyday lives, enterprises can interact with them in a familiar environment without requiring them to download additional applications or learn new interfaces.

CPAAS PLATFORMS UNIFY MULTICHANNEL JOURNEYS

As communication channels continue to multiply, enterprises require an orchestration layer that connects them into coherent customer journeys. Communications Platform as a Service (CPaaS) solutions address this need by integrating multiple communication channels—such as voice, SMS, messaging applications, and email—within a single programmable platform.

Through developer interfaces, application programming interfaces (APIs), and low-code or no-code orchestration tools, enterprises can design communication workflows that combine authentication, alerts, notifications, and conversational interactions. These platforms also incorporate analytics capabilities that provide insights into customer behaviour and engagement patterns.

Such orchestration allows organisations to build multichannel communication journeys while maintaining telecom-grade reliability and security.

CLOUD NUMBERS ENABLE GLOBAL IDENTITY

For organisations operating across multiple markets, maintaining a local presence while managing communication centrally can be challenging. Cloud-based numbering services are helping address this issue by enabling enterprises to establish local identities in different countries without the need for physical infrastructure.

These services typically provide a range of numbering options, including fixed, mobile, and toll-free numbers. Through technologies such as SIP trunking and programmable messaging interfaces, enterprises can integrate voice and messaging capabilities into their applications and customer service platforms.

By appearing local in different markets, organisations can build trust and familiarity with customers while maintaining operational efficiency through centralised systems.

EXPERIENCE BECOMES TELECOM'S DEFINING LAYER

The evolution from transactional messaging to conversational engagement reflects a broader transformation in telecom and digital communication ecosystems. As enterprises adopt richer messaging technologies, omnichannel orchestration platforms, and cloud-based communication services, the role of telecom infrastructure is expanding.

Connectivity is no longer viewed solely as a transport layer for information. Instead, it is becoming an intelligent engagement layer that supports secure, contextual, and responsive interactions between organisations and their customers.

In an economy where digital services increasingly define customer relationships, the ability to deliver seamless communication experiences is becoming a key differentiator. Telecom networks and communication platforms are therefore evolving to support not only connectivity but also the quality, relevance, and intelligence of every interaction.

The author is the Group CEO of Globe Teleservices.
feedbackvnd@cybermedia.co.in

AI's 2050 question: Who governs the algorithmic age

As AI reshapes economies and institutions, societies must confront questions of governance, accountability, data ownership, and human relevance.

BY JAIDEEP GHOSH

The trajectory of artificial intelligence (AI) is no longer a matter of technological speculation limited to economic impact or job losses. It has become the defining economic and social vector of this century. AI is emerging as the structural force that will shape governance, markets, and social cohesion through mid-century. Projecting forward to 2050, therefore, demands a deeper inquiry. AI will fundamentally alter how society functions and how decisions affecting citizens are executed.

Past industrial revolutions substituted human muscle with machinery. AI represents the first technological leap capable of replicating aspects of human cognition and judgment. The twentieth century was defined by the pursuit of technology for maximum productivity. The defining challenge of the twenty-first century is to ensure that technology preserves human dignity. The central question for 2050 is not whether machines will achieve advanced intelligence, but whether humanity will maintain control. This reality elevates AI from a technological evolution to a critical shift in global governance.

LIVING WITHIN PERVASIVE AI ECOSYSTEMS

By mid-century, the idea of consciously "using" AI in the way people interact with digital tools today may become obsolete. Citizens will instead live within pervasive AI ecosystems embedded in everyday systems and institutions.

Yet this hyper-efficiency introduces serious risks. AI is transforming the twenty-first century from an industrial capitalist order into what may be described as an algorithmic civilisation. If algorithms increasingly influence decisions affecting citizens, including loan approvals, hiring outcomes, insurance eligibility, and tax scrutiny, the risk extends beyond the science-fiction trope of hostile machines. The real threat lies in invisible decision-making structures shaping outcomes without transparency.

Future governance will therefore require strict algorithmic accountability alongside traditional administrative law.

> Invisible algorithms will increasingly influence decisions affecting citizens, forcing governments to treat AI oversight as a core pillar of public governance.

Technology must function as an augmentative instrument for human judgment rather than a silent replacement.

AI'S ECONOMIC ENGINE AND GLOBAL STAKES

The economic momentum behind AI is immense. PwC research estimates that AI could contribute as much as USD 15.7 trillion to the global economy by 2030. By 2050, AI could form the foundational layer of global economic activity.

For India, projected to reach a USD 30 trillion economy by mid-century, advanced, context-aware artificial general intelligence (AGI) may become a critical lever for overcoming structural bottlenecks in healthcare, education, and public service delivery.

Yet this growth is accompanied by cautionary forecasts. Analyses such as Citrini Research's report on a potential Global Intelligence Crisis outline scenarios in which AI could accelerate layoffs across sectors that currently appear resilient. Industries ranging from payment processing to food delivery could face disruption as intelligent automation expands its reach.

PROFESSIONAL RELEVANCE IN THE AI WORKPLACE

The global population is expected to reach approximately 9.7 billion by 2050, with demographic momentum shifting toward the Global South. The workplace of the future will not exclude humans entirely, but it will significantly reduce the role of routine labour. This includes both blue-collar tasks and cognitive white-collar roles. AI's disruption of middle-class professions such as analysis, diagnostics, documentation, and middle management suggests that the coming challenge may not simply be unemployment, but widespread erosion of professional relevance.

Early signals of this transformation are already visible. Agentic AI systems are beginning to reshape traditional IT services and software-as-a-service (SaaS) industries, generating terms such as "Saaspocalypse" and "AI scare trade". As this transition unfolds, human capital in 2050 will increasingly be valued for complex problem-solving, ethical judgment, and empathy rather than computational efficiency.

Educational qualifications may depreciate faster than practical capabilities. The long-standing model of stable careers is gradually giving way to continuous reskilling. Adaptability is therefore emerging as a core requirement for both corporate institutions and national economies.

TELECOMMUNICATIONS: THE CENTRAL NERVOUS SYSTEM

None of these futuristic systems can operate without telecommunications infrastructure. If AI represents the brain of the 2050 economy, telecom networks will function as its central nervous system.

Smart megacities, precision agriculture, autonomous transport, and industrial automation will generate extraordinary volumes of data. Supporting such systems will require unprecedented bandwidth and near-zero-latency connectivity.

Future communications networks may operate on 7G or 8G wireless technologies integrated with low-earth-orbit (LEO) satellite constellations. In this environment, telecom operators will evolve beyond their traditional role as bandwidth suppliers. They will increasingly function as orchestrators of digital ecosystems, reflecting the broader industry transition from Telcos to TechCos.

Their long-term valuations will depend on their ability to provide secure, AI-native infrastructure that prioritises data sovereignty, cybersecurity, and privacy.

DATA POWER AND THE RISK OF INEQUALITY

In the industrial age, economic expansion was driven by capital, labour, and machinery. In the AI era, data becomes the central economic resource. Every digital interaction generates predictive value that can be analysed, modelled, and monetised.

This shift raises a fundamental policy question. Should data ownership reside with corporations, with the state, or with citizens themselves? Countries that design credible and trusted frameworks for data governance will be better positioned to preserve economic sovereignty.

> As AI ecosystems expand, the real risk may not be hostile machines but opaque decision systems shaping credit, employment, insurance, and taxation.

At the same time, AI systems are increasingly being optimised for engagement. This creates a structural social challenge. Societies depend on shared trust and social cohesion. Hyper-personalised information streams risk fracturing this shared reality and creating a future in which the primary societal divide is information inequality. Digital ethics, therefore, becomes a central pillar of national governance.

POLICY ARCHITECTURE FOR RESPONSIBLE AI

These structural realities call for a practical policy framework that strengthens accountability while encouraging innovation. Governments will need to mandate independent algorithmic impact assessments for high-stakes decision systems used by both public institutions and commercial organisations. These assessments would function in a manner comparable to environmental impact studies.

Decision systems that affect citizen rights or entitlements must generate auditable decision logs. These logs should produce explainable traces that allow human reviewers to understand, question, and challenge automated outcomes when necessary.

Governments must also move beyond symbolic data consent toward a rights-based framework that enables portability, revocation, and clearly defined limits on the use of behavioural data. Digital Public Infrastructure should be strengthened as a public good, enabling interoperable services and reducing dependence on a small number of dominant global platforms.

Regulatory incentives should encourage the convergence of telecom infrastructure and AI systems. Telecom operators must be supported in investing in AI-native networks and edge computing capabilities, while safeguards protect data localisation, privacy, and security.

For this transition to succeed, governments must cultivate three institutional capabilities. Policymakers must develop a structural understanding of AI systems and their societal implications. Decision frameworks must become fully auditable and explainable. Above all, explicit protections must preserve citizen agency within algorithmically mediated systems.

As A K Bhargava argues in his book Manifesto 2050 Humans First, contemporary economic systems remain heavily oriented toward efficiency, growth, and shareholder value. They are far less optimised for human dignity, mental well-being, and social cohesion. A human-centric development model is therefore required.

THE INDIA FACTOR: ARCHITECTURE OVER CAPITAL

India stands at a critical juncture. It can pursue a capital-intensive replication of the Western platform model or design policy and infrastructure that amplify inclusive public value.

From a capital expenditure perspective, particularly in data centre infrastructure, India is significantly outpaced. In 2026, American hyperscalers committed roughly USD 650 billion to AI infrastructure following USD 450 billion in 2025. This infrastructure expansion could push global hardware spending toward the USD 1 trillion mark by 2030, a scale beyond India's current reach.

However, capital alone does not determine success. India's distinct advantage lies in its demographics, its established Digital Public Infrastructure, and its complex social landscape. These factors offer a unique opportunity to design an inclusive socio-economic framework before 2050, aligned with the vision of "AI for all, welfare for all, happiness of all".

If the coming decades offer a single lesson, it is that a prosperous and resilient society requires more than efficient technological systems. It requires systems consciously designed to serve human needs.

The future will undoubtedly be intelligent. The responsibility of this generation is to ensure that it remains unmistakably human.

The author is a management consultant and former Big 4 partner. He writes on business strategy, technology, and geopolitics. (Views are personal.).
feedbackvnd@cybermedia.co.in

TV RAMACHANDRAN

5G'S NEXT TEST: TURNING INFRASTRUCTURE INTO REAL RETURNS

India built a vast 5G infrastructure at a remarkable speed, yet the next phase demands course correction to translate networks into enterprise productivity.

The nascent 1990s saw the advent of 2G, the first GSM-based digital mobile system. Since then, the juggernaut of successive generations has rolled forward inexorably. Seven years ago, 5G was launched commercially on 3 April 2019 in South Korea by SK Telecom, KT, and LG U+.

Within weeks, Verizon launched 5G in the United States. By October 2019, China's three national carriers had begun nationwide deployments. Through 2020 and 2021, Europe, the Middle East and parts of Asia followed. By 2021, more than 60 countries had operational 5G networks.

India entered later. Commercial services began on 1 October 2022. Yet the pace since then has been exceptional. By early 2025, 5G services were reported to be available across more than 99% of districts and to reach roughly 85% of the population. By global standards of rollout velocity, India stands among the fastest.

> There is no conclusive evidence that 5G has enabled mass-market consumer applications or speeds that were technically impossible on 4G LTE-Advanced.

The scale of investment underscores that seriousness. In the 2022 spectrum auction, telecom operators committed Rs 1,50,173 crore—one of the largest single-cycle spectrum commitments globally. That figure excludes network capital expenditure, which itself has been substantial. Industry assessments suggest that capex during the 5G build phase has remained in the range of Rs 70,000–75,000 crore annually (excluding spectrum), directed towards Massive MIMO radios, mid-band densification, fibre backhaul and core modernisation.

The government has also backed the transition in an unprecedented manner, committing an estimated Rs 1,200 crore across at least five initiatives covering test beds, R&D for use cases and other development programmes for 5G and beyond-5G domains. On the surface, the narrative is one of extraordinary momentum.

Yet seven years into global 5G deployment—and nearly three years into India's rollout—the deeper economic question remains open.

ADOPTION VERSUS PERCEPTION IN 5G

Globally, there is still no conclusive evidence that 5G has enabled mass-market consumer applications or speeds that were technically impossible on 4G LTE-Advanced. Its advantages remain largely architectural rather than experiential: greater spectral efficiency, lower theoretical latency, higher device density support, improved energy efficiency per bit and enhanced programmability of networks. None of these improvements, however, is directly visible or necessarily of interest to the average consumer. These are meaningful technical improvements, but they are not, by themselves, transformative.

The adoption curve suggests that, for the average user, the incremental benefit of 5G over 4G LTE-Advanced may not yet be compelling enough to alter switching behaviour. This pattern is not unique to India. In many advanced markets, 5G has primarily improved network capacity and peak speeds rather than enabling visibly new digital behaviours.

NSA AND SA ARCHITECTURE: THE GAP

A critical technical nuance often overlooked in public

IN BRIEF

- India completed one of the fastest 5G rollouts globally, with services reaching over 99% of districts and nearly 85% of the population.
- Consumer experience gains remain modest because many deployments still rely on non-standalone architecture anchored to existing 4G cores.
- The strongest economic case for 5G lies in enterprise deployments across manufacturing, ports, logistics, mining and utilities.
- China's large-scale industrial 5G deployments demonstrate how repeatable enterprise use cases convert trials into viable economics.
- Policy uncertainty around private 5G spectrum access continues to slow enterprise adoption in India.
- High spectrum costs, network capex and rising energy consumption make new revenue models essential for telecom operators.

> 5G's real economic value will emerge when networks integrate deeply with industrial systems rather than remaining a faster consumer connectivity layer.

discourse is the distinction between Non-Standalone (NSA) and Standalone (SA) 5G architectures. Most early deployments globally—including those in the United States, Europe and Asia—were NSA, anchored to existing 4G cores. NSA improves throughput but does not fully enable ultra-reliable low-latency communications (URLLC), deterministic slicing or deeper network programmability.

The transition to enterprise-grade applications typically requires SA cores, network slicing capabilities, and high-fibre connectivity—often exceeding 70% site fibreisation for consistent mid-band performance. The monetisation inflexion point, therefore, is less about rollout and more about architectural migration.

ENTERPRISE 5G AS THE MULTIPLIER

Internationally, the strongest monetisation pathway for 5G has not emerged from consumer speed upgrades but from enterprise deployments in sectors such as manufacturing, ports, mining, logistics and utilities.

Countries that are extracting an economic multiplier from 5G share a common characteristic: industrial deployments are operational at scale rather than on an episodic basis. When 5G becomes embedded in production environments, it begins to deliver measurable operational outcomes.

China's "5G + Industrial Internet" programme is best understood as an industrial policy instrument rather than merely a telecom upgrade. Public briefings indicate that China had already established more than 30,000 5G virtual private networks, over 300 5G-enabled factories and more than 13,000 "5G + industrial internet" projects by mid-2024.

This scale matters because it changes the economics. Once industrial 5G becomes repeatable, it stops being "trial cost" and becomes "unit economics." China is deploying 5G as a backbone for factory modernisation rather than simply as a consumer access layer. In such deployments, monetisation emerges from measurable operational outcomes, such as improved uptime, production yield, predictive maintenance, safety automation, machine vision, and closed-loop control, rather than generic claims of faster internet connectivity.

Region	Policy Approach	Industrial Deployment Scale	Key Enablers
China	National industrial policy integrating "5G + Industrial Internet"	- 30,000+ virtual private networks - 300+ 5G factories - 13,000+ industrial projects	- Centralised industrial digitisation strategy - Strong manufacturing ecosystem - State-backed investments
Europe (Germany focus)	Local spectrum licensing for enterprise campus networks	- 431 local spectrum licences in the 3.7–3.8 GHz band for private networks	- Regulatory support for campus networks - Industry 4.0 integration - Strong manufacturing clusters
India	CNPN framework allowing private networks via telecom operators or direct spectrum assignment	- Limited and largely pilot-based enterprise deployments	- Regulatory uncertainty around direct spectrum vs telecom-mediated models - Evolving enterprise ecosystem

Source: *State Council of the People's Republic of China (English.Gov.Cn); Digital Regulation Platform, The World Bank; and DoT CNPN Guidelines and Spectrum Leasing Framework.*

> China's "5G + Industrial Internet" programme is best understood as an industrial policy instrument rather than merely a telecom upgrade.

Europe's approach differs but remains equally structural. A key enabler has been local spectrum licensing for campus networks, particularly in Germany. By November 2024, Germany's regulator had awarded 431 local licences in the 3.7–3.8 GHz band for enterprise and private networks, enabling deployments across manufacturing sites, airports and logistics parks.

INDIA'S PRIVATE 5G POLICY GAP

India's framework for private networks exists in principle, with the Union Cabinet approving recommendations related to captive non-public networks. However, enterprise adoption remains limited.

The reasons appear to lie less in technological capability and more in policy execution and market design. Uncertainty persists over whether enterprises should receive spectrum directly or rely on telecom operators through leasing or slicing. Eligibility thresholds and demand-assessment requirements have further contributed to a cautious "wait-and-watch" approach among potential adopters.

The consequence is that India's 5G narrative risks remaining consumer-led even when consumer demand alone may not produce significant incremental value. The enterprise layer—particularly across manufacturing, ports, mining, utilities and logistics—could provide the economic multiplier. However, policy friction continues to delay that transition.

ENERGY ECONOMICS OF 5G NETWORKS

Another dimension of 5G that receives limited attention is energy intensity. Mid-band Massive MIMO radios used in 5G deployments are more power-intensive per site compared with legacy 4G infrastructure.

Energy optimisation, therefore, becomes central to long-term network sustainability. Techniques such as AI-driven sleep modes, dynamic spectrum management and more efficient network architectures are increasingly important.

