

VOICE & DATA

Connecting the Digital World

CyberMedia

THE AI SURGE CAN INDIA HOLD IT?

India's AI infrastructure is expanding at speed, but constraints on power availability, orchestration, and access will determine whether this surge can sustain itself.



"AI is enabling networks to self-learn and optimise in real time"
ARUNAV ROY

30



"Orbital data centres are the next evolution of AI infrastructure"
VIJAYAKUMAR ARUMUGA NADAR

34



FOCUS
NETWORKS
RULE THE
BATTLEFIELD

46





APEEJAY SCHOOL

Mahavir Marg, Jalandhar | Estd. In 1968



THE LEGACY OF 50+ YEARS
OF EXCELLENCE CONTINUES

ADMISSIONS
OPEN 2026-27

PRE NURSERY TO IX & XI



Follow us on:



APEEJAY EDUCATION



Quality Education

from Pre-Nursery to
Doctoral level



5,000+

Educators & Staff Members



26

Educational institutions
across the country



40,000+

Students

KEY HIGHLIGHTS



Value-based Holistic Education



Curriculum aligned with
NEP 2020



State-of-the-art infrastructure



Safe & Secure Campus



Outstanding Results in CBSE
and Competitive Exams

Admission Helpline:

+91-181-2453608 | 9311446232

Email:

skool.ms.jln@api.edu



Apeejay School, Mahavir Marg,
Jalandhar, Punjab-144001



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

EDITORIAL

MANAGING EDITOR: Thomas George
CONSULTING GROUP EDITOR: Ibrahim Ahmad
EDITOR: Shubendu Parth
CONSULTING EDITOR: Pradeep Chakraborty
CONTRIBUTING EDITOR: Pratima Harigunani
ASSISTANT EDITOR: Ayushi Singh
SUB EDITOR: Manisha Sharma
SR. MANAGER DESIGN & COVER DESIGN: Vijay Chand

VICE PRESIDENT RESEARCH: Anil Chopra

MANAGER CYBERMEDIA LABS: Ashok K Pandey

LARGE BUSINESS CONVENTIONS & PROJECTS
CONFERENCE PRODUCER: Ajay Dhoundiyal

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

MARKETING & ALLIANCES
SR MANAGER: Ajay Dhoundiyal
ASSISTANT MANAGER: Mohd Atif Uddin

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

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

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

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

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

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

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

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

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

April 2026

[CONTENTS]

COVER STORY 22

THE AI SURGE CAN INDIA HOLD ITS GROUND?

India's AI infrastructure is expanding at speed, but constraints on power availability, orchestration, and access will determine whether this surge can sustain itself.



INDUSTRY SPEAK

- 08** When networks falter, observability must take command
- 10** Cloud risks rising as security gaps widen across systems
- 12** AI-led SOC infrastructure shifts from data to outcomes
- 15** Time to measure data centre sustainability claims

TECHNOLOGY]

- 37** Networks shift from connectivity to intelligence at scale
- 40** AI in networks: Speed up front, strain beneath the hood
- 44** Mesh vs extenders: Rethinking home Wi-Fi design

REPORT

- 66** Power, not proximity, redrawing data centre maps
- 70** Global 5G IoT market to touch USD 85 billion by 2036
- 72** India turns to AI infrastructure for data-driven governance

TELECOM TALK



- 18** Connectivity as strategic infrastructure in uncertain times

LT. GEN. DR. SP KOCHHAR

INTERVIEW



- 30** “AI is enabling networks to self-learn and optimise in real time”

ARUNAV ROY



- 34** “Orbital data centres are the next evolution of AI infrastructure”

VIJAYAKUMAR ARUMUGA NADAR

FOCUS

- 46** Networks rule the battlefield

- 50** “Space is becoming the first line of sensing and defence”

LT. GEN. AK BHATT



- 52** “The traditional kill chain has evolved into a kill web”

GP. CAPT. DR. ASHOK KUMAR



- 55** “Missiles deliver impact, networks decide timing and effect”

CDR. ADITYA VARMA



COMMENTARY

- 60** Quantum threats test India’s cybersecurity doctrine shift

- 63** India’s hyperscale push raises stakes for power quality

REGULARS

06 Voicemail

07 Opening Note

74 Postscript

[NEXT ISSUE]



MARCH 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



Share your views at vndedit@cybermedia.co.in

NEXT
ISSUE

PRIVATE 5G & INDUSTRY 5.0



For any query: ajaydh@cybermedia.co.in



SHUBHENDU
PARTH

[OPENING NOTE]

CCTV crackdown begins, but too late

"There are more things in heaven and earth than meet the eye."