Network economics must simultaneously balance spectrum amortisation from the Rs 1.50 lakh crore auction commitment, sustained annual capital expenditure of roughly Rs 70,000–75,000 crore during deployment phases, and ongoing operating expenditure, including energy consumption and fibre maintenance. Without proportional revenue expansion, financial returns remain constrained.

EXTRACTING VALUE BEFORE 6G ARRIVES

Even as 5G monetisation continues to evolve globally, attention is already shifting towards the next generation. India has articulated a Bharat 6G Vision and approved grants of approximately Rs 240.51 crore for two advanced 6G test beds focusing on terahertz communications and advanced optical networking.

Early participation in research is strategically sensible because standards and intellectual property positions are established years before commercial deployment. However, the strategic risk does not lie in pursuing 6G. The risk lies in treating it as a substitute for extracting value from 5G.

Telecom history suggests that each generational transition follows two phases. The first is a coverage phase marked by rapid rollout, heavy capital expenditure and aggressive marketing. The second is a realisation phase in which networks become economically meaningful through enterprise integration and platform capabilities.

India has completed the first phase with remarkable speed. The next phase must ensure that this foundation produces measurable economic dividends through enterprise deployments, operational efficiency improvements and platform-level revenue opportunities. Only then will 5G evolve from a generational label into programmable productivity infrastructure—and become the most credible bridge to the 6G era.

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

(Research inputs by Neha Hathiari and Debashish Bhattacharya; views are personal.)

feedbackvnd@cybermedia.co.in

Enterprise AI moves from pilots to infrastructure built for scale

Tech leaders at MWC showcased how AI deployment is shifting to production-scale systems built on secure, sovereign and energy-efficient infrastructure.

Photo courtesy: © 2026 GSMA / MWC

BY PRABHU RAM

At Mobile World Congress (MWC) Barcelona 2026, the telecom and cloud ecosystem delivered a clear signal—the industry is moving rapidly from AI experimentation to AI industrialisation. Across briefings, discussions, and demonstrations with companies including AMD, Intel, Nvidia, Qualcomm, Hewlett Packard Enterprise, and Red Hat, the focus shifted from isolated AI experiments to building the infrastructure needed to deploy AI at scale.

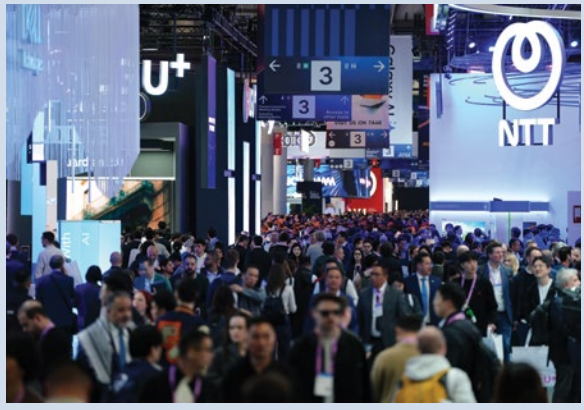
Conversations with industry leaders throughout the event reinforced a central theme: AI-native infrastructure is becoming the foundation of next-generation enterprise and telecom transformation.

ENTERPRISE AI SHIFTS TO PRODUCTION SCALE

Across the event, it was evident that enterprise AI use cases have moved well beyond conceptual demonstrations, and organisations across industries are now embedding AI into operational workflows.

Manufacturers are scaling predictive maintenance systems to reduce downtime. Financial institutions are deploying AI-driven fraud detection and risk analysis. Logistics companies are using digital twins

MWC 2026 indicates that AI adoption is entering a new phase, with enterprises focusing on infrastructure capable of supporting secure production deployments.



IN BRIEF

- Enterprises are embedding AI into operational workflows across industries, including manufacturing, banking, logistics and enterprise IT operations.
- Hybrid cloud architectures and AI platforms are helping enterprises deploy AI while meeting security, compliance and sovereignty requirements.
- Infrastructure providers are evolving from component innovation toward full-stack AI platforms that integrate compute, networking, and orchestration.
- Telecom operators increasingly view AI infrastructure, data centres, and GPU clusters as strategic assets that support national digital capability.
- Early 6G research is exploring AI-native networks that leverage autonomous management and distributed computing to support future digital services.

to optimise supply chains. Increasingly, enterprises are also exploring agentic AI systems to automate business processes and improve workforce productivity.

During a session hosted by Amazon Web Services, the company demonstrated how platforms such as Amazon Bedrock enable enterprises to build agent-based AI workflows, while infrastructure offerings such as AWS Outposts support hybrid deployments that bring AI capabilities closer to enterprise data environments.

These demonstrations underscored a growing reality: enterprise AI adoption is shifting from pilot projects toward production-scale deployments governed by security, compliance, and operational accountability.

INDUSTRIALISING AI ACROSS HYBRID CLOUDS

At an analyst briefing hosted by IBM, the company emphasised that the era of AI experimentation is ending and enterprise AI industrialisation has begun.

Enterprises face mounting pressure to accelerate digital transformation while ensuring governance, security, and trust. Scaling AI across sectors such as banking, telecom, and government requires architectures that are secure by design, sovereign-aware, and capable of orchestrating multiple AI models across enterprise workflows.

IBM highlighted that its hybrid cloud architecture, powered by Red Hat technologies, is designed to help organisations deploy AI globally while respecting regulatory and data sovereignty requirements.

Another notable theme from the discussions was the convergence between AI and quantum computing. IBM has built more than 80 quantum systems globally, with a number already supporting research and optimisation workloads in production environments. While large-scale quantum computing adoption remains several years away, enterprises are increasingly exploring quantum-ready architectures that can evolve alongside emerging computing paradigms.

BUILDING DATA CENTRE SCALE AI PLATFORMS

Another major theme across MWC was the rapid evolution of AI-optimised infrastructure. At the event, Qualcomm demonstrated its rack-scale AI infrastructure platform built around its AI accelerator architecture. The system integrates compute acceleration,

> A broader industry shift is underway: infrastructure providers are moving from component-level innovation to full-stack AI computing platforms for hyperscale deployments.

memory, networking, and orchestration software into a unified platform designed to support large-scale AI inference workloads.

As AI models grow in size and complexity, service providers must balance performance, energy efficiency, and operational scalability. Infrastructure is therefore increasingly evaluated not as standalone silicon but as integrated platforms combining compute, networking, and software orchestration.

This shift reflects a broader industry transformation: infrastructure providers are moving from component-level innovation to full-stack AI computing platforms designed for hyperscale deployments.

SOVEREIGN AI RESHAPING DIGITAL STRATEGY

One of the most compelling strategic discussions at Mobile World Congress featured SK Telecom, which outlined its vision for sovereign AI infrastructure. Unlike many telecom operators that focus primarily on AI applications, the company is pursuing a vertically integrated approach across the AI stack. It is investing in hyperscale AI data centres, GPU clusters, and cloud platforms designed to attract global AI workloads while supporting domestic innovation.

It is also developing its own foundation models and multimodal AI capabilities while collaborating with global technology partners to expand the broader ecosystem. The company's vision positions telecom infrastructure as the backbone of national AI capability, delivering compute infrastructure, AI platforms, and industrial applications across sectors such as semiconductors, manufacturing, and energy.

This strategy reflects a broader global trend: governments and telecom operators increasingly view AI infrastructure as strategic national infrastructure.

AI-NATIVE NETWORKS PREPARE PATH TO 6G

Looking ahead, many companies at MWC outlined how future telecom networks will evolve into AI-native platforms. Industry initiatives led by companies including Qualcomm, Nvidia, and Google Cloud are exploring how to embed AI directly into network operations to enable autonomous management, predictive optimisation, and real-time service orchestration.

These developments are also shaping early work on 6G network architectures, where AI, sensing technologies, and distributed compute infrastructure will converge to enable entirely new digital services.

Commercial 6G deployments are expected later in the decade, but the foundational research and ecosystem collaborations are already underway.

THE STRATEGIC SHIFT TO AI-NATIVE INFRASTRUCTURE

Together, the discussions, demonstrations, and analyst briefings at MWC 2026 highlight a profound shift in the technology landscape.

One, enterprise infrastructure is evolving towards a model that spans hybrid environments across cloud, edge, and private deployments, while increasingly embedding AI-orchestrated automation across operational processes. Two, organisations are becoming more sovereign-aware as they address regulatory obligations and national policy requirements, and three, these architectures are also being designed to remain future-ready, preparing enterprises for emerging computing paradigms, including quantum technologies.

For enterprises, the opportunity lies in building architectures that support the convergence of AI, intelligent connectivity, and distributed computing. For telecom operators, the opportunity may be even greater. As networks evolve into AI-native platforms, telecom infrastructure itself could become the foundation for large-scale AI innovation across industries.

MWC 2026 made one point unmistakably clear: the next phase of digital transformation will not simply be defined by AI applications, but by the AI-native infrastructure that powers them.

The author is the VP at CyberMedia Research (CMR) and has served as a GSMA GLOMO Awards judge across multiple editions of MWC at Barcelona and Shanghai.

feedbackvnd@cybermedia.co.in

Telecom becomes responsible AI's toughest governance test

As AI embeds deeper into telecom networks, operators must build explainability, sovereignty and auditability into systems where failure carries systemic risk.

BY SHUBHENDU PARTH

As artificial intelligence (AI) moves deeper into enterprise operations, the question is no longer whether AI can scale, but whether it can scale responsibly. Few industries expose this challenge as clearly as telecom, which has emerged as the backbone of the digital economy.

Telecom networks operate in real time, underpin critical services, and are subject to continuous regulatory

> Responsible AI in telecom is not only about ethics frameworks but about preserving reliability in networks that support economies and essential services.

"Telecom is harder because AI operates inside critical real-time infrastructure, where mistakes can affect service continuity, emergency access and national resilience."

KALYAN KUMAR, Chief Product Officer, HCLSoftware

IN BRIEF

- Telecom networks are the toughest proving ground for responsible AI because automated decisions can affect service continuity and trust.
- Survey data shows telecom firms split between pilot and early transformation stages, signalling progress in responsible AI adoption.
- Unlike digital platforms, telecom must deploy AI under regulatory, licensing and sovereignty rules, making explainability essential.
- Many enterprises pilot bias detection and explainability tools, but far fewer have implemented privacy audits or formal fairness metrics.
- Telecom operators are introducing oversight boards and explainable AI systems to keep automated decisions transparent and defensible.
- As AI becomes operational infrastructure rather than experimentation, telecom governance models may guide other regulated sectors.

oversight. Decisions made by AI systems—whether in network optimisation, fraud detection or customer engagement—can have immediate operational and societal consequences. This makes telecom a natural stress test environment for responsible AI.

The recently-released Tech Trends 2026 report by HCLSoftware positions telecom at a crucial juncture. The survey data shows a balanced maturity curve, with roughly half of telecom organisations in pilot stages and half in early transformation for responsible AI adoption. This reflects both momentum and caution.

This primary research conducted by MarketsAndMarkets is based on inputs from over 173 CXO- and director-level respondents across industries and regions. It includes large-scale sentiment and signal analysis and secondary research spanning analyst reports, industry publications and market data.

WHY TELECOM CANNOT ADOPT AI LIKE DIGITAL NATIVES

Unlike digital first industries, telecom cannot afford opaque AI systems. Networks must be reliable, customer decisions defensible, and regulatory obligations met across jurisdictions. As AI systems take on more responsibility, explainability and accountability become non-negotiable.

"Telecom is harder because AI is acting inside critical, real-time infrastructure—not just inside digital channels," said Kalyan Kumar, Chief Product Officer at HCLSoftware. "In a digital native business, an AI mistake is usually a customer experience defect. In telecom, it can become a service continuity, emergency access, or national resilience issue."

He added that telecom AI agents do not optimise one domain at a time. "They act across network performance, spectrum, energy, and customer operations simultaneously. The exposure is systemic—and the bar for

> The scale, complexity and regulatory oversight of telecom networks make the sector one of the first where autonomous AI must prove accountability.

explainability, reliability and accountability is materially higher," Kumar said.

The report shows that 34% of enterprise leaders now rank cybersecurity, trust and transparency as near-term priorities, with responsible AI already reshaping decision-making. More than 90% cite ethics, brand reputation and risk avoidance—rather than regulation—as the primary drivers of responsible AI adoption.

For telecom operators, however, regulation is not secondary. "In telecom, regulation is not downstream—it is the starting condition," Kumar said. "Responsible autonomy must operate under licence obligations, neutrality requirements, auditability and sovereignty constraints."

He added that digital sovereignty in telecom is "practical, not philosophical", because cross-border data rules, lawful access requirements and localisation mandates collide directly with autonomous operations. "The system is always on, and the blast radius is real," Kumar said.

HOW RESPONSIBLE AI IS TAKING SHAPE INSIDE TELECOM

The report highlights that responsible AI is moving from principle to practice, though unevenly. Across industries, 71% of enterprises have moved from exploration into pilots or early adoption. In telecom, governance mechanisms such as AI oversight boards and explainable AI tools are becoming more common.

Yet deeper maturity indicators lag. While 76% of organisations are piloting bias detection tools and 78% are experimenting with explainability, only 37% have conducted privacy audits, and just 7% have tested formal fairness metrics. This gap is significant in a sector handling sensitive customer and network data at scale.

Kumar said telecom's operational reality is forcing earlier institutionalisation of governance. "Telecom is being compelled to operationalise responsible AI sooner because autonomy is entering mission critical, always on systems first," he said. "Governance cannot be layered on later—it has to be embedded into architecture."

He noted that this extends beyond internal controls. Telecom operators must ensure that AI systems can explain how traffic is prioritised, how data is accessed and localised, and how decisions are made across interconnected networks without breaching jurisdictional rules. "Cross operator interoperability has to be maintained without violating regional policy constraints," Kumar said. "That requires clear human–machine decision boundaries in high impact scenarios."

TELECOM AS A REFERENCE MODEL FOR REGULATED AI SCALE

Digital sovereignty further complicates the picture. Telecom operators must manage data localisation requirements, lawful interception obligations and cross border operations simultaneously. The report notes that organisations treating sovereignty as a core architectural principle are significantly more advanced in scaling trusted AI systems.

"Industries that manage autonomy under the toughest constraints tend to define standards for others," Kumar said. "Telecom is effectively building a reference architecture for responsible autonomy—showing how AI can scale without losing control, trust or societal licence to operate."

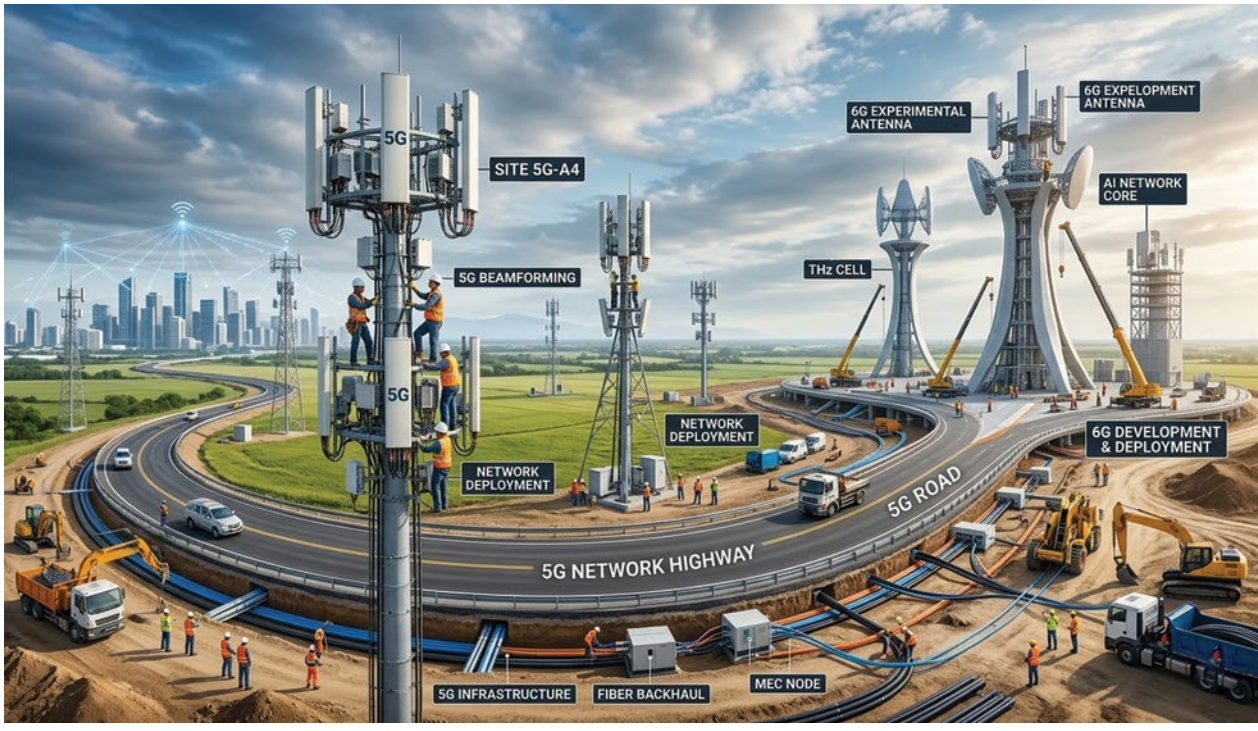
Energy, utilities and financial services face similar pressures, but telecom's scale, interconnectedness and real-time requirements make its experience particularly instructive.

As AI becomes infrastructure rather than experimentation, telecom's ability to combine autonomy with accountability may influence how other regulated sectors design their governance frameworks. Responsible AI, in this context, is no longer a defensive posture. It is becoming the condition for scaling intelligent systems where reliability, compliance and public trust cannot be compromised.

shubhendup@cybermedia.co.in

Is 5G paving the road or blocking the path to 6G

As telecoms prepare for 6G, the industry must ask whether 5G investments and upgrades will become a launchpad for the next G or complicate the journey.



BY PRATIMA HARIGUNANI

There is headwind. There is tailwind. And then there is the crosswind. Right now, it is difficult to say which way 5G has been blowing to determine the real speed and direction of 6G. This generation marked an important milestone, ushering the world into a new era of digitalisation, modularity, AI, immersive services, low-latency applications, and new approaches to networks, such as automation, real-time intelligence, predictive controls, slicing, and private networks.

Now that the industry is looking towards the next generation—6G—it is a good moment to ask an important question: will investments in 5G serve as stepping stones towards 6G, or complicate that transition?

5G ADVANCED AS A TRANSITION PLATFORM

Has 5G Advanced served as a useful on-ramp for 6G? Sanjay Sehgal, CEO and MD, TP-Link India, believes it has. "It has been a good precursor, given that even 5G required software and hardware refresh cycles and interoperability catch-ups. In that sense, it worked as a useful dress rehearsal."

Pinkesh Kotecha, MD and Chairman of Ishan Technologies, also argues that 5G Advanced has helped lay the groundwork for 6G from an infrastructure and network-readiness perspective. "In India, 5G Advanced introduces features such as improved network efficiency, better latency control and early AI-based network management. These upgrades allow operators and

ICT providers to test new capabilities on live networks without waiting for an entirely new generation."

Andrew Kitson, Director of Technology at BMI, notes that 5G Advanced has yielded insights relevant to future technologies. "It has offered useful insights into AI-native networking, integrated sensing and communications and energy efficiencies that could form the basis of future 6G technologies."

However, he cautions that spectrum choices will be critical. "The higher frequencies initially chosen for 5G struggled with urban and in-building coverage and created cost challenges for enterprise and industrial IoT use cases."

These lessons are shaping early discussions around how future spectrum bands must balance performance with practical deployment economics across dense cities, indoor environments and industrial connectivity scenarios. "6G needs careful thought, with sophisticated use cases placed at the centre of development work," Kitson says.

Kotecha similarly emphasises that 5G Advanced is not a substitute for 6G. "While it improves performance and reliability, 6G will require new spectrum bands, deeper AI integration into network design and fresh approaches to sensing and connectivity. What 5G Advanced has done well is provide India with a stable platform to build skills and test use cases."

John Strand, CEO of Strand Consult, notes that such evolutionary steps are not new. "Operators are speaking about 5G Advanced today much in the same way that 4G evolved into LTE-Advanced. However, these upgrades have not necessarily translated into significantly better sales or earnings for mobile operators."

This raises another question: will the enormous investments in 5G infrastructure act as a bridge to 6G—or become a burden?

5G CAPEX AND THE ROAD TO 6G

With billions invested in 5G networks and returns still emerging slowly, capital expenditure inevitably shapes the conversation about 6G.

Sehgal believes telecom operators will continue investing while older technologies remain in use. "There will always be lower-end users consuming earlier technologies. For example, 3G remains present in parts of rural India. Adopting 6G will not prevent operators from monetising already-deployed technologies."

Kotecha agrees that slower returns on 5G will influence the pace of spending. "Telecom operators in India are still improving 5G monetisation, particularly through enterprise connectivity, private networks and cloud-led services. Over the next few years, the focus will be on sweating existing assets rather than rushing into another large capex cycle."

This partly explains why 6G timelines are aligning closer to 2030, allowing operators to stabilise returns from 5G while technology development continues.

BEYOND THE LADDER TOWARDS A 6G CLIMB

For Kotecha, the more important discussion is how networks will support future demands. "Energy efficiency, AI-driven network operations, satellite integration and support for industrial and public-sector use cases will be central to the relevance of 6G in India."

Thomas van Briel, Chief Network Architect at Group Technology of Deutsche Telekom, notes that the current phase is still exploratory. "6G research is identifying promising technologies and defining future requirements. Multi-stakeholder collaboration will be critical to realise its innovation potential."

Strand believes technology alone will not determine success. "The most important element for 6G will be new services and business models. Without them, it could become another commercial disappointment." Kitson also warns that 6G may risk becoming little more than a faster version of 5G if development focuses primarily on mass-market visions rather than transformative machine communication.

Van Briel nevertheless expects a gradual evolution. "5G Advanced represents a step towards 6G. We expect a largely software-based transition, with early 6G deployments in the early 2030s while 5G remains mainstream for at least another decade."

For now, 5G appears less like a runway to 6G and more like a taxiway—guiding the industry forward, even if the final direction of flight is still uncertain.

pratimah@cybermedia.co.in

FROM PILOTS TO PLATFORMS: INDUSTRIAL IOT GROWS UP

Factory systems are evolving into a layered digital infrastructure where sensors, connectivity, edge computing and AI are driving real-time operational decisions.

BY SHUBHENDU PARTH

India's factory floors are entering a new phase of digitisation—one that is moving beyond isolated sensors and dashboards toward a production-grade digital infrastructure capable of ingesting, processing and acting on operational data in real time.

Across manufacturing hubs, from automotive clusters to chemical plants and foundries, predictive maintenance systems are scaling beyond proof-of-concept. Today, connected worker platforms are improving safety in hazardous environments and artificial intelligence (AI)-driven video analytics is becoming a routine operational input alongside Supervisory Control and Data Acquisition (SCADA) and Manufacturing Execution Systems (MES).

This shift is not just about deploying more sensors. Rather, it reflects a deeper transformation: Industrial Internet of Things (IIoT) is evolving into a structured infrastructure layer spanning sensorisation, connectivity, edge computing, cloud platforms, AI pipelines, operational technology (OT) security and integrated operational workflows.

Praveen Arora, Vice President – IoT Unit at Tata Communications, describes the transition as a move from reactive monitoring toward proactive operational systems. Industrial environments, he notes, are increasingly integrating data streams from sensors, machines, enterprise applications and manufacturing systems into a single operational view.

"The shift is taking place through integration of data coming from sensors, devices, enterprise systems and manufacturing systems on the shop floor," Arora says. "Industrial systems are moving from reactive alerts to proactive operational intelligence."

Increasingly, this digital layer is being treated as an industrial backbone—similar to power systems, safety instrumentation and telecommunications connectivity—rather than an IT add-on.

Experts indicate that for the first time, India's IIoT deployments are moving beyond isolated pilots and becoming enterprise-wide operational platforms.

"IoT deployments scale only when connectivity, device management and orchestration are treated as foundational infrastructure."

R GOPALAKRISHNAN
EVP, Chief Technology Officer, & Head – IoT, Vi Business

"Industrial systems are moving from reactive alerts to proactive operational intelligence as data from sensors, machines and enterprise systems converges."

PRAVEEN ARORA
Vice President – IoT Unit, Tata Communications

IN BRIEF

- Industrial IoT in India is moving beyond isolated pilots toward production-grade infrastructure supporting real-time operational intelligence.
- Modern IIoT stacks combine sensors, connectivity, edge computing, cloud platforms and AI pipelines into integrated factory platforms.
- Manufacturers increasingly treat connectivity as a foundational layer supporting digital twins, predictive maintenance and analytics.
- Hybrid edge-cloud architectures enable factories to process time-sensitive data locally while using cloud platforms for AI training.
- Operational technology security is emerging as the weakest link as factories connect legacy machines and control systems to networks.
- Large deployments, such as smart electricity meters, demonstrate how IIoT networks are becoming part of the national digital infrastructure.

Sushant Rabra, Partner and Head of Digital Strategy and Transformation at KPMG in India, d escribes the transition as a shift from experimentation to operational systems tied directly to performance metrics.

"IIoT initiatives are scaling beyond isolated pilots into full-factory platforms linked to revenue, throughput and energy efficiency," Rabra says, adding that transformation is no longer about presentations and strategy discussions. "It is about operational metrics."

That operational shift is visible in the questions industrial leaders are now asking. Enterprises are no longer asking whether IoT works; they are asking who owns the outcome and how deployments scale across multiple plants and production environments. Sunil David, Digital Technology Consultant, observes that the focus has shifted from technology demonstrations to measurable operational improvements.

"IIoT in India is graduating from experimentation to infrastructure," he explains. "The organisations that succeed will not be those running the largest number of pilots, but those converting operational data into repeatable decisions at shop-floor speed," David says.

The transformation is also institutional in nature. IIoT is increasingly governed by formal risk frameworks, regulatory compliance structures and contractual accountability mechanisms. According to Gaurav Sahay, Founding Partner at Arthashastra Legal, the shift reflects a broader maturity in how industrial digital systems are deployed and managed.

"The defining change is the transition from isolated proof-of-concept deployments to production-grade digital infrastructure embedded into oper-ational and compliance frameworks," Sahay explains. "IIoT is moving from experimentation to regulated infrastructure where architecture design, cyber-security governance and contractual accountability become central."

"IIoT initiatives are scaling beyond isolated pilots into factory-wide platforms tied directly to revenue outcomes, throughput gains and energy efficiency."

SUSHANT RABRA
Partner & Head – Digital Strategy & Transformation, KPMG in India

The implications for India's manufacturing sector are significant. IIoT is no longer simply about connecting machines; it is about engineering a resilient digital infrastructure layer capable of sustaining continuous operations, improving safety and delivering measurable business value.

BUILDING THE INDUSTRIAL IOT STACK

Traditional IIoT deployments in India often began as isolated experiments—temperature sensors installed on individual machines, vibration monitoring on critical equipment, or dashboards tracking energy consumption within a single production facility. While such initiatives demonstrated the potential of connected systems, they rarely transformed operations at scale.

The new generation of deployments looks fundamentally different. Enterprises are building multi-layered architectures that resemble modern digital infrastructure stacks, where each layer performs a distinct operational function.

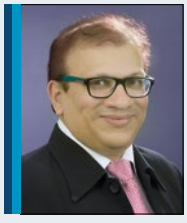
At the foundation lies sensorisation: industrial sensors, smart cameras, wearable devices and gateway hardware that convert physical events on the shop floor into structured digital signals. These sensors feed into the connectivity layer, which may include industrial Ethernet, Wi-Fi, low-power wide-area networks (LPWAN), private Long Term Evolution (LTE) systems or private 5G cellular networks.

Above the connectivity layer sits the compute tier, where edge devices process data close to the production line to ensure low-latency response and operational continuity. Cloud platforms provide the next tier, enabling large-scale data aggregation across multiple facilities, AI model training and enterprise system integration. Finally, the intelligence layer, where analytics engines, AI models, and workflow systems translate data into decisions and actions that influence daily operations.

Arora notes that industrial deployments are increasingly integrating operational systems that historically functioned independently. "In large manufacturing environments, interactions across production lines, auxiliary systems and logistics workflows generate enormous volumes of operational data," he explains.

"The objective now is to bring these interactions together into what we call a 'factory span', where the shop floor and enterprise systems operate within a unified digital environment."

Modern IIoT architecture in India is therefore layered and hybrid by design. Ritwij Kulkarni, Regional General Manager at Honeywell Process Automation, explains that this architecture is particularly relevant for brownfield plants where legacy infrastructure must be modernised without replacing core equipment. "In many Indian plants, IIoT is essentially a retrofit exercise," Kulkarni says.



"In many Indian factories, IIoT is essentially a retrofit exercise, adding sensors and gateways to legacy systems to unlock predictive maintenance."

RITWIJ KULKARNI
Regional General Manager, Honeywell Process Automation

"IIoT in India is graduating from experimentation to infrastructure where operational data drives repeatable decisions at shop-floor speed."

SUNIL DAVID
Digital Technology Consultant

He further adds: "Sensors and edge gateways are added to legacy programmable logic controller (PLC) and distributed control system (DCS) environments, allowing operational data to flow into digital platforms where predictive maintenance and performance optimisation can be applied."

These layered architectures enable brownfield facilities to extract new value from existing assets without disruptive equipment replacement. The result is improved equipment visibility, better asset utilisation and more informed operational decision-making.

However, the architecture must also accommodate practical constraints. Sandeep Redkar, Consultant Leader at Rockwell Automation India, notes that most manufacturing facilities operate equipment that was never designed for connectivity. "Modern IIoT architecture in India is shaped by brownfield realities," he says, highlighting that plants often run equipment that is ten to thirty years old. "The architecture must work around those constraints rather than replacing entire production systems."

As a result, many deployments rely on hybrid architectures in which on-premises edge systems handle local operations while cloud platforms support analytics and enterprise integration.

CONNECTIVITY BECOMES INDUSTRIAL BACKBONE

While sensors and analytics attract considerable attention, connectivity remains the foundation of IIoT deployments. Unlike consumer applications, industrial systems must function reliably in environments where connectivity disruptions can halt production, damage equipment, or create safety risks.

For telecom service providers supporting IIoT, connectivity must therefore be engineered as a foundational layer rather than an afterthought. R Gopalakrishnan, Executive Vice President, Chief Technology Officer, and Head of IoT at Vi Business, emphasises that IoT deployments succeed only when network architecture is designed specifically for industrial requirements.

"IoT scales only when it is approached as foundational infrastructure rather than an isolated project," he says, adding that connectivity, device management and orchestration are non-negotiable building blocks.

Industrial connectivity must account for reliability, redundancy and lifecycle management. In large deployments, network architecture determines whether systems can operate continuously across distributed environments.

"Network-first design is critical," Gopalakrishnan explains. "Industrial deployments require robust operations, lifecycle management and redundancy mechanisms to ensure that operations continue even under network stress," he adds.

"Modern IIoT architecture in India must work around brownfield realities where factories operate equipment that may be decades old."

SANDEEP REDKAR
Consultant Leader, Rockwell Automation India

"IIoT is moving from proof-of-concept deployments to regulated infrastructure where cybersecurity governance and contractual accountability matter."

GAURAV SAHAY
Founding Partner, Arthashastra Legal

Another challenge slowing IIoT expansion is interoperability across heterogeneous industrial systems. Gopalakrishnan notes that proprietary protocols and vendor-specific integrations can complicate large-scale deployments. As a result, enterprises increasingly prioritise open standards and multi-vendor interoperability to avoid long-term technology lock-in and integration complexity.

Connectivity also plays a role in enabling new operational models. Private cellular networks, including private LTE and 5G systems, are gaining attention in manufacturing environments where reliability, security and mobility requirements exceed the capabilities of traditional wireless local area networks.

David notes that manufacturers increasingly view connectivity as a strategic enabler of digital transformation. "Manufacturers need high-speed, reliable and secure connectivity to support technologies such as IoT, AI and digital twins," he points out, indicating that private wireless networks are fast becoming part of the discussion, although adoption in India is still evolving.

EDGE AND CLOUD SHARE THE WORKLOAD

One of the most important architectural decisions in IIoT deployments is determining where computation should occur. Some processes must operate locally at the edge to guarantee real-time response, while others benefit from the scalability and computational power of cloud platforms.

The choice between edge and cloud is therefore driven primarily by operational requirements rather than technology preferences. Gopalakrishnan explains that edge environments typically handle latency-sensitive workloads such as real-time analytics, video processing and protocol translation. "Edge workloads support tasks that require immediacy—real-time analytics, local control and data buffering," Gopalakrishnan says. "Cloud environments are better suited for AI model training, fleet-wide analytics and enterprise integration."

David frames the decision similarly, describing edge and cloud as complementary elements of a broader data architecture. "At the edge, controllers and sensor systems must make decisions in milliseconds," David explains. "The cloud becomes the system of record for analytics, machine learning pipelines and digital twin environments."

Hybrid architectures combining edge and cloud capabilities are therefore emerging as the dominant model. Edge systems ensure operational continuity and deterministic response, while cloud platforms enable large-scale analytics and cross-plant visibility. Arora points out that video analytics deployments clearly illustrate this hybrid architecture. Cameras deployed across production lines often support multiple operational use cases—from monitoring worker safety to detecting productivity deviations and material movement.

"These video analytics systems often run multiple use cases simultaneously," he says, adding that processing

"Production-grade IIoT networks must deliver consistent performance over decades, and architecture determines whether systems scale."

SEBASTIAN PELLORCE
Senior Vice President – AMI India, Wirepas

> For India's manufacturing sector, IIoT is evolving from machine connectivity to resilient digital infrastructure that supports safety, continuity, and measurable value.

happens at the edge for immediate response, while model training and optimisation take place in the cloud to improve accuracy over time.

DIGITAL TWINS MOVE TOWARD OPERATIONS

As IIoT infrastructures mature, attention is shifting toward the intelligence layer that converts operational data into actionable insights. Digital twins are becoming a key component of this layer. Once considered primarily as a modelling tool, digital twins are increasingly being used to monitor and optimise live industrial operations.

Kulkarni notes that digital twins are evolving rapidly in Indian process industries, particularly in sectors such as chemicals and refining, where operational optimisation delivers significant financial benefits.

"Digital twins are moving beyond static modelling," Kulkarni says. "Today they are real-time replicas used for predictive maintenance, anomaly detection and operational optimisation."

However, the maturity of digital twins varies across industries. Redkar cautions that while monitoring twins are widely deployed, more advanced predictive and prescriptive twins require a robust data infrastructure. "The monitoring twin—essentially a real-time mirror of asset conditions—is already operational in many plants. Predictive and prescriptive twins remain limited by data quality and IT–OT integration," he explains.

SECURITY BECOMES THE WEAKEST LINK

As factories connect machines, sensors and control systems to digital networks, the attack surface expands dramatically. IIoT deployments, therefore, introduce new cybersecurity challenges, particularly in environments where legacy systems were never designed for connectivity. However, one concern that consistently surfaces across industry conversations is how operational technology security is the most under-invested layer of the IIoT stack. Rabra describes operational technology security as the fastest-growing risk in connected factories.

"The weakest link in India's IIoT stack today is operational technology security," Rabra says. "As factories connect legacy equipment and controllers to enterprise systems, attack surfaces multiply faster than security investments."