A CCTV camera does not simply watch. It captures, encodes, and transmits—quietly extending the boundary of a network into physical space. In a connected environment, visibility is no longer local. It is persistent, transferable, and, if compromised, permeable in ways that are not immediately apparent.

India's decision to enforce security certification for CCTV systems from 1 April 2026 is therefore necessary. Networked cameras are no longer passive devices. They are data nodes embedded across cities, transport corridors, military perimeters, and homes. When compromised, they do not just leak footage; they expose patterns, movements, and intent.

The new regime, anchored by certification through the STQC Directorate under the Ministry of Electronics and Information Technology, introduces long-missing discipline. Requirements around component traceability, firmware disclosure, and resistance to unauthorised access bring accountability to a widely diffused system.

Globally, such concerns are not new. Several countries, including Australia, Canada, Japan, and the United States, have restricted the use of certain foreign-origin telecom and surveillance equipment citing national security risks. The rationale is clear: in connected systems, vulnerability lies not in hardware, but in unseen layers—code, control pathways, and data flows that resist audit.

In India, CCTV systems have evolved from limited deployments in the 1990s to a pervasive presence across cities, transit systems, and homes. They underpin counter-terrorism, traffic management, and policing. Over time, they have formed a distributed sensing layer—an always-on fabric of observation.

That makes their integrity a matter of infrastructure trust, not device compliance. The certification framework is therefore justified. It aligns with broader measures such as the Telecommunication Act, 2023 and the Digital Personal Data Protection Act, 2022, which recognise networks and data flows as critical assets.

But the question that remains is uncomfortable: why now?

The risks associated with connected surveillance systems are neither new nor peripheral. Concerns around firmware opacity, remote access vulnerabilities, and uncontrolled data flows have been documented for years. Governments elsewhere acted early to ring-fence networks and scrutinise supply chains. India, too, moved in telecom and data governance.

Yet surveillance infrastructure—despite its scale and sensitivity—expanded without a commensurate security architecture. Cameras proliferated across cities and strategic locations, but without a framework to interrogate what lay beneath their lenses: the chipsets, firmware, and data pathways.

The exposure of Pakistan espionage module in Ghaziabad in March 2026, where networked devices were reportedly used to transmit visual and location data, does not define policy. But it crystallises a structural oversight—that surveillance systems were treated as instruments of security, not as potential ingress points.

This is where the delay becomes consequential. In critical infrastructure, vulnerabilities do not stay contained—they metastasise with scale. What is being corrected today should have been embedded at inception.

India has acted, and the direction is correct. But in systems that define both visibility and vulnerability, foresight is not optional—it is foundational.

The lens may now be secure. The question is whether the system that left it exposed for so long has truly been corrected.

shubhendup@cybermedia.co.in

When networks falter, observability must take command

With outages exposing gaps in detection and control, telcos must shift to intelligent observability to predict failures, cut downtime, and maintain network stability.



BY GANESH NARASIMHADEVARA

Telco outages are making headlines in India quite often, with users reporting disruptions to mobile internet, signal failures, and even landline issues. In a country where digital public infrastructure is the backbone of daily life, an hour of downtime can trigger massive financial losses. With the digital economy contributing an estimated 12–14% to India's GDP and projections of this growing sharply in the coming decade, the impact of repeated outages is significant.

Rapid digitisation and surging data consumption have expanded the attack surface and created levels of network complexity that older tools cannot keep up with. Because telco stability underpins the functioning of government systems, critical sectors, remote work, and modern workplaces, providers are now investing heavily in AI-driven, intelligent observability.

This gives telcos the ability to spot anomalies early, understand root causes faster, and prevent costly

downtime, ensuring that India's digital economy continues to run without disruption.

A closer look at the landscape reveals several recurring issues that make reliability harder to sustain. Their complexity often overwhelms traditional monitoring, making it harder for telcos to keep networks stable and available.