According to Rabra, the problem is rooted partly in the historical design of industrial systems. Operational technology environments were traditionally isolated from external networks, and many organisations still treat OT security as an extension of information technology security rather than a specialised discipline. As legacy machines become connected to enterprise platforms and cloud systems, this assumption is rapidly breaking down.

Sahay notes that IIoT deployments increasingly require formal governance mechanisms to manage cyber risks and regulatory exposure. "IIoT systems are now being deployed with defined cybersecurity architecture, data governance frameworks and contractual accountability," he explains. "Security must be designed into the architecture rather than added after deployment."

Similarly, David adds that device lifecycle management is emerging as a second critical challenge as deployments scale. Enterprises must manage firmware updates, certificate management, provisioning and asset lineage across thousands of connected assets operating over long industrial lifecycles.

"Scaling IIoT is not only about connecting devices. You also have to manage them securely for 10 to 15 years. Security and lifecycle discipline are what separate pilots from production-grade infrastructure," he explains.

INFRASTRUCTURE LESSONS FROM SCALE

The importance of architecture becomes even clearer when IIoT deployments reach a national scale. A case in point is the smart electricity meter ecosystem, where millions of connected devices now operate as part of India's digital infrastructure. Sebastian Pellorce, Senior Vice President AMI India at Wirepas, notes that more than ten million smart electricity meters in India now operate on decentralised mesh networks. "These are not pilot deployments. They are production networks supporting daily grid operations," he points out.

> For telecom service providers, IIoT success depends on network architectures engineered for reliability, redundancy and lifecycle management in industrial environments.

In decentralised mesh networks, each device participates in routing and network management, eliminating single points of failure. As additional devices are deployed, the network becomes stronger rather than weaker, allowing large infrastructure systems to scale organically.

The success of such deployments depends heavily on architectural design. In mesh networks, each device participates in routing and network management, enabling systems to scale without central bottlenecks. "Production-grade systems must deliver consistent performance over decades," Pellorce explains. "Architecture determines whether deployments remain pilots or become infrastructure."

COMMERCIAL MODELS BEGIN TO SHIFT

IIoT deployments in India are also triggering changes in commercial models. While core plant infrastructure—sensors, gateways and connectivity—continues to be funded through capital expenditure, surrounding software and analytics layers are increasingly delivered through subscription or managed-service frameworks.

David notes that many manufacturing deployments now follow hybrid models combining capital investment with recurring service layers. "Typically, connectivity infrastructure and sensors remain capital expenditure, while analytics, reliability services and predictive maintenance platforms move toward subscription models," he says.

Pellorce observes similar trends in large infrastructure programmes such as smart metering. Long-term service contracts increasingly tie vendor revenues to operational performance metrics such as uptime and reliability.

FROM PILOTS TO OPERATIONAL BACKBONE

Ultimately, the success of IIoT depends on its ability to deliver measurable improvements in operational performance. Across manufacturing sectors, common use cases include predictive maintenance, energy optimisation, quality monitoring and worker safety.

David cites the example of Tamboli Castings, a Gujarat-based investment casting manufacturer, where phased Industry 4.0 initiatives have delivered measurable operational improvements. The company deployed SCADA-based overall equipment effectiveness (OEE) monitoring and predictive maintenance systems that use thermal imaging and sensor analytics.

These systems reduced computer numerical control machine downtime by 10–12%, while predictive maintenance alone delivered annual energy savings of approximately Rs 8.8 lakh. Robotics deployed for hazardous operations also improved safety while reducing manual intervention.

He further highlights examples where digital technologies have delivered tangible operational benefits. "In many manufacturing deployments, IoT-driven predictive maintenance and analytics have reduced downtime, improved energy efficiency and increased production throughput," David says.

However, the transition from pilot to production is not automatic. Redkar notes that many projects stall because pilots are designed as technology demonstrations rather than operational systems. "Pilots often prove the technology but not the integration and organisational readiness required to scale," he explains.

Sahay adds that governance maturity plays a critical role in determining whether programmes succeed. "The initiatives most likely to fail are those treated as technology deployments rather than institutional transformations," he shares.

The emerging lesson is clear: IIoT success depends less on individual technologies and more on architecture, governance and operational discipline. In India's manufacturing sector, the shift from pilots to platforms is already underway. The next phase will determine how effectively industrial enterprises convert digital infrastructure into sustained productivity gains.

IIoT is no longer a technology experiment. It is becoming part of the operational backbone of modern manufacturing.

shubhendup@cybermedia.co.in

The invisible security moat in a connected world

As cyber risks grow in hyperconnected systems, air-gapping resurfaces as a protective barrier for critical assets, even as modern networks demand secure connectivity.

BY PRATIMA HARIGUNANI

If you see someone walking through a crowded mall wearing PPE, you might assume they are either extremely cautious or unusually paranoid. If you watch a 1970s Bollywood father locking his daughter away in a distant castle on a remote island to prevent a clandestine marriage, you might laugh while recognising the logic behind his tactic of pre-emptive isolation.

What explains such approaches of physical distance and deliberate isolation in spaces where connections normally fuel both life and mischief? The answer is simple: the instinct for safety and protection from threats that spread easily through excessive connectedness.

In essence, air-gapping is the modern equivalent of a moat around a castle. It is the foam, the vacuum, the buffer that separates an important asset from the digital tides around it. In plain terms, it is exactly what it sounds like: placing air between something one wants to protect and something that might exploit it.

UNDERSTANDING THE LOGIC OF AIR-GAPPED SECURITY

Air-gapping is a security approach that relies on the physical isolation of assets, data, or systems from networks and external devices. By breaking links with environments connected to networks, air-gapping

"Air-gapping offers complete isolation, but most enterprise environments require controlled connectivity. Segmentation often provides a more practical security balance."

SEKAR VEMBU
Founder & CEO, Vembu Technologies

offers a robust way of protecting critical devices and data from infiltration, cyberattacks, disasters, accidents, and exploitation.

It can also provide a reliable method for backing up data, which becomes invaluable during hardware failures, denial-of-service attacks, ransomware incidents, network intrusions, or system corruption.

In its most literal form, air-gapping can be entirely physical and airtight, allowing access only through direct physical interaction with a system that is strictly separated from all networks. This involves removing cables, disabling Wi-Fi, shutting down plug-ins, and eliminating wireless interfaces or communication channels.

However, air-gapping does not always have to be purely physical. It can also be logical, where systems are disconnected from networks through configuration or firewall rules. In many modern deployments, hybrid approaches combine network segregation, encryption, hashing, and strict access controls.

WHERE AIR-GAPPING STILL MAKES SENSE TODAY

Whether implemented physically or logically, air-gapping can provide a powerful barrier against remote attacks, malware, cyber incidents, and data exfiltration. The approach is particularly relevant for environments where compromise would have severe consequences.

These include critical infrastructure, defence systems, medical equipment, oil and gas facilities, shipping operations, mining environments, and industrial control systems such as Supervisory Control and Data Acquisition (SCADA) platforms. Industries such as refineries and energy utilities often consider air-gapping because the operational risks associated with network intrusions are extremely high.

The rapidly expanding Internet of Things (IoT) landscape, with its vast web of connected devices, is

STRENGTHENING AIR-GAPPED SECURITY

- Air-gapping can provide strong isolation, but gaps in processes, access controls, and operations can still expose systems to risk. Organisations therefore need disciplined practices to ensure that isolated systems remain secure, functional, and manageable over time.
- Use secure off-site facilities and isolation techniques for sensitive systems.
- Restrict access to authorised personnel and enforce strict physical controls.
- Regularly test, audit, and encrypt air-gapped systems and stored data.
- Prepare for threats such as wireless sniffing, social engineering, and covert channels.
- Protect against supply-chain compromise and physical infiltration.
- Secure data transfers through controlled channels and hardened removable media.
- Guard against USB-based malware, hardware implants, and human error.
- Plan upgrades carefully, as internet-based patching may not be possible.
- Design resilient architectures with continuous monitoring and hardware-based controls such as cross-domain security solutions.
- Anticipate operational challenges, including higher costs, slower patch cycles, and limited compatibility with cloud-centric environments.

"A true air gap removes the possibility of remote access attacks, which makes it valuable for protecting critical infrastructure systems where compromise is unacceptable."

JP MISHRA
Founder & CEO, Deep Algorithms

also frequently cited as an area where some degree of isolation may help protect sensitive assets.

Sekar Vembu, Founder and CEO of Vembu Technologies, explains the difference clearly: "Air-gapping is absolute isolation. Network segmentation is controlled connectivity. In practice, segmentation is suitable for most enterprise IoT deployments. Air-gapping is justified only where the cost of compromise is extremely high."

JP Mishra, CEO and Founder of Deep Algorithms, also highlights why the approach remains relevant in IoT and edge computing environments. Edge IT and IoT ecosystems share a fundamental weakness: many devices were originally designed without security as a primary consideration.

"While traditional air-gapping was intended for static, isolated systems and can seem impractical in today's highly connected edge and IoT ecosystems, it has become more important than ever, depending on the sensitivity of the digital asset being protected. Unlike software-based control mechanisms, a true air gap eliminates the possibility of remote network access with malicious intent," Mishra explains.

He adds that the consequences of compromise in critical infrastructure environments, such as power grids and nuclear facilities, are too severe to ignore. In such cases, maintaining air-gapped control systems can remain a worthwhile trade-off despite operational limitations.

MODERN ALTERNATIVES TO COMPLETE ISOLATION

Not everyone agrees that full physical isolation is practical in modern digital environments. Vivek Srivastava, Country Manager at Fortinet, argues that although air-gapping remains relevant in highly sensitive sectors such as defence and nuclear infrastructure, it is increasingly difficult to implement in today's connected world. Industrial systems, smart devices, and distributed operational environments require continuous data exchange for monitoring, analytics, and operational efficiency.

In these circumstances, modern security architectures attempt to replicate some of the benefits of air-gapping without completely disconnecting systems. "Rather than disconnecting systems entirely, organisations create tightly controlled, policy-driven environments where communication is allowed but continuously inspected, authenticated, and monitored," Srivastava says. Approaches such as logical segmentation, Zero Trust architectures, and unidirectional gateways are therefore gaining traction.

According to Srivastava, intelligent segmentation combined with strong identity controls and real-time threat intelligence can often deliver more scalable protection than complete isolation in enterprise IoT and edge deployments. Vembu also highlights the architectural differences between these approaches.

Network segmentation divides a network into zones and restricts traffic between them, thereby reducing the potential "blast radius" of an attack. "If rules are misconfigured, attackers can move laterally," Vembu notes. "Zero-trust models assume nothing is trusted and everything is verified. But they also assume connectivity."

OPERATIONAL CHALLENGES OF AIR-GAPPED SYSTEMS

Air-gapping may sound deceptively simple, but implementing it in real environments can be far more complex than merely disconnecting a cable. Mishra points out that physical, logical, and hybrid air-gapped environments require extremely strict data-transfer and access-control protocols. Among these models, the fully physical air gap introduces the greatest operational complexity and often-overlooked cost: operational friction.

"Full physical isolation is rarely practical in modern connected operations, so organisations rely on tightly controlled architectures and continuous monitoring."

VIVEK SRIVASTAVA
Country Manager, Fortinet India

Routine security activities, such as software updates, require carefully controlled procedures involving physical supervision, restricted vendor access, and airlock-style handling. Patch management in particular can become cumbersome and time-consuming. Removable media such as USB drives can become major threat vectors.

Srivastava emphasises that air-gapped systems are not automatically immune to threats. "Operationally, they introduce complexity, especially in patch management, monitoring, and controlled data exchange. Updates must often be performed manually, which can delay remediation if processes are not disciplined." Physical isolation also does not eliminate insider threats, supply-chain risks, or social engineering attacks.

Mishra illustrates the challenge with a simple scenario. When a zero-day vulnerability is discovered, threat actors can begin exploiting it within hours. However, deploying a patch in a physically air-gapped environment may take days or even weeks due to validation procedures, transfer controls, and staged deployment processes. This delay can give attackers a temporal advantage.

A LAYERED APPROACH TO MODERN SECURITY

Air-gapping, therefore, should not be treated as a stand-alone security strategy. Security researchers have demonstrated numerous ways to breach isolated systems, ranging from infected USB drives to acoustic side-channel attacks that transmit data through sound or heat.

Pankit Desai, CEO and Co-Founder of Sequretek, argues that relying solely on air-gapping is no longer sufficient. "Gone are the days when you could simply air-gap systems and consider them secure. Security today must be more sophisticated than just cutting a cable. Physical isolation is not a magic shield." The well-known Stuxnet attack, which infiltrated Iranian nuclear facilities through infected USB drives, illustrates how determined adversaries can bypass isolation mechanisms.

The human factor remains another major vulnerability. With the rise of generative AI, phishing campaigns have become more convincing and scalable. According to Mishra, the increase in AI-assisted phishing attacks highlights a critical reality: the human layer remains one of the most exploitable components of any security architecture.

For most enterprises, therefore, the objective should not be disconnection but secure connectivity. IoT systems are designed to collect, transmit, and analyse data across distributed environments, making full physical isolation impractical.

Srivastava recommends focusing instead on strong network segmentation, Zero Trust access controls, continuous monitoring, threat intelligence, and unified visibility across IT, operational technology, and IoT environments. Platform-based architectures that integrate networking and security can help organisations protect distributed deployments without sacrificing performance.

Vembu also emphasises that air-gapping should be applied selectively. It works best as one layer within a broader security architecture. For sectors such as energy, defence, or certain healthcare systems where compromise could have national or safety implications, some degree of air-gapping may be justified. However, for most enterprise environments, disciplined patching, strict access controls, strong segmentation, and continuous monitoring often provide more practical and scalable protection.

Ultimately, security is about reducing risk rather than chasing absolute isolation. If only air-gaps were as effortless as an invisible cloak rather than as cumbersome as walking through a crowded mall in a PPE suit.

pratimah@cybermedia.co.in

Free-space optics open a new path for networks

Taara Beam promises fibre-like speeds without trenching cables, enabling operators to bridge urban connectivity gaps and extend network capacity.

BY PRABU RAM

As demand for high-capacity connectivity accelerates, network operators and enterprises are exploring alternatives beyond traditional fibre and radio-based wireless technologies. One emerging approach gaining attention is free-space optical communication, which uses beams of light to transmit data through the air at fibre-like speeds.

At Mobile World Congress 2026 in Barcelona, Taara unveiled an optical wireless platform—Taara Beam—designed to deliver high-speed connectivity across urban environments without trenching fibre or acquiring additional spectrum. The launch marks a milestone for the company, which spun out of X, Alphabet's innovation lab.

While Taara initially focused on bridging connectivity gaps in remote regions, its latest platform targets a different challenge: extending high-capacity networks within cities where fibre infrastructure exists but remains difficult to access. By transmitting data using tightly focused infrared light beams, Taara's technology aims to create a new middle layer of network infrastructure that complements fibre, wireless and satellite connectivity.

THE PERSISTENT CHALLENGE OF LAST-MILE FIBRE

Despite massive global investment in fibre networks, access remains uneven. Even in urban areas with extensive fibre infrastructure, physical and regulatory barriers often prevent connectivity from reaching specific buildings, campuses or network hubs.

Installing fibre often requires excavation, right-of-way approvals and complex construction processes that can take months to complete. In dense urban environments, these hurdles can significantly delay network expansion.

Taara's approach bypasses the need for physical cables. Instead of transmitting data through buried fibre, Taara

> The technology uses beams of light to create a middle layer of network infrastructure that complements fibre, wireless and satellite connectivity.

systems send information through the air using invisible near-infrared light. The technology creates highly focused optical links between two terminals, enabling high-capacity connections over several kilometres without new infrastructure. This allows operators to deploy links in hours rather than months.

A notable example involves Google connecting facilities located a few hundred metres apart near a submarine cable landing point in California. Although fibre existed nearby, land access restrictions prevented conventional deployment. A Taara optical link enabled the connection without trenching through restricted areas.

TAARA BEAM FOR URBAN CONNECTIVITY

Taara Beam reflects the company's shift towards dense urban deployments and enterprise networking applications.

Roughly the size of a shoebox and weighing about eight kilograms, the device can be mounted on rooftops, streetlight poles or building façades. Two Beam terminals establish a line-of-sight optical link capable of transmitting data at speeds of up to 25 gigabits per second across distances of up to 10 kilometres. Latency is approximately 50 microseconds, delivering near-fibre performance and significantly lower delay than satellite-based connectivity platforms.

For telecom operators, the key advantage lies in deployment speed. Fibre connections often require lengthy regulatory approvals and extensive civil engineering, whereas Taara links can be installed in a matter of hours. As a result, the platform is positioned primarily as a middle-mile connectivity solution, bridging gaps between fibre networks, data centres, cellular infrastructure and enterprise facilities.

OPTICAL PHASED ARRAYS BEHIND THE SYSTEM

A major innovation in Taara Beam lies in how it steers and maintains its laser connection. While traditional free-space optical systems rely on mechanical mirrors and motors to align laser beams between endpoints, Taara Beam replaces these moving parts with a semiconductor-based optical phased array that electronically controls the direction of light.

Inside the device is a photonics chip containing more than 1,000 microscopic light emitters. By controlling tiny timing delays between these emitters, the system shapes and directs the outgoing beam towards the receiving terminal.

By integrating this capability onto a photonics chip roughly the size of a fingernail, Taara has reduced the size and power requirements of optical networking hardware while improving reliability compared with mechanical systems.

Taara's earlier optical networking platform, Lightbridge, has already addressed one of the key operational challenges of optical communication: weather interference. Lightbridge Pro mitigates weather disruptions by switching traffic to a radio-frequency backup link, enabling up to 99.999% availability.

EXPANDING TELECOM AND ENTERPRISE USE

Taara is positioning its technology primarily for enterprise and telecom infrastructure applications rather than direct consumer connectivity. One key opportunity lies in interconnecting data centres, particularly as artificial intelligence workloads drive exponential growth in data traffic. Free-space optical links could provide high-bandwidth, low-latency connections between facilities without waiting for new fibre deployment.

Another potential use case involves 5G and future 6G backhaul, where optical wireless links could provide rapid connectivity between small-cell base stations and core infrastructure.

The broader potential of free-space optical communication remains significant. Laboratory demonstrations have already achieved terabit-per-second transmission rates, suggesting that the technology's capacity could rival conventional fibre links.

By turning beams of light into high-speed network links, Taara is attempting to bridge the persistent gap between where fibre exists and where high-capacity connectivity is needed. If the technology scales successfully, optical wireless networking could become an important complement to fibre, wireless and satellite infrastructure in the next generation of global connectivity.

feedbackvnd@cybermedia.co.in

India's data centres face the AI infrastructure shift

Data centres in India are entering an AI era where power supply, cooling efficiency, and sustainability are redefining how digital infrastructure is designed and scaled.

BY SHRIKANTH G

India's data centre industry has entered a decisive phase. What was once a conversation dominated by space, uptime, and connectivity has shifted sharply towards power density, cooling efficiency, and sustainability at scale. The rise of artificial intelligence (AI) workloads, particularly graphics processing unit or GPU-intensive training and inference models, has fundamentally altered how data centres are designed, built, and operated.

Enterprises, cloud providers, and governments are no longer planning for incremental growth. Instead, they are preparing for step-change demand driven by AI platforms, sovereign cloud initiatives, and the expansion

> AI is transforming India's data centres into engineered infrastructure systems where power planning, cooling architecture, and grid readiness determine scalability.

Capacity planning for AI infrastructure is becoming power led, where grid readiness, captive power, energy storage, and cooling efficiency shape scalability.

AMIT AGRAWAL
President, Techno Digital

of global capability centres. This shift is pushing infrastructure beyond traditional enterprise norms and exposing structural constraints that were previously manageable, most notably around power availability, grid readiness, and water usage.

Across India, new facilities are being conceived as AI-ready by default. This means planning for rack densities far above historical norms, designing cooling systems that can handle sustained thermal loads, and securing long-term power through a mix of grid supply, renewables, captive generation, and storage. The data centre is no longer a passive container for IT; it has become an active, engineered system that must balance performance, resilience, and environmental impact simultaneously.

Industry observers say this transformation mirrors developments seen globally. Vineet Mittal, Senior Vice President at Ziroh Labs, said India is witnessing the emergence of multiple new data centre models, including AI-dedicated facilities, energy-efficient campuses, and infrastructure supporting global capability centres. He said the trend is being driven by two forces: growing enterprise AI adoption and power shortages in developed markets that are pushing infrastructure investments towards emerging regions such as India.

POWER CONSTRAINTS REDEFINE DATA CENTRE DESIGN

Power has emerged as the defining bottleneck for the next phase of data centre growth. Large AI-focused facilities can require more than 100 MW, pushing both grid infrastructure and commercial viability to their limits. In many regions, power availability, not land or connectivity, is now the gating factor for expansion.

Mittal said the scale of demand is comparable to the energy consumption of a mid-sized town. Without reliable power at a viable cost, long-term profitability becomes difficult. He also pointed out that cooling systems can significantly increase operational expenditure, while water consumption associated with conventional air conditioning systems adds further environmental pressure.

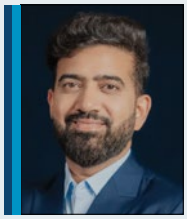
This reality is driving a shift towards power-led planning. Operators are investing in long-term power purchase agreements, captive renewable assets, energy storage, and behind-the-metre solutions to reduce dependence on constrained grids. In parallel, grid congestion in developed markets is prompting global cloud providers to look towards countries like India, where demand growth aligns with infrastructure build-out.

Amit Agrawal, President at Techno Digital, said the constraint shaping most investment decisions today is power and cooling rather than land availability. As AI workloads increase, including those associated with national initiatives such as the IndiaAI Mission, capacity planning is becoming power-led.

"Grid readiness, power purchase agreement (PPA) or captive power arrangements, energy storage, and cooling efficiency now have a direct bearing on uptime, scalability, and long-term cost structures," Agrawal said.

AI infrastructure success will depend not on GPU capacity alone but on sustained utilisation across power, cooling, networking, and viable service models.

AS RAJGOPAL
CEO & Managing Director, NxtGen Cloud Technologies



Cooling architectures are shifting towards liquid and hybrid systems as AI workloads generate sustained thermal loads that conventional air-cooling struggles to manage.

NARENDRA SEN
Founder & CEO, RackBank & NeevCloud

However, securing power is only part of the equation. The cost, reliability, and sustainability of that power directly influence uptime, scalability, and long-term economics. As AI workloads reduce tolerance for instability, data centres must be engineered to deliver predictable performance even as power systems become more complex and distributed.

COOLING SYSTEMS BECOME CORE INFRASTRUCTURE

As rack densities rise, cooling has shifted from an operational concern to a strategic capability. Traditional air-based cooling struggles to cope with sustained AI workloads, accelerating adoption of liquid-assisted and hybrid cooling architectures. These systems promise higher efficiency, but they also introduce new operational challenges around maintenance, monitoring, and lifecycle management.

Narendra Sen, Founder and Chief Executive Officer of RackBank and NeevCloud, said cooling technologies are evolving rapidly to support AI-driven workloads. According to him, the industry is increasingly moving towards liquid-based or hybrid cooling systems that can deliver significantly higher efficiencies compared with conventional air-based designs.

Making liquid cooling mainstream is less about hardware readiness and more about operational maturity. Data centre teams must manage coolant quality, detect leaks early, and coordinate tightly between IT, power, and thermal systems. Retrofitting legacy facilities adds further complexity, requiring modular designs that allow gradual transition without disrupting live operations.

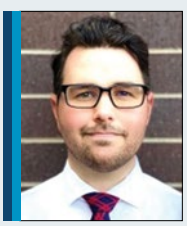
The most resilient operators are adopting hybrid approaches, retaining air cooling for standard workloads while deploying liquid solutions selectively where density demands it. This flexibility reduces risk, protects capital, and ensures facilities can evolve as AI adoption patterns mature.

SUSTAINABILITY SHIFTS FROM INTENT TO ENGINEERING

Sustainability is no longer an aspirational add-on. It is becoming a core design principle. Metrics such as power usage effectiveness, water usage effectiveness (WUE), and carbon intensity are now being considered at the earliest stages of planning. Closed-loop water systems, renewable-heavy power mixes, and energy-efficient cooling are increasingly standard rather than exceptional.

Sen said many operators are adopting closed-loop water systems and watershed recycling models, particularly in water-stressed regions, to reduce environmental impact.

Agrawal said sustainability metrics are increasingly embedded into the engineering design of facilities rather than being treated as operational targets. He



AI workloads are driving specialised data centre designs that require far more power and space, increasing costs and leaving little tolerance for instability.

DOUGLAS DONNELLAN
Research Analyst, Uptime Institute

Large AI data centres can demand over 100 MW of power, comparable to a small town, making reliable energy supply the most critical constraint for growth.

VINEET MITTAL
Senior Vice President, Ziroh Labs

cited Techno Digital's Chennai facility, which integrates UPS-backed critical loads, water-cooled chillers with adiabatic cooling towers, renewable energy integration, and a power usage effectiveness or PUE of 1.35. "These choices are driven by reliability and efficiency rather than density alone," he said.

At the same time, there is growing scrutiny of whether sustainability commitments translate into real-world outcomes. Mittal said that as AI increases baseline energy consumption, the industry must demonstrate measurable energy savings rather than relying solely on sustainability claims.

Mittal added that new architectural approaches could also improve efficiency. Ziroh Labs has been working on AI frameworks that allow models to run on central processing units or CPUs with lower energy consumption, potentially reducing power usage to about one-third of GPU-based deployments without sacrificing performance.

MITIGATING THE RISKS OF AI INFRASTRUCTURE HYPE

While AI is clearly influencing investment decisions, industry leaders are increasingly cautious about overbuilding rigid, narrowly optimised infrastructure. The risk is not AI adoption slowing, but assets becoming stranded if they cannot support a broader mix of workloads.

Douglas Donnellan, Research Analyst at Uptime Institute, said AI workloads are driving greater specialisation in data centre design because their infrastructure requirements differ significantly from traditional enterprise workloads. "This has increased demand for power and space, raised costs, and reduced tolerance for instability," he pointed out.

He further added that concerns about an "AI bubble" primarily relate to facilities designed exclusively for high-density AI workloads. If demand shifts, those assets could face utilisation challenges. Facilities designed with flexibility to support multiple workloads are more resilient, Donnellan stated.

A S Rajgopal, Chief Executive Officer and Managing Director at NxtGen Cloud Technologies, said the risk of idle infrastructure arises when GPU capacity is built speculatively without visibility into long-term workloads.

"Simply adding GPU capacity does not create value on its own," Rajgopal said, adding, "For that capacity to be meaningfully productive, the entire stack must be engineered for sustained utilisation including power density, cooling, networking, storage throughput, platform maturity, and commercially viable service models."

According to him, operators are increasingly adopting portfolio-based strategies that combine AI-optimised infrastructure with traditional enterprise environments that provide stable, long-term revenue streams. In this context, the biggest challenge ahead is not any single risk but managing systemic interdependencies across power, cooling, regulation, geopolitics, and security.

Donnellan said the industry must increasingly focus on managing systemic risk rather than isolated incidents. "Outages, energy constraints, geopolitical shifts, and data sovereignty concerns are becoming interconnected challenges, especially as AI workloads increase baseline power demand and reduce tolerance for disruption."

As India accelerates its digital infrastructure investments, the data centre is emerging as a critical foundation of the country's digital economy. Its future will depend not only on scale but also on how effectively the industry balances power, sustainability, resilience, and flexibility in an AI-driven world.

shrikanthg@cybermedia.co.in.
(With inputs from Pratima Harigunani)

ASHOK SHIVASHANKAR
Managing Director – Partner Organisation,
Cisco India & South Asia

"Customers today are buying outcomes, not products"

Enterprise technology conversations have changed dramatically over the past decade. Organisations that once focused on procuring routers, switches and connectivity infrastructure are now asking a different set of questions: how to secure AI workloads, extract value from software platforms and deliver measurable digital outcomes.

***Ashok Shivashankar**, Managing Director – Partner Organisation, Cisco India & South Asia, in this interaction with **Shubhendu Parth,** explains why this shift has compelled Cisco to redesign its global partner ecosystem through the Cisco 360 Partner Programme. He discusses the transition from resale-driven models to outcome-led engagements, the growing role of AI across Cisco's portfolio, and how new partner designations and incentives are reshaping capabilities, customer engagement and profitability across India and South Asia. Excerpts:*

Tim Coogan, Cisco's Senior Vice President – Global Partner Sales, recently wrote that 26 years ago, customer conversations were about routers and uptime. In contrast, today, CIOs are asking how to secure AI workloads and prove ROI on generative AI. From your perspective in South Asia, how real is this shift—and why did it require a reset like the Cisco 360 Partner Programme?

If you look at the broader evolution of the market, we have seen that shift quite clearly in South Asia, and more specifically in India. If you go back 20 years, the partnership ecosystem was largely resale-centric. Customers typically had a very clearly defined requirement. They would say, "I need connectivity," and the conversation would revolve around the product, its features, specifications, and price. Once that product was procured, the transaction was essentially complete.

Today, the environment is completely different. Customers are no longer looking to buy a product, or even a standalone service or software solution. They are looking to buy outcomes. When customer behaviour changes so fundamentally, partner programmes also have to evolve. Cisco's earlier partner programmes were actually industry-leading. However, those programmes were designed primarily for a world where the partner's role centred on reselling products.

In the current environment, where customers expect integrated outcomes, we realised there was a need to simplify the programmes and ensure partners build

> Hyper-specialised partners are becoming critical as enterprises deploy AI-ready digital infrastructure that integrates networking, security and software platforms.

> Digital infrastructure conversations have shifted from hardware procurement to measurable outcomes, where partners must ensure software adoption and lifecycle value.

capabilities in adoption, lifecycle management, and customer experience.

With IT markets projected to grow strongly and infrastructure spending accelerating, customers are no longer debating whether to invest in AI but how quickly and with whom. How does the Cisco 360 Partner Programme respond to this urgency differently from earlier partner models?

There are two important aspects to this. First, if you look at Cisco's portfolio, AI is not confined only to the cloud or compute layers. Many people tend to associate AI primarily with infrastructure for training and inference, but in our case, AI cuts across the entire portfolio. Similarly, AI capabilities are integrated across networking, security, collaboration and cloud technologies. From a portfolio perspective, AI is pervasive across everything we do.

The second aspect is the partner experience. Within the Cisco 360 framework, we have introduced the Partner Experience Platform (PXP). AI is embedded into this platform as well. It helps partners navigate the programme more efficiently, understand their incentives, track their progress and make faster decisions.

Cisco has described the new model as a shift from transactions to outcomes. What were the limitations of the earlier incentive structures, and how does focusing on total contract value, software adoption and lifecycle engagement change partner behaviour?

It is not really that something in the earlier programme was not working. However, the programme was no longer perfectly aligned with what customers expected, what partners needed, and how Cisco itself was evolving.

Over time, the programme had become complex. There were separate elements for products, services, adoption and customer experience. Also, customer buying behaviour was changing. Customers were no longer purchasing products such as compute, networking or security separately. Rather, they were increasingly purchasing integrated solutions. The Cisco 360 Partner Programme brings these elements together into a single structure, simplifying the overall experience for partners.

Another important aspect is capability specialisation. Earlier, a Gold partner might have had strong expertise in one area, such as networking, but lacked deep capability across other architectures, such as collaboration or security.

The new programme recognises partners based on their expertise in specific portfolios. Partners are now designated as portfolio partners or preferred partners for particular architectures. This allows customers to clearly identify which partners have deep specialisation in specific technology areas.

Besides, Cisco itself has been transitioning from a hardware-centric company to a software-centric organisation over the past decade. In that environment, adoption becomes critical. Delivering an outcome is not just about selling the technology, but about ensuring it is deployed, adopted, and delivering value.

In a software-driven environment, the focus shifts to ensuring that customers are actively using the capabilities they purchased and achieving the outcomes they expected. That means partners must focus much more on deployment, adoption, lifecycle management and customer experience.

The new Cisco Partner Incentive promises predictable earnings from the first dollar. In a price-sensitive market like India, how important is this shift for partner confidence and long-term investment in AI capabilities?

One of the key principles behind the programme was protecting existing partner investments. Many of our long-standing partners had already built strong technical capabilities. Those capabilities transition into the new programme. Partners were not expected to start from scratch.

> AI is no longer confined to data centres; it now runs across networking, security and collaboration platforms, reshaping how digital infrastructure is deployed.

Another important element is predictability. At the beginning of every cycle, partners know exactly what returns they can expect from their investments. The incentives apply across multiple dimensions—services, architecture portfolios and lifecycle incentives related to adoption and customer experience.

We have also introduced clear measurement mechanisms based on telemetry data. This transparency gives partners the confidence to make long-term investments in new capabilities. They know what milestones they need to achieve and what the financial returns will be.

Cisco has introduced new partner designations along with tools such as the partner locator and the partner value index. How will customers experience this change, and how does Cisco ensure genuine expertise stands out?

A key concept here is hyper-specialisation. For each portfolio, we have defined a value index that measures partner capability on a scale of one to ten. The score reflects several factors, including technical certifications, sales expertise, market performance and adoption of enterprise buying programmes.

When a partner reaches a score of five out of ten in a portfolio, they qualify as a Cisco portfolio partner for that architecture. When they reach a score of 7.5 or higher, they become a preferred partner for that portfolio, representing the highest level of specialisation. This helps customers clearly identify which partners have the strongest expertise in specific architectures such as networking, security or cloud.

At the same time, the model allows partners to collaborate. If a customer requires a secure networking solution, one partner might lead the engagement while working with another partner that has specialised security capabilities. This creates an ecosystem approach in which partners collaborate to deliver the best possible outcome for the customer.

Cisco spent more than 15 months co-designing the programme with partners. What were the toughest debates during that process?

One of the biggest challenges for any global company is balancing standardisation with local market realities. Initially, we had designed a highly standardised programme that could work worldwide. However, partners in Asia-Pacific—and particularly in India—provided feedback that certain aspects needed localisation.

This is what we call "T-shirt sizing". The expectations for a partner generating USD 50 million in networking revenue cannot be the same as those for a USD 2-million partner. Based on partner feedback, we introduced tiers that adjust expectations based on partner size and scale.

Similarly, public sector procurement processes in the Asia-Pacific differ significantly from corporate purchasing models. Partners highlighted that enterprise agreement models may not always apply in these environments. We incorporated those insights into the final design.

Looking ahead to 2026–27, what indicators will tell you that Cisco 360 is working in South Asia? What are the key metrics?

There are several metrics we monitor. The first is partner capability capacity. We want to ensure that we have the right number of capable partners across each technology portfolio in India and across South Asia. The second metric is partner profitability. One of our key commitments is that partners should earn at least as much as they did under the earlier programme, and ideally more.

Finally, we will track how effectively partners build capabilities in emerging areas such as AI infrastructure, next-generation networking and secure networking. If we see strong partner capacity and specialisation in these areas, it will indicate that the programme is delivering the intended outcomes.

shubhendup@cybermedia.co.in

Networks find their next foothold at the edge

As edge computing shifts workloads from centralised data centres, it creates new infrastructure demands, telco opportunities and strategic choices for enterprise IT.

BY PRATIMA HARIGUNANI

When Alex Honnold placed his first lithe foot on Taipei 101—without any harness or safety net—many onlookers watching from the street, and from couches far away, must have gasped and asked why. Those looking through boardroom windows may have said another why somewhere. Why climb along the edges of a 1,600-foot skyscraper? Would the centre not be easier to scale? Is there something about the ledges and corners that offers a better foothold or a longer-lasting strategy?