RISING COMPLEXITY IN OUTAGE DETECTION

Today, more than 57% of telecom companies experience at least one outage every week, and the bigger problem is that it takes an average of 42 minutes to detect an outage. In that window, every system, be it payments, delivery platforms, hospitals, government portals, or remote teams, starts feeling the impact.

With data usage rising and network infrastructure stretched, operators lose visibility into what is failing and why. Issues that begin as minor quickly escalate into broader disruptions when detected too late. The

Detection delays are no longer tolerable, with observability enabling early signals that prevent small faults from cascading into outages.

combination of legacy systems, traffic spikes, and limited real-time insight is making outages more frequent and harder to control.

This is exactly where intelligent observability changes things. By combining real user monitoring (RUM) with browser, mobile, and synthetic monitoring, telcos can gain live insights into how their network is performing at any given moment. They can spot anomalies early, understand where performance drops, and act before customers feel the impact.

This not only reduces the mean time to detect (MTTD) but also prevents small issues from snowballing into large-scale outages. Instead of firefighting once the system is down, operators can stay ahead of failures and maintain consistent uptime to handle increased digital load.

NETWORK GROWTH STRAINS LEGACY SYSTEMS

In India, nearly every major sector, including education, banking, healthcare, logistics, and e-commerce, now depends heavily on telecommunications connectivity. This rapid shift has put enormous pressure on network infrastructure, making it increasingly difficult to maintain consistent uptime.

The co-existence of 4G and 5G adds another layer of complexity. Managing two network generations at once requires precise handovers and coordinated traffic flows. When these slip, users experience slower speeds, higher latency, and localised outages.

Monitoring becomes equally difficult because telecom infrastructure varies widely across the country. On top of this, fragile infrastructure, rising third-party dependencies, and the use of multiple disconnected monitoring tools lead to further silos, making visibility and reliability even harder to maintain.

OBSERVABILITY RESHAPES NETWORK VISIBILITY

Intelligent observability provides a single, unified view of distributed systems, eliminating silos that slow and inconsistent issue detection. Instead of relying on multiple, disconnected tools, teams get a complete picture of network health in one place, enabling early detection and troubleshooting to be far more efficient.

It also analyses traffic patterns alongside real-user, browser, and mobile monitoring, and synthetic testing in real time to flag anomalies, predict failures, and pinpoint performance degradation.

Observability platforms can correlate data across both 4G and 5G, track end-to-end handover behaviour, and pinpoint where interoperability breaks, enabling telcos to stabilise performance across technologies. With the addition of agentic AI, the system doesn't just surface issues; it can autonomously fix many within seconds, dramatically reducing both MTTD and MTTR.

CYBER RISKS GROW WITH NETWORK SCALE

Weak infrastructure provides attackers with potential entry points to access critical data and systems, and Gen AI-driven threats such as automated phishing, data leaks, and rapidly evolving ransomware are becoming more sophisticated, making traditional security models inadequate.

The widespread use of multiple, siloed tools for monitoring worsens the existing risk by widening the attack surface. Thankfully, observability uncovers hidden threats created by the complexity of 5G, supports AIOps for real-time remediation, and breaks silos between development, security, and operations to maintain service reliability. This prevents outages from exploits, ensures compliance, and scales for high-stakes digital services.

As India scales its digital infrastructure, telcos cannot rely on fragmented tools or delayed detection. Intelligent observability provides the clarity and responsiveness needed to keep networks stable and users connected. Through clearer visibility, faster detection, and automated resolution, telcos can manage distributed systems more effectively and reduce the chance of disruption.

As digital services continue to expand across sectors, adopting AI-led observability will be key to maintaining consistent uptime and supporting the country's broader digital growth. 🌐

*The author is the Director of Solutions Consulting – India, New Relic.
feedbackvnd@cybermedia.co.in*



Cloud risks rising as security gaps widen across systems

Misconfigurations, weak access control, and new architectures are exposing cloud environments, making continuous monitoring and automated protection critical.



BY KUNAL MAHAR

The use of the cloud has increased notably in recent years. Companies are moving their data and applications to the cloud to work faster and reduce costs. This shift also brings significant risks. Hackers are attempting to attack these systems with new techniques every day.

World Cloud Security Day, celebrated on 3rd April each year, is a reminder of these dangers. It highlights that protecting cloud systems requires effort from all stakeholders. A single breach can cost millions in fines and lead to a loss of customer trust. This is a timely moment for organisations to strengthen how they protect their digital assets.

EXPANDING RISKS ACROSS CLOUD MODELS

The cloud threat landscape is expanding at an unprecedented rate, with attackers actively exploiting vulnerabilities across various service models.

While Infrastructure as a Service (IaaS) provides granular server control, that very flexibility increases the likelihood of human error. Platform-as-a-Service (PaaS) streamlines application management but often masks underlying security risks. Similarly, the perceived simplicity of Software as a Service (SaaS) can be deceptive, as shared access frequently creates critical visibility gaps.

Without comprehensive oversight, even minor oversights can escalate into catastrophic security breaches. Limited visibility means that small errors can quickly turn into major security incidents, often before organisations realise the extent of exposure.

MISCONFIGURATIONS DRIVE MOST BREACHES

Misconfigurations remain the most common cause of cloud breaches. Open storage buckets, such as AWS S3, can allow public access to files and expose sensitive data. Overly broad access permissions and exposed credentials further increase risk.

Cloud environments are no longer static systems; they are dynamic ecosystems where even minor errors can cascade into large-scale breaches without visibility.

Statistics indicate that misconfigurations account for more than 80% of cloud leaks. These issues are preventable. Regular audits and automated scans can help detect and correct them before they escalate into incidents.

Access management is equally critical. Weak authentication makes it easier for unauthorised users to gain entry. Over time, permissions accumulate, leading to “privilege creep”, where users hold more access than necessary.

Stolen credentials and unmanaged machine identities further complicate the landscape. Strong identity and access management practices—such as enforcing least privilege and regularly reviewing access—are essential to maintaining control.

NEW ARCHITECTURES WIDEN ATTACK SURFACES

New technologies such as serverless computing and containers enable speed and scalability, but they also introduce new risks.

Container images may contain vulnerabilities introduced by outdated or unverified code. Serverless functions are short-lived, making them difficult to monitor consistently. Microservice architectures create multiple points of exposure, where a single weak link can affect the entire system.

These environments demand proactive security practices. Continuous scanning, rigorous testing, and vulnerability management are essential to ensuring that speed does not come at the cost of security.

ZERO TRUST AND CONTINUOUS MONITORING

Good cloud security begins with the fundamentals. Cloud Security Posture Management (CSPM) tools help organisations continuously track and remediate risks across environments. These tools provide persistent visibility rather than periodic checks, enabling organisations to stay secure throughout the year.

Zero Trust requires verification at every step. No user, device, or application is inherently trusted. Every interaction must be authenticated before access is granted.

Segmenting networks, enforcing strict access controls, and continuously monitoring activity can significantly reduce the risk of lateral movement within systems. Organisations should adopt a phased approach, starting small and expanding Zero Trust principles across their environments.

AUTOMATION, RESILIENCE AND RESPONSE READINESS

Manual processes are no longer sufficient. Automated compliance tools can continuously monitor frameworks such as SOC 2 or HIPAA, identifying issues in real time.

Encryption remains critical. Data must be protected both at rest and in transit using protocols such as TLS and managed key systems. Proper data classification ensures that sensitive information receives the highest level of protection.

Security must be embedded into development processes. DevSecOps integrates security into every stage of the lifecycle, enabling early detection of vulnerabilities. Techniques such as SAST, DAST, and SCA help identify risks before applications reach production. Similarly, Infrastructure as Code must be scanned to prevent the deployment of insecure configurations.

Despite best efforts, incidents can occur. Organisations must prepare with robust response strategies. Cloud-native tools such as AWS GuardDuty and Azure Sentinel provide real-time detection and alerts. Disaster recovery approaches, including immutable backups and multi-region replication, help ensure business continuity during disruptions.