Some of the telcos, data centre operators and cloud movers-and-shakers may know the answer. Something must explain the shift unfolding across the industry towards the edge, especially as companies search for the next path forward while climbing the rough but inviting rocks of AI inference, 6G, fibre, IoT and low-latency digital services.

WHY EDGE COMPUTING FINDS A FIRM GRIP

Manoj Paul, Managing Director of Equinix India, explains the drivers behind the shift. Edge computing is accelerating because modern AI workloads and real-time digital experiences demand processing closer to where data is generated.

"Low latency, bandwidth reduction and data sovereignty requirements are now the primary triggers for shifting workloads from centralised clouds to distributed edge locations. At the same time, AI has become inherently distributed: training may remain centralised, but inference increasingly needs to occur at the edge for applications such as computer vision, fraud detection, retail analytics and industrial automation."

Biswajeet Mahapatra, Principal Analyst at Forrester, echoes this view. Edge computing moves compute and analytics closer to where data is produced, reducing latency, lowering bandwidth consumption and dependence on distant cloud regions.

"The edge is driven by application locality, IoT proliferation, AI inference needs and data sovereignty," he says adding that these factors make distributed processing

"AI workloads are inherently distributed. Training may remain centralised, but inference must move closer to users and devices for real-time applications."

MANOJ PAUL
Managing Director, Equinix India

more efficient than routing everything to large core sites. The shift is visible in manufacturing, retail, healthcare and smart city deployments where real-time decision-making requires sub-10 millisecond responsiveness.

Historically, data centres followed fibre landing stations—Mumbai and Chennai served as the default hubs, reflects Narendra Sen, Founder and CEO of RackBank and NeevCloud. That pattern is now changing.

"We are seeing a shift from 'carrier-neutral' to 'power-neutral' and 'carbon-neutral' facilities," Sen explains. "Secondly, density is being redefined. A few years ago, 8–10 kW per rack was considered high density. Today, with NVIDIA's H100 and upcoming Blackwell architectures, facilities are being engineered for 100–150 kW per rack. This is not an upgrade; it is a structural rethink of data centre physics, from floor loading to cooling loops."

Ranganath Sadasiva, CTO, HPE India, notes that edge computing is likely to dominate the next phase of enterprise growth because organisations increasingly need to process data where it is generated rather than relying entirely on centralised infrastructure.

"This decentralised approach enables organisations to convert data into actionable insights with lower latency, higher efficiency and improved reliability. By deploying AI-ready compute optimised for edge environments, businesses can enable real-time decision-making across sectors including manufacturing, healthcare, transportation and retail."

Yet there are nuances to the shift. AS Rajgopal, CEO and MD of NxtGen Cloud Technologies, argues that workloads are not migrating entirely from data centres to the edge.

"Instead, certain components of an application execute at the edge to reduce latency for end users and improve the efficiency of centralised applications running in core data centres. For example, biometric authentication in a banking application can occur at the device or edge, reducing response time while easing the load on the central data centre."

INFRASTRUCTURE SHIFTS FOR CLOUDS AND TELCOS

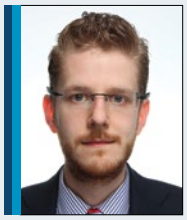
The movement toward the edge is reshaping the underlying infrastructure. Paul notes that high-density AI computing is driving demand for purpose-built data centres with liquid cooling and higher power delivery.

"At the networking layer, interconnection becomes essential. For telecom operators, the core-to-edge migration is especially transformative. With 5G MEC and emerging AI-RAN architectures, telcos are merging connectivity and compute so that RAN functions and enterprise AI inference can run on the same accelerated infrastructure at the network edge."

Enterprise IT strategies are also shifting from monolithic cloud architectures to distributed AI models spanning centralised training clusters, regional aggregation sites and local inference edges. Many

"Processing data where it is created allows organisations to generate actionable insights faster and enables real-time decisions across industries."

RANGANATH SADASIVA
CTO, HPE India



"Distributed edge architectures improve responsiveness but replicate data across many nodes, which may reduce efficiency compared with centralised systems."

ALEX DE VRIES-GAO
Founder, Digiconomist

enterprises are prioritising multicloud adjacency, private data pathways and sovereignty-aligned architectures as regulatory demands grow.

Sen observes that smaller distributed edge data centres are increasingly appearing in metro-adjacent locations as well as tier-2 and tier-3 cities. "Edge compute and telecom networks, particularly 5G, are converging. There is also growing adoption of containerised workloads, orchestration platforms and AI at the edge, combined with stronger emphasis on security-by-design and remote infrastructure management."

This shift is already visible across sectors such as streaming, payments, smart city platforms, healthcare services, retail analytics and industrial monitoring, where proximity improves performance and resilience.

EDGE REVENUE STREAMS FOR TELECOM OPERATORS

Edge computing is also opening new revenue opportunities for telecommunications operators. According to Sen, the technology allows operators to monetise their 5G networks through enterprise services such as private networks, edge-hosted applications and ultra-low latency solutions.

"Telecommunications operators now have the opportunity to develop managed edge platforms for industries including manufacturing, logistics, healthcare and entertainment."

Paul adds that the shift enables operators to monetise their distributed infrastructure through edge-hosted AI services. "Telcos increasingly rely on neutral interconnection hubs to federate their MEC regions with cloud providers, SaaS platforms and enterprise ecosystems. This federation is essential for delivering consistent low-latency experiences."

Mahapatra notes that telecom operators are integrating MEC and private 5G with hyperscaler ecosystems to support latency-sensitive applications such as AI inference, video analytics and industrial automation. "For enterprises, IT strategies increasingly revolve around distributed workload placement, stronger IT-OT integration and AIOps-driven operations to maintain security and resilience across multiple sites."

EDGE CHALLENGES AND STRUCTURAL CONSTRAINTS

Edge computing also introduces new challenges. Alex de Vries-Gao from the VU Amsterdam Institute for Environmental Studies and Founder of Digiconomist cautions about redundancy in distributed architectures.

"Instead of sending everything to a single central cloud server, you rely on a distributed network of local servers where data and applications are replicated across multiple nodes. While this improves latency and reliability, it can also reduce efficiency because multiple copies are created rather than using a single central system."

"Edge computing is driven by application locality, IoT proliferation and AI inference needs, making distributed processing more efficient than core routing."

BISWAJEET MAHAPATRA
Principal Analyst, Forrester

Edge computing is forcing telcos and data centres to rethink where intelligence should reside as AI-driven applications demand faster processing closer to users.

TELECOM'S EDGE MOMENT

- **Networks become compute platforms**
  With Mobile Edge Computing (MEC) and emerging AI-RAN architectures, telecom operators are integrating compute capabilities within network infrastructure, allowing applications and AI inference to run closer to users.
- **5G infrastructure supports enterprise workloads**
  Edge deployments enable telecom operators to support latency-sensitive services such as industrial automation, video analytics, smart city platforms and real-time financial transactions.
- **New revenue models emerge**
  Operators can monetise their distributed network footprint through managed edge platforms, private 5G networks, and edge-hosted enterprise applications.
- **Connectivity and cloud ecosystems converge**
  Telecom networks are increasingly federated with cloud providers, SaaS platforms and enterprise ecosystems to deliver consistent low-latency services.
- **Infrastructure moves closer to demand centres**
  Edge sites located near aggregation points in telecom networks help reduce latency while supporting distributed AI and IoT deployments.

Capacity planning is also evolving. Sen notes that data centre development is shifting from linear expansion to modular and scalable models that align capital expenditure more closely with demand.

However, power availability has emerged as the most critical constraint. Operators are therefore exploring long-term power purchase agreements, captive renewable energy generation and hybrid grid-renewable strategies. Agrawal emphasises that edge deployments demand strong architectural discipline around security, remote operations, standardisation and power reliability.

Rajgopal reiterates that not all workloads belong at the edge. Latency-sensitive transactions such as authentication may run locally, while data-intensive processing and core applications continue to reside in centralised data centres.

Despite these complexities, edge computing will not replace centralised facilities. Instead, both architectures will coexist within distributed digital infrastructure.

"The core-to-edge transition is more than a passing trend," Sen concludes. "It represents a fundamental shift in how digital infrastructure will be designed, built and utilised."

De Vries-Gao highlights another dimension: energy consumption. "Cloud computing stabilised data centre electricity use over the past decade, but edge deployments may reverse this trend by increasing the number of facilities."

Tough questions for campus infrastructure planning indeed. Edge computing brings opportunity and constraint in equal measure. Guess what did Honnold reportedly say when he finally reached the top of that dangerously high building? "It is windy here."

pratimah@cybermedia.co.in

[INTERVIEW]
GEOPOLITICS

"Geopolitics may encourage domestic technology development"

ANDREW KITSON
Director – Technology, BMI

The US and Israel launched a large-scale military campaign against Iran on 28 February, targeting the regime's leadership as well as military and security infrastructure. Beyond geopolitical ramifications, the conflict raises important questions about digital infrastructure resilience—from internet shutdowns and submarine cables to data centre risks and cybersecurity exposure.

BMI, a unit of Fitch Solutions, has analysed the potential ripple effects across global connectivity systems. ***Andrew Kitson,*** *Director, Technology at BMI, discusses possible scenarios with* ***Pratima Harigunani.*** *Excerpts:*

What is your overall outlook on this recent war with Iran?

The scale of the attacks aligns with our Country Risks team's view of a conflict that could last several weeks if diplomacy fails. With the Tehran regime considering the attacks an existential threat, its response has targeted Israel and US military bases in the UAE, Saudi Arabia, Bahrain, Qatar and Kuwait. Civilian assets in Bahrain, Kuwait, the UAE and Oman have also been affected at the time of writing.

Iranian forces have issued threats against ships passing through the Strait of Hormuz. More recently, the Lebanon-based paramilitary group Hezbollah has attacked Israel, prompting a limited response and increasing concerns that the conflict could spread across the wider Middle East.

What about lights-out scenarios on the internet?

Monitoring systems such as Cloudflare Radar showed a near-complete cessation of internet traffic from early on 28 February, with subsequent sporadic spikes. These are believed to represent communications between government and military elites using rare "white-pass" mobile data SIM cards or laptops.

We believe the state has developed a shadow internet infrastructure accessible only to a small number of highly trusted individuals. This network is unlikely to have been affected by cyberattacks conducted over public internet infrastructure.

As a result, the Iranian government, its military and the Islamic Revolutionary Guard Corps likely retain extensive ability to communicate through digital channels. The cyber disruptions appear to have primarily affected civilian communications rather than government systems.

What is possible next in terms of digital attacks?

Potential targets could include data centres, satellite earth stations, submarine and terrestrial cable systems and communications towers. Such attacks could take both physical and digital forms. Weaponised drones may be deployed against key facilities, while cyberattacks could target data centres or network infrastructure. Ecosystem-adjacent assets such as power grids could also be targeted.

As of 2 March, only one UAE-based data centre—a facility in Dubai operated by Amazon Web Services—had been hit by Iranian-launched ordnance, causing a large fire that put the facility temporarily out of service. However, the strike may have been accidental rather than deliberate, as no other regional data centres have been hit, and the Dubai facility was not critical to the functioning of internet services in the UAE.

If Iran or its allies were to target connectivity infrastructure more directly, submarine cables in the Persian Gulf would likely become primary targets. The Strait of Hormuz is particularly vulnerable because its narrow geography means multiple submarine cables run close to one another. A single attack could cause significant disruption that might not be repairable until after the conflict ends.

However, such an action would also isolate Iran from the wider region and limit its ability to monitor adversaries. For this reason, such a scenario would likely only occur if the conflict escalates significantly.

What does this development tell CXOs and CIOs about the fragility of digital infrastructure?

Most CTOs and CIOs are already aware of the fragility of digital infrastructure due to the highly interconnected ecosystems in which networks operate. However, a degree of complacency often persists, particularly in politically stable markets, where a mindset holds that such disruptions cannot occur locally.

Disruptions to submarine cables during the Red Sea crisis and the destruction of digital infrastructure in Ukraine illustrate how vulnerable sovereign networks can be. These incidents underline the importance of asset diversity and route redundancy in an increasingly volatile geopolitical environment.

There are also emerging geopolitical implications for technology supply chains. For instance, the Trump administration is reportedly exploring measures to control Nvidia's international GPU sales to markets considered unfriendly. Such policies could potentially extend even to allied nations depending on their geopolitical alignments.

How would this conflict affect data centre planning and investment?

All economies are striving to leverage disruptive technologies such as artificial intelligence to remain competitive with neighbours, trading partners and even adversaries. Consequently, digital infrastructure—including data centres, satellite ground stations, submarine cables and communications towers—will continue to be deployed even in regions exposed to geopolitical risks.

Risk-averse investors may reduce exposure to volatile regions, while others may see strategic opportunities in markets where competition is declining. However, such investments are likely to attract higher insurance premiums. Insurance costs across the digital infrastructure sector are already rising due to increased cybersecurity threats, climate risks and geopolitical tensions. Many investors may therefore accept higher risk levels as a structural reality of the current environment.

Would connectivity shift towards satellite or decentralised networks?

Submarine cables remain the most cost-effective means of transmitting large volumes of data globally. Satellite networks face bandwidth limitations. Even with ambitious projects such as Starlink, individual satellites can support only a limited number of communication channels. In contrast, satellite-to-phone links currently support basic voice and messaging rather than full broadband services.

As a result, terrestrial alternatives and new cable routes that bypass conflict zones are likely to become more important in regions such as the Middle East. Edge and IoT networks can offer limited local alternatives if international connectivity is disrupted, but they cannot replace global cable infrastructure.

What should CIOs in India worry about?

BMI does not make direct recommendations, but it would be prudent for CIOs in India to prioritise robust cybersecurity and data protection frameworks. This includes ensuring that employees at all organisational levels are trained in fundamental data security practices.

Organisations should also avoid excessive reliance on purely sovereign digital ecosystems. While geopolitical dynamics may encourage local technology development, relying entirely on a single national ecosystem risks reduced interoperability, rapid obsolescence and limited fallback options if systems become compromised.

A balanced strategy combining sovereign infrastructure with diversified global platforms is likely to offer greater resilience.

Click here to read the complete version of the interview.

pratimah@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.

[USE CASE]
NETWORK INTELLIGENCE

BFSI security moves to AI-driven video infrastructure

AI-enabled video platforms are emerging as critical digital infrastructure for banks, strengthening security, compliance, analytics and operational oversight.

BY NARESH B WADHWA

India's banking and financial ecosystem is undergoing one of the most significant transformations in its history. With millions of daily transactions, a rapidly expanding network of branches and ATMs, and increasingly demanding consumers, financial institutions operate in a landscape that is far more dynamic and vulnerable than ever before. Security threats have evolved, operational complexity has multiplied, and customer expectations have shifted from basic service to seamless, frictionless experiences.

> Intelligent video platforms turn cameras into data sensors that generate real-time insights across ATMs, vaults and branches, strengthening security and operations.

Edge processing allows cameras to analyse events locally while central systems correlate alerts across distributed banking networks and security operations centres.

IN BRIEF

- Traditional bank surveillance recorded events but offered little intelligence, leaving institutions exposed to evolving fraud and security threats.
- AI-powered video platforms analyse behaviour, detect anomalies and trigger alerts across ATMs, vaults and branches.
- Banks are adopting phased deployments, starting with high-risk assets before expanding analytics across wider branch networks.
- Distributed architectures combine edge processing for rapid detection with central platforms for search, correlation and reporting.
- RBI mandates such as 180-day video retention and camera placement rules are accelerating the adoption of intelligent platforms.
- Video analytics now support branch operations too, helping banks analyse customer behaviour, manage queues and optimise layouts.

For decades, bank surveillance systems largely functioned as passive recorders. They provided footage, but rarely intelligence. In an environment marked by sophisticated fraud attempts, rising physical security risks, and regulatory compliance requirements, this approach is no longer adequate. What the sector requires today is intelligent video infrastructure capable of anticipating risks, supporting rapid decision-making, and offering insights that enhance operations as much as security.

FROM PASSIVE CAMERAS TO AI PLATFORMS

Modern video intelligence platforms can analyse live footage, interpret behavioural patterns, detect anomalies, and raise alerts before situations escalate, shifting from reactive to predictive capability. Institutions deploying these systems report rapid incident detection for high-priority scenarios such as ATM tampering or vault breaches, with significantly faster response times when integrated with automated workflows. This acceleration is critical: faster response times reduce loss severity, increase the likelihood of apprehending suspects, and minimise customer impact.

For institutions transitioning from legacy systems, a phased deployment strategy minimises disruption while delivering measurable value at each stage. The most effective approach begins with high-risk assets, ATMs and vaults, where security vulnerabilities are most acute, and ROI is clearest. Use cases such as loitering detection, tampering alerts, and vault access violations demonstrate immediate impact.

The second phase expands to branch networks, incorporating customer behaviour analytics, queue management, and compliance verification. Finally, institutions scale regionally, integrating mobile assets like cash vans while building centralised intelligence platforms. Critically, modern platforms overlay onto existing video management systems via standard protocols such as RTSP and ONVIF, avoiding costly infrastructure replacement.

EDGE INTELLIGENCE MEETS CENTRAL COMMAND

The architecture of these systems is equally important.

> Attribute-based forensic search helps investigators quickly trace incidents using filters such as clothing colour, vehicle type, and movement direction.

The most effective deployments employ distributed intelligence: edge processing within cameras or on-premises appliances handles latency-sensitive tasks like intrusion detection and facial recognition, dramatically reducing bandwidth consumption.

Centralised platforms enable advanced correlation, forensic search, and enterprise-wide reporting, connecting data from thousands of endpoints. Integration with existing VMS, access control, and SIEM platforms through open APIs ensures seamless workflows—when a vault breach is detected, the system simultaneously triggers SOC notifications, automated access lockdowns, and SIEM entries for correlation with other security events.

COMPLIANCE MANDATES RESHAPE SECURITY

Compliance has become a major driver of adoption. As regulations expand to cover transparency and secure data management, including RBI mandates for 180-day video retention and camera placement at entry, exit, and vault locations, financial institutions must maintain clear, searchable trails of evidence.

AI-driven platforms streamline compliance by providing automated incident logs, centralised monitoring, and advanced search capabilities. What once took hours now completes in minutes, with far greater accuracy. Institutions report reducing audit preparation time from weeks to days.

Fraud investigation has been similarly transformed. Instead of manually reviewing hours of footage, investigators now use attribute-based searches, clothing colour, vehicle type, and movement direction to quickly trace incidents and close cases faster. These capabilities not only strengthen incident response but also create powerful deterrents against future crime.

Beyond security, these systems deliver operational insights that improve branch performance. AI analytics help banks understand customer behaviour, reduce wait times, and optimise layouts, with deployments showing measurable reductions in average wait times, creating data-driven insights comparable to those used in digital channels.

BUILDING INTEROPERABLE VIDEO ECOSYSTEMS

When evaluating platforms, decision-makers should prioritise several critical factors: interoperability through open APIs and ONVIF compliance to avoid vendor lock-in; cloud readiness for hybrid deployment models; data localisation capabilities to meet RBI requirements; robust cybersecurity posture, including end-to-end encryption and ISO 27001 certification; and AI governance with explainable models and comprehensive audit trails.

Platforms designed specifically for financial institutions tend to offer deeper compliance and fraud-detection capabilities than general-purpose surveillance tools. And the business case is compelling. Beyond the operational improvements already mentioned, these systems typically pay for themselves within 18–24 months through a combination of loss prevention, efficiency gains, and compliance cost savings.

The measurable impact extends across every dimension of security and operations, from seconds-fast threat detection to dramatically reduced investigation times to improved audit readiness. Of course, adoption must be guided by responsible AI principles, balancing innovation with privacy, preventing algorithmic bias, and ensuring human oversight to maintain public trust.

The institutions that invest in intelligent, future-ready surveillance will define the next era of financial security in India. This is not simply a technological upgrade but a strategic shift that strengthens customer trust, protects assets, enhances resilience, and ensures India's financial backbone remains secure as it grows. In a country where financial inclusion is expanding at unprecedented speed, building smarter, more responsive security infrastructure is foundational to the stability and credibility of the entire ecosystem.

The author is the Vice Chairman and Managing Director of Videonetics.
feedbackvnd@cybermedia.co.in

PCQUEST
TECH TODAY & TOMORROW

CyberMedia

PCQUEST MARCH 2026 EDITION
THE ARCHITECTURE OF INCLUSION

ALSO READ MORE ON

- India's AI turning point: From pilots to real power
- From AI experiments in 2025 to enterprise scale in 2026
- AI on the ground: Practical use cases of AI in large enterprise operations
- How hospitals can use AI without risking patient data
- How automation at the periphery is accelerating digital transformation
- REVIEWS: Sennheiser HD 560S with HD 500 BAM | Sony InZone E9 | Halo smart sensor

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

[COMMENTARY]
POLICY

MeitY's deepfake clampdown: short, sharp and suddenly real

India's new rules require platforms to label AI-generated content and comply with accelerated takedown orders, signalling tighter oversight of synthetic content.

BY GANGESH VARMA & SRIJA NASKAR

On 10 February 2026, the Ministry of Electronics and Information Technology (MeitY) gave legal form to a policy conversation that has been gaining urgency for more than a year: deepfakes and artificial intelligence or AI-generated content are now explicitly regulated under India's Information Technology Act (IT Act) and its intermediary rules (IL Rules). The notification marks a new frontier in digital governance, a move that could reshape how platforms, users and businesses coexist in the rapidly evolving landscape of synthetic media.

The urgency behind this shift is easy to understand. Ultra-realistic synthetic videos, audio clips and images created or altered using artificial intelligence have evolved from technological curiosities into tools capable of causing real-world harm. They have been used to undermine reputations, mislead voters, enable financial frauds and create non-consensual sexual content.

What once required advanced technical expertise can now be done with widely available tools and a smartphone, dramatically lowering the barrier to misuse at unprecedented scale and velocity.

BRINGING SYNTHETIC MEDIA INTO LEGAL SCOPE

Governments around the world have been grappling with the challenge of encouraging AI-driven innovation while protecting individuals and institutions from abuse. Until recently, India's legal framework, while applying to new and emerging technologies, did not expressly categorise deepfakes or synthetic media as a distinct regulatory class under the IT Act and its rules. Platforms largely relied on their own policies, while courts addressed harmful synthetic content on a case-by-case basis, resulting in uneven enforcement and regulatory uncertainty.

MeitY's amendment seeks to close this gap by clarifying that existing intermediary obligations, including

> By formally defining synthetic information, India has moved deepfakes from a regulatory grey zone into a structured compliance category under the IT Act.

IN BRIEF

- India has formally recognised synthetically generated information, including deepfakes, under the IT Act, bringing Gen AI content under intermediary rules.
- Platforms must now label AI-generated or AI-modified content, introducing transparency to help users distinguish authentic material from synthetic media.
- Takedown timelines for unlawful synthetic content may fall to three hours when ordered by courts or authorities, tightening platform compliance duties.
- The amendment follows incidents of election-related deepfakes, scam calls and impersonation frauds, which intensified scrutiny of platform responsibility.
- Technology platforms must strengthen detection tools, provenance metadata and trust-and-safety teams to respond quickly to regulatory orders.
- The new framework seeks to balance innovation in generative AI with safeguards against misinformation, reputational harm and digital fraud.

due diligence, transparency, and compliance with lawful takedown directions, apply equally to AI-generated and synthetic content. In doing so, it brings generative AI platforms squarely within India's established digital compliance framework and sets the stage for more structured enforcement in the months ahead.

At its core, the notification introduces three major shifts. First, it gives "synthetically generated information" (SGI), including deepfakes and AI-generated visuals, a formal legal identity. This provides regulators and courts with a clearer regulatory objective, moving synthetic media from a grey zone into a defined compliance category. Second, the amendment mandates greater transparency by requiring platforms and intermediaries to clearly label AI-generated or AI-modified content.

The aim goes beyond basic tagging; it is intended to help users quickly distinguish between authentic and machine-created material. This transparency seeks to reduce confusion, curb manipulation, and limit the potential for harm. Third, and perhaps most strikingly, the amendment drastically compresses takedown timelines. In some cases, when a competent authority or court issues a lawful order, platforms must now remove unlawful synthetic content within just three hours, a significant acceleration from the earlier 36-hour standard under the general IT Rules. Overall, these developments indicate the continued transition towards more proactive content moderation in the IL Rules.

GLOBAL POLICY DEBATES SHAPE INDIA'S MOVE

For India, this amendment was not a flash decision. Over the past year, MeitY engaged in structured consultations with technology platforms, industry bodies, civil society groups, and academic experts, particularly in the aftermath of widely publicised incidents involving election-related deepfakes and AI-generated scam calls impersonating public figures. These episodes intensified regulatory scrutiny and heightened urgency around platform accountability. International developments also shaped policy discourse.

The European Union's Digital Services Act, which imposes enhanced transparency and due diligence obligations on large platforms, and ongoing regulatory debates in the United States around AI labelling and electoral integrity, provided comparative reference points for India's evolving framework. Perhaps most critically, in the regulatory vacuum, domestic courts became increasingly involved, issuing piecemeal orders against specific pieces of harmful content.

> A three-hour take-down window dramatically changes platform accountability, forcing intermediaries to develop faster detection and response systems.

The absence of a statutory anchor for synthetic media meant those rulings were often slow, uncertain or inconsistent. The amendment crystallises these policy responses, such as standardised labelling, improved transparency, and definitional clarity, into a legal mandate.

MeitY's timing reflects three converging pressures: the speed at which deepfakes spread and cause irreversible harm within minutes, the growing recognition that platform self-regulation has not kept pace with technological risk, and a broader global push among governments to act on AI-enhanced harms. Given India's aspiration to provide a 'third-way' to technology regulation, its vast internet user base, and rapidly expanding digital economy, it does not want to lag behind.

With the amendment now in force and only a short transition window, attention shifts from notification to execution: Social networks, video sites and generative AI platforms will need to overhaul internal systems, strengthen detection tools, integrate provenance metadata and operationalise 'Trust and Safety' teams or tools capable of responding to official orders within hours.

Further, courts are likely to become early testing grounds for defining the contours of synthetic information, who qualifies as a competent authority to trigger takedowns, what safeguards protect legitimate expression, such as satire or critique, and how conflicts are handled when orders or takedowns are contested.

COMPLIANCE RACE BEGINS FOR PLATFORMS

The amendment's impact on stakeholders is multifaceted. The clarity and certainty in AI's regulatory landscape are welcome, but they come with specific challenges. Larger platforms are better positioned to manage the costs and complexities of compliance, especially in terms of technical capacity to implement automated processes to meet shortened timelines. However, the same could prove onerous to some smaller businesses or niche services.

For advertisers and publishers, adapting verification processes and building labelling systems is urgent, since disseminating unlabelled synthetic content could have both legal and reputational consequences. Ordinary users may benefit from improved visibility about the authenticity of online content, though there is a risk that overzealous enforcement could impact legitimate artistic or political expression.

Meanwhile, civil society groups and legal experts remain watchful, emphasising that rapid takedown mandates raise serious concerns about due process, transparency, and appeal mechanisms, particularly because they apply far beyond the scope of the newly introduced definition of SGI.

BALANCING INNOVATION WITH DIGITAL RIGHTS

Regulation in the AI era is never binary. Swifter takedowns and mandated transparency aim to reduce harm and restore user trust, but also concentrate decision-making power with authorities and platforms operating under tight timeframes.

While this amendment is conceived as a pre-emptive policy posture regarding AI-generated or modified harmful content, it also addresses an older challenge: misinformation online. The new law, while recognising that synthetic media is here to stay, also asks whether we can shape its circulation before harm outruns mitigation. Whether this approach balances safety and rights or will result in collateral damage will be determined as the law is implemented and enforced in the future.

For platforms, it is a compliance sprint. For courts, it is a new procedural frontier. For users, it is an attempt to make the digital world more legible. For policymakers globally, it is another data point in the never-ending experiment of governing technology.

However, the success of this intervention will be measured not merely by compliance with the statutory text, but by whether it can effectively reduce the ubiquity and increase the visibility of the creation and diffusion of harmful synthetic content to the average internet user in India.

Varma (left) is a Principal Associate and Naskar is an Associate, both at Saraf and Partners.
feedbackvnd@cybermedia.co.in

DATAQUEST 40+ YEARS THE BUSINESS OF INFOTECH

CyberMedia

DATAQUEST MARCH 2026 EDITION:
FROM RANK TO READINESS: WHAT DEFINES INDIA'S BEST T-SCHOOLS IN 2026

ALSO READ MORE ON

- India's AI moment is not about models alone, but who gets access, trust, and control
- Cognizant CAIO Babak Hodjat explains how Agentic AI will transform enterprises - Babak Hodjat
- Why India may need a middle-power AI alliance to secure digital sovereignty - Mark Brakel
- India's test-drive, World's triathlon - Chris Casey
- Are You Bleeding While Leading? | • AI slop. Not AI spit. Yet
- The AI Crayon Box: Where's The Pink?

Scan QR Code & Subscribe now…

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

https://shorturl.at/vn6tN

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

Dataquest dataquestindia

#ImpactingICTfor4Decades

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

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

Cyber insurance: The new backbone of India's digital resilience

As India's digital infrastructure expands across payments, commerce and services, cyber insurance is emerging as a financial layer that protects continuity.

BY EVAA SAIWAL

Over the past decade, India's growth story has been transformational. The country's Gross Domestic Product (GDP) grew by more than 40% between 2014–22, and India is now set to become the third-largest economy in the world. Alongside India's physical economy, the digital economy is also booming. But with great scale comes greater risk.

The country has reached an inflexion point where cyber insurance is emerging as the essential barrier between digital ambition and digital vulnerability. It is the silent engine critical for ensuring India's growth remains uninterrupted.

Today, almost every Indian household uses the internet and digital services in their daily lives, including UPI transactions, online shopping and much more. Businesses have also become fully digitalised, relying on digital platforms for operations and various functions. Hence, there is a growing risk of cyber fraud targeting businesses and individuals.

Cybersecurity incidents surged from 10.29 lakh in 2022 to 22.68 lakh in 2024, reflecting the scale of digital threats across sectors. With vast volumes of sensitive customer data at hand, businesses are highly vulnerable to data breaches, phishing attacks, and ransomware that can cost them heavily in terms of financial losses and penalties. Small and midsize enterprises, which form the majority of India's commercial backbone, often lack the financial resilience to absorb such shocks.

Cyber insurance addresses this gap in the digital economy by protecting businesses and individuals from unexpected incidents. Today, personal cyber insurance policies cover a wide range of risks, including theft of funds, identity theft, malware removal, fake online shopping sites, and cyberbullying.

> Cyber insurance is moving beyond a technical add-on to become a core risk-transfer and risk-financing layer in modern Enterprise Risk Management frameworks.

Additionally, these policies are very affordable, with the premium being less than Rs 500 for a Rs 1 lakh cover. The cost of a Rs 3 lakh cover is around Rs 500–600, while a Rs 10 lakh cover costs under Rs 1,000. You can get Rs 1 crore coverage for under Rs 3,000—about the price of a pizza or a movie ticket. Cyber liability insurance for businesses covers first-party costs, including business interruption, forensic costs, and data breach costs. It also covers third-party costs, including privacy and network security liability protection, multimedia liability, and IPR infringement.

With the Digital Personal Data Protection (DPDP) Rules coming into effect last year, such protection is no longer optional; it is essential. Given the rising frequency of cyber threats, the adoption of cyber insurance—especially among individuals and SMEs—is fast becoming central to strengthening long-term growth in India's digital economy.

CYBER INSURANCE ENTERS ENTERPRISE RISK STACK

For enterprises and SMEs, cyber insurance has moved beyond being a technical add-on. It is increasingly positioned as a core risk-financing and risk-transfer mechanism within modern Enterprise Risk Management (ERM). In practice, cyber insurance strengthens the business case for resilience by connecting cyber incidents directly to revenue continuity, cash-flow stability, regulatory exposure, and board-level accountability—areas that matter not only to CISOs but also to CFOs, CIOs, and risk committees.

#1
BUSINESS INTERRUPTION AND OPERATIONAL CONTINUITY

Cyber business interruption (BI) coverage responds when a cyber incident disrupts systems that the organisation depends on to generate revenue or deliver services. Such disruptions can lead to income losses when websites, applications, internal systems, or digital platforms become unavailable due to outages or cyberattacks.

Beyond revenue loss, organisations may incur increased costs of working (ICW) as they attempt to maintain operations during the disruption. These expenses can include engaging cybersecurity specialists, deploying temporary IT infrastructure, shifting workloads to alternative environments, or even reverting to manual operational processes. Companies may also face temporary continuity expenses during the recovery phase, while systems are restored and operations gradually return to normal.

Within the ERM framework, this coverage ensures that operational resilience is not only planned for but also financially supported, reducing the risk that prolonged disruptions escalate into solvency challenges or reputational crises.

#2
CYBERATTACKS AND ENTERPRISE CASH-FLOW SHOCKS

One of the most immediate enterprise-level impacts of a cyber incident is liquidity stress, particularly for SMEs and mid-sized organisations. Cyber events such as ransomware attacks, data breaches, or major IT outages often trigger simultaneous financial pressures, including rising expenses and delayed revenue.

Organisations frequently incur immediate costs related to incident response and recovery efforts, including forensic investigations, cybersecurity remediation, legal advisory, and crisis communication. In many cases, these incidents may also lead to direct financial losses arising from fraud, stolen funds, or extortion payments associated with ransomware attacks. At the same time, revenue streams may be delayed or suspended when systems remain unavailable, or business operations slow down during recovery.

This mismatch between escalating costs and deferred income can place acute pressure on working capital. In such circumstances, cyber insurance acts as a financial stabiliser, helping organisations absorb the immediate financial shock while recovery and remediation efforts are underway.

#3
REGULATORY PENALTIES AS A MATERIAL FINANCIAL RISK

Regulatory exposure has emerged as a material financial risk following cyber incidents, particularly in India's evolving data protection landscape. Under the DPDP Act, penalties are

> As India scales its digital economy, cyber resilience will depend not only on stronger technology safeguards but also on smarter risk-transfer mechanisms.

designed to serve as strong deterrents against inadequate data protection practices and governance failures.

The law provides for penalties of up to Rs 250 crore for failure to implement reasonable security safeguards to protect personal data. Organisations may also face penalties of up to Rs 200 crore for failing to comply with obligations related to children's data protection or for not reporting breaches to the Data Protection Board and affected individuals. Significant data fiduciaries that fail to meet additional statutory responsibilities can face penalties of up to Rs 150 crore.

Further penalties of up to Rs 50 crore may apply for violations relating to consent management and other general compliance obligations. In addition, individuals may face a penalty of Rs 10,000 per instance for filing frivolous or false complaints under the Act.

From an ERM perspective, these provisions elevate cyber incidents from operational disruptions to balance-sheet risks, reinforcing the need for risk-transfer mechanisms and compliance-aligned incident response frameworks.

#4
BOARD ACCOUNTABILITY AND GOVERNANCE OVERSIGHT

Cyber risk governance now sits firmly at the board level. Under Section 166(3) of the Companies Act, 2013, directors are required to exercise due and reasonable care, skill, and diligence in overseeing organisational risks. Increasingly, corporate governance interpretation treats cybersecurity as a material enterprise risk that demands active board oversight.

Regulatory expectations reinforce this accountability. The Information Technology Act and CERT-In rules mandate the timely reporting of cyber incidents, while the DPDP framework requires organisations to comply with data protection obligations, including breach notification requirements.

Within ERM structures, boards are therefore expected to oversee not only technical response strategies but also the broader management of business impact, regulatory reporting obligations, and stakeholder communication. Cyber insurance supports this governance framework by enabling structured incident response and financial resilience when cyber risk materialises in real time.

SECTOR-SPECIFIC RISKS DEMAND TAILORED COVER

Different industries face distinct cyber exposures and therefore require different insurance priorities. The financial impact, operational disruption, and regulatory consequences of cyber incidents vary widely across sectors, depending on how digital systems support core business functions.

Retail and E-commerce: Such platforms face elevated exposure to customer data breaches, payment system compromise, and platform downtime. Because transactions and customer interactions are highly digitised, cyber incidents can immediately translate into revenue loss through transaction failures, suspended online sales, and disruptions to order processing.

Beyond lost revenue, such incidents often trigger a cascade of additional costs. Organisations may incur expenses related to notifying affected customers, handling consumer claims, and managing payment liabilities arising from compromised transactions. At the same time, companies must manage crisis communication and reputational damage, particularly when incidents affect large volumes of customer data.

Recent cyber incidents involving a large UK-based multinational retailer illustrate how attacks on core IT systems can disrupt omnichannel operations. The disruption affected online order fulfilment, inventory visibility, and in-store processes, demonstrating how deeply digital infrastructure is now integrated across payments, logistics, merchandising, and customer engagement.

BFSI and Fintech: Cyber incidents often escalate rapidly from IT disruptions into financial, regulatory, and trust crises in the sector. Even brief outages can interrupt payments, lending operations, or customer access to funds, making operational continuity a critical risk factor for financial institutions.

> For SMEs and digital enterprises, cyber insurance helps absorb financial shocks when cyberattacks disrupt operations, cash flow and customer trust.

A combination of business interruption, direct financial theft, and fraud losses typically drives the financial impact of such incidents. Organisations must also manage the costs of incident response, including forensic investigations and system remediation. In parallel, financial institutions face mandatory regulatory notifications and heightened supervisory scrutiny following cybersecurity breaches.

Emerging segments such as crypto and digital asset platforms have further highlighted these vulnerabilities. In 2025, a major Indian crypto-fintech player reportedly experienced a significant cyber incident after attackers gained access to an internal operational account used for liquidity management, resulting in losses of approximately Rs 370 crore in digital assets.

Although customer funds were reportedly protected through wallet segregation, the incident exposed weaknesses in operational controls and governance. It subsequently triggered regulatory scrutiny, forensic investigations, and sustained reputational consequences for the organisation.

CHALLENGES SLOWING CYBER INSURANCE ADOPTION

While cyber insurance adoption in India is gradually increasing, several structural challenges continue to limit deeper penetration—particularly among small and medium enterprises (SMEs). These challenges stem from a combination of awareness gaps, uncertainty around claims processes, and evolving regulatory frameworks.

Cyber risk is still often perceived as a technology issue rather than an enterprise, financial, and governance risk. This limits early involvement from CFOs, boards, and risk committees, slowing adoption and leading to underinsurance. Limited claims history, evolving policy wordings, and misconceptions around exclusions and sub-limits create uncertainty about claim outcomes. This can lead to misaligned expectations between insured organisations and insurers.

There is also ambiguity around coverage for regulatory penalties, as insurability depends on policy wording, judicial interpretation, and public policy considerations. This can lead to mismatched expectations at the time of a claim.

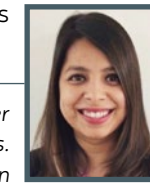
REGULATORY ALIGNMENT UNDER THE DPDP REGIME

The evolving regulatory environment has also raised questions about the interaction between cyber insurance and data protection laws. While the DPDP Act is designed as a strong deterrent against non-compliance, the insurability of such penalties often depends on policy wording, judicial interpretation, and broader public policy considerations. This can create ambiguity about whether certain penalties or liabilities are covered under cyber insurance policies. As a result, organisations may face uncertainty when claims arise if policy language and regulatory expectations are not clearly aligned.

Another challenge relates to incident reporting timelines. DPDP obligations around breach notification may require rapid disclosure, while cyber insurance policies impose strict conditions on notice, panel appointments, and response coordination. Any misalignment between regulatory timelines and policy requirements can complicate incident management.

Cyber insurance is no longer a "nice-to-have". In an economy where digital adoption is accelerating across households, SMEs, and large enterprises, cyber insurance functions as critical infrastructure—protecting operational continuity, stabilising cash flows after incidents, enabling structured response, and supporting regulatory and board-level accountability.

As India continues to scale its digital economy, strengthening cyber resilience will require not only stronger technology controls but also smarter risk-transfer mechanisms. Cyber insurance is the missing layer that can help ensure India's digital growth remains resilient, trusted, and uninterrupted.



The author is Head of Liability and Cyber Insurance at Policybazaar for Business.
feedbackvnd@cybermedia.co.in

Telco capex walks a tightrope of returns

As capex surges to fund 5G and AI-era networks, telecom operators face the harder challenge of turning massive infrastructure investments into real returns.

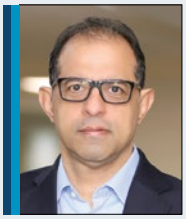
BY PRATIMA HARIGUNANI

Moving from one generation of mobile technology to the next requires equipment upgrades and network modernisation. Seeking customer stickiness in a competitive market demands capacity expansion, new sites and improvements in network experience for sharper signal quality and better Return on Invested Capital (ROIC). Competing with hyperscalers also requires significant capital expenditure.

Yet capex is becoming a difficult Scylla and Charybdis situation for telecom operators. The challenge is no longer about capex turning into a cliff, but about it becoming something closer to a glass cliff.

Even as it becomes imperative to add and maintain network assets and equipment, telecom operators struggle to extract meaningful returns in an intensely competitive market. More critically, they risk tightening

> Telecom networks are expanding rapidly to meet data demand, but the gap between infrastructure investment and revenue growth continues to widen.



"Rising data consumption across mobile networks, fixed wireless access and broadband will continue to drive strong investment in network expansion."

TARUN CHHABRA
SVP & Country Head, Nokia India

their purse strings precisely when investment makes the strongest strategic sense. Invested capital has grown faster than revenue over the past decade, as data from McKinsey illustrates.

In the United States, invested capital expanded by more than 77%, while globally it increased by around 23%. Global telecom network operators spent about USD 315 billion in capital expenditures in 2023, with capex accounting for roughly 17% of revenue. At the same time, global mobile operator capex between 2022 and 2030 is expected to decline at a compound annual growth rate of –2.5%. If data traffic growth does not translate into proportional revenue growth that justifies capacity upgrades, expanding capex becomes a complicated decision for operators.

The mathematics of capital intensity has also evolved. Capital intensity measures how much capital investment is required to generate a dollar of revenue. A high ratio indicates a capital-intensive industry, while a lower ratio suggests a more asset-light model. After four years of rising capex-to-revenue ratios, capital intensity showed a notable decline in 2024 compared with the 2022 peak.

In emerging markets, capital intensity tends to remain above the global average as telecom operators invest to meet growing connectivity demand. According to the Boston Consulting Group, median ROIC in emerging markets exceeds the Weighted Average Cost of Capital (WACC) by about 60 basis points, supported by favourable regulatory environments and sustained capex investments.

In developed markets, however, median ROIC falls about 90 basis points below WACC. Continuous upgrades and rising digitisation demand compel operators to invest even when returns fall short of capital costs.

India illustrates this paradox clearly. The year 2025 saw strong momentum in network capacity expansion, with the country crossing 5.15 lakh 5G Base Transceiver Station sites, tele-density rising to 86.76%, and average mobile data usage reaching 36 GB per month. Forecasts suggest this could rise to 65 GB per month by 2031.

In an industry snapshot released earlier, Mahendra Nahata, Managing Director of HFCL, observed that the telecommunications infrastructure landscape has reached a critical threshold where capacity, density and deployment speed determine competitive advantage. India installed more than five lakh 5G base stations, achieving around 85% population coverage, while total wireless data traffic reached 65,009 petabytes in the second quarter of 2025—growth that makes fibreisation essential for maintaining network quality.

Nahata also pointed to another structural shift: hyperscale operators now account for around 44% of global data centre capacity, operating more than 1,100 large facilities worldwide. This concentration is accelerating infrastructure build-outs across fibre networks and data centres.

Tarun Chhabra, Senior Vice President and Country Head, Nokia India, similarly pointed to strong investment momentum across multiple connectivity layers, noting that rising data consumption across mobile networks, fixed wireless access and broadband will continue to drive substantial investment in network expansion and upgrades.

Despite these investments, revenue uplift has not always matched the pace of deployment. "In many markets, telecom operators have invested heavily in 5G and fibre, but revenue growth has not kept pace," observes Titus M, Practice Director at Everest Group.

"This is driving a more cautious capex posture, sharper prioritisation and increased focus on lowering the cost to serve." Capex therefore presents a complex strategic

"Operators have invested heavily in 5G and fibre, yet revenue growth has not kept pace, forcing sharper capex prioritisation and cost discipline."

TITUS M
Practice Director, Everest Group

TELCO CAPEX PRIORITIES

- Fibre expansion: Densifying fibre networks to support surging data traffic and strengthen 5G backhaul capacity.
- AI infrastructure: Building data centres, GPU capacity and distributed compute platforms to support emerging AI workloads.
- Network modernisation: Upgrading legacy systems, integrating BSS and OSS platforms, and increasing automation.
- Enterprise networks: Investing in private 5G, edge computing and secure connectivity services for industrial customers.
- Operational efficiency: Using AI-driven automation and smarter planning tools to optimise network performance and reduce costs.

dilemma for telecom operators. While upgrade cycles and rising digital demand compel continuous investment, the challenge of generating returns forces operators to rethink how capex should be deployed in the next phase of telecom growth.

BALANCING INVESTMENTS AND RETURNS

Telecom operators are responding by tightening investment discipline and focusing capex on areas where demand is proven. According to Titus, operators are prioritising network coverage, capacity expansion and modernisation while adopting automation and artificial intelligence in operations to improve efficiency and reduce recurring network costs.

At the same time, they are expanding enterprise propositions that combine connectivity with security services, private wireless networks and edge-enabled platforms. Instead of attempting to monetise every capability independently, telecom providers are increasingly building ecosystems through partnerships.

However, several structural challenges remain. One is the monetisation lag, where new network capabilities take longer to translate into pricing power and revenue growth. Another issue is the slow commercialisation of Multi-access Edge Computing (MEC), where fragmented footprints, limited developer engagement and a shortage of repeatable industry solutions have constrained adoption.

There is also a persistent mismatch in go-to-market approaches. Enterprise value is typically linked to business outcomes and system integration rather than connectivity alone, requiring different sales strategies and partner models compared with traditional consumer connectivity businesses. Competitive pressures further complicate the picture, as capacity expansion combined with price competition can dilute returns even as network quality improves.

MONETISATION PATHS FOR TELECOM CAPEX

Capex need not remain a financial quagmire if operators can convert infrastructure investments into monetisation opportunities. One pathway lies in supporting hyperscale and sovereign AI infrastructure. Fibre networks, data centre connectivity and distributed computing resources can support emerging AI workloads and national AI infrastructure initiatives.

"Spectrum-as-a-service can help operators monetise network assets while enabling enterprises to access high-performance connectivity without heavy capex."

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

Operators are also exploring opportunities around AI-enabled Radio Access Networks and infrastructure sharing models that allow underutilised processing capacity to be repurposed for AI applications.

Another approach involves creating enterprise services that justify ongoing upgrade cycles across 4G, 5G and eventually 6G networks. As telecom networks become more programmable, operators can monetise advanced capabilities through specialised services and enterprise platforms. Modernisation of operational systems offers another avenue, where integrating historically fragmented Business Support Systems and Operational Support Systems can improve efficiency and enable more flexible service creation.

Industry analysts also observe a shift in capex priorities. According to Dell'Oro Group, telecom operators are reallocating investments away from blanket coverage expansion towards improvements in capacity, quality, automation and energy efficiency.

A recent Omdia report similarly highlights the emergence of AI infrastructure as a major driver of telecom investment. Operators across Asia, Europe, Canada and the Middle East are committing multi-year capex programmes focused on cloud platforms, data centres, GPU-as-a-Service offerings and AI-driven network architectures. New business models are also being explored. Spectrum-as-a-service represents one such opportunity.

Stan Gray, Senior Vice President for IoT Broadband and High-Cap Vertical Sales at Telit Cinterion, notes that the model reflects a broader shift as telecom operators search for new monetisation avenues beyond saturated consumer markets. "As consumer mobile markets approach saturation and the financial return on 5G investments remains uncertain, operators are actively exploring new monetisation strategies," he explains.

According to Gray, spectrum-as-a-service aligns with enterprise demand for flexible, high-performance connectivity without the capital and operational burden of private network deployments. As standalone 5G networks mature and edge computing capabilities expand, spectrum-as-a-service could allow operators to position themselves as end-to-end solution providers rather than simply traffic carriers, opening new revenue streams across manufacturing, logistics, healthcare, utilities and public safety sectors undergoing digital transformation.

Operational efficiency can also improve capital productivity. McKinsey notes that capacity simulation models allow telecom operators to optimise capital expenditure plans more effectively. In some cases, operators have improved capex efficiency by 10–15% while repurposing as much as 25% of planned investments. Reducing maintenance costs of legacy infrastructure is another option, where strategic removal or monetisation of idle network assets—including the gradual retirement of copper networks—can free up capital for modern deployments.

Unutilised fibre capacity offers a similar opportunity. Often the result of over-provisioning or slower-than-expected adoption, spare fibre capacity represents sunk capital but can also serve as a strategic buffer for future growth. Gray notes that the more immediate risk may lie in early operational challenges around 5G deployments, particularly in areas such as security, interoperability and deployment complexities.

For telecom operators, capex therefore remains both a challenge and an opportunity. The coming years will determine whether these investments become financial burdens or strategic assets capable of supporting the next phase of digital infrastructure growth. What was once perceived as a cliff may yet prove to be a turning point for the telecom industry.

pratimah@cybermedia.co.in

Brain signal implant cleared for spinal injury care

The coin-sized implant decodes neural signals to control a robotic glove, helping spinal cord injury patients regain hand use.

China's medical regulator has approved a brain-computer interface developed by Neuracle Medical Technology for commercial use in people with spinal cord injuries, marking the first regulatory clearance of such a device for routine clinical application.

According to the National Medical Products Administration, the system is designed to help partially paralysed adults regain limited hand movement through brain signal recording combined with robotic assistance.

Developed by Shanghai-based Neuracle Medical Technology, the system includes a wireless implant roughly the size of a coin that sits on the surface of the brain's outer membrane. Electrodes capture electrical signals produced by neurons, which are then processed by software that decodes the activity into digital commands.

These commands are transmitted to a pneumatic robotic glove worn by the patient. The glove responds to the decoded signals and assists with hand movements such as grasping objects, enabling some daily functions despite disrupted nerve pathways between the brain and limbs.

The device is approved for adults with spinal cord injuries who still retain some upper arm function. The system attempts to bypass damaged neural pathways by translating brain activity into mechanical movement.

Brain-computer interfaces, also known as brain-machine interfaces, have been studied for decades in clinical research. Invasive versions involve implanting electrodes on or inside the brain to capture neural signals with greater precision.

Early research programmes such as the BrainGate consortium demonstrated that people with paralysis could control computer cursors and type using neural activity, laying the foundation for assistive technologies that convert brain signals into device control.

CyberMedia

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

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

UNMATCHED REACH ACROSS OUR FLAGSHIP BRANDS

DATAQUEST
Enterprise &
Tech Leadership

PCQUEST
CIOs, Tech
Influencers & SMBs

VOICE&DATA
Telco & Digital
Infra Leaders

DQCHANNELS
ICT Partners &
Channel Decision Makers

OUR BESPOKE B2B MARKETING PROGRAMMES BUILD, ENGAGE AND SCALE COMMUNITIES

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

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

DELIVER INFLUENCE AND OUTCOMES WITH CYBERMEDIA

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

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

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

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 OF MANAGEMENT

Dwarka, New Delhi | Estd. in 1993

50+ Years of EXCELLENCE Since 1967 — APEEJAY EDUCATION

ADMISSIONS OPEN 2026-28

Transform Your Career with World-Class PGDM Program at Apeejay

Ranked among the top business schools in India by Times B-School Ranking 2025

Post Graduate Diploma In Management

(MBA equivalent by AIU)

Specialisations Offered:

Business Analytics | Accounting & Finance | Human Resource | Marketing | Operations & Decision Science

WHY CHOOSE APEEJAY SCHOOL OF MANAGEMENT?

- Industry-Driven Curriculum
- State-of-the-Art Campus
- Distinguished Alumni Network
- International collaborations and opportunities for global exposure
- Guest lectures, internships, and placement drives by leading companies

ACCREDITATIONS

NBA | AICTE | Association of Indian Universities

Times B School 2025 RANKINGS

- Ranked 7th — ALL INDIA (Private)
- Ranked 3rd — NORTH INDIA (Private)

GET CHOSEN BY TOP RECRUITERS

amazon | HDFC BANK | Deloitte. | ICICI Bank | ACUITY | MARUTI | TCS TATA CONSULTANCY SERVICES

Gartner | HCL | ION | accenture | cvent | Ameriprise Financial

& many more...

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

Scan for website

Inviting applications for PGDM Batch 2026-28

Institutional Area, Sector - 8, Dwarka, New Delhi – 110077

E-mail: admissions.asm@apeejay.edu | *Website:* apeejay.edu/asm

FOR ADMISSION QUERIES DIAL: +91 9560 222 999