Cloud security requires sustained effort. It is not a one-time activity. It demands continuous monitoring, regular updates, and shared responsibility across teams. Today, organisations must move beyond awareness to action—adopting Zero Trust, automating security practices, and building resilient systems as threats continue to evolve. 🧩

*The author is Head of Security Operations
with 5Tattva.*

feedbackvnd@cybermedia.co.in



AI-led SOC infrastructure shifts from data to outcomes

As AI reshapes SOC systems, organisations must measure what matters, aligning data, analytics, and workflows to deliver outcome-driven decisions at scale.



BY DIPESH KAURA

Security Operations Centres (SOCs) have long been measured by activity—alerts processed, incidents closed, and data ingested. These metrics once reflected effectiveness in environments where visibility was limited, and response speed was the primary concern. That model is now under strain.

Across modern enterprises, the scale and architecture of security operations have shifted. Telemetry now flows continuously from cloud platforms, Software-as-a-Service (SaaS) applications, identity systems, and endpoints, creating a highly distributed data environment.

At the same time, adversaries are operating across these layers, exploiting gaps between tools and systems.

This shift is not merely operational. It reflects a deeper redesign of the underlying security infrastructure—from data ingestion pipelines and analytics platforms to artificial intelligence (AI) compute layers and decision systems. Traditional architectures, built around volume-driven data processing, are struggling to keep pace with this complexity.

In parallel, expectations from leadership have evolved. Boards are no longer satisfied with activity metrics.

Security operations are evolving into infrastructure, where AI, data, and execution layers converge to deliver measurable outcomes at scale.

As data volumes grow, organisations are re-architecting SOC infrastructure to prioritise relevance, reduce noise, and improve decision quality.

They want to understand whether security investments are reducing risk, improving resilience, and delivering measurable outcomes.

This raises a more fundamental question: what does effective SOC performance look like in an AI-driven infrastructure environment?

LIMITS OF LEGACY SECURITY INFRASTRUCTURE

Many SOC's today are operating at full capacity, yet still struggling to demonstrate a clear impact. Analysts spend significant time triaging alerts, assembling fragmented context, and preparing investigations before meaningful response actions can begin. The work is constant, but much of it is repetitive and operationally heavy.

Adding more tools rarely solves the problem. It often increases noise and further fragments workflows, placing additional strain on an already disjointed security infrastructure. Expanding data ingestion can improve visibility, but it also drives up cost without guaranteeing better decisions, as data pipelines scale without corresponding gains in analytical efficiency. Hiring more analysts provides temporary relief, but it does not scale effectively to keep pace with modern threats.

Underneath this is an economic model that has not kept up. Traditional SIEM approaches are built around data volume, treating all telemetry equally regardless of its relevance or analytical value. As environments grow, costs rise steadily while outcomes improve incrementally at best, highlighting the limitations of infrastructure designed for ingestion rather than decision-making.

We end up with a system where effort continues to increase, but returns become harder to justify.

WHY AI LAYERS HAVE NOT DELIVERED VALUE

AI has been widely positioned as the solution to SOC complexity, yet many implementations have struggled to move beyond isolated use cases. While models may perform well in controlled scenarios, their impact in production environments is often less clear. A key reason is not the capability of these models, but rather how they

are integrated into the SOC's operating model and, more importantly, into the underlying infrastructure stack.

When AI-driven decisions cannot be clearly explained, audited, or linked to measurable improvements in analyst productivity, establishing trust becomes difficult. Security teams hesitate to rely on outputs they cannot fully validate. Leaders struggle to quantify value. Boards question both the cost and the risk. These gaps often stem from AI being deployed as an overlay rather than fully integrated into data pipelines, workflows, and control systems.

In many cases, AI becomes an additional layer rather than a transformative force. It accelerates certain tasks, but it does not fundamentally change how work is done or how success is measured, because the core infrastructure it depends on remains unchanged. Hence, a different approach is beginning to emerge.

REBUILDING INFRA FOR PRODUCTIVITY GAINS

Forward-looking organisations are starting to redefine SOC performance around productivity rather than throughput. Instead of asking how much work is being done, they are focusing on how effectively that work contributes to meaningful security outcomes, and how efficiently the underlying infrastructure supports those outcomes.

In a productivity-driven model, AI is not measured by features or theoretical capability. It is measured by the work it completes alongside analysts. How much investigation effort does it remove? How much time does it save? How consistently does it improve the quality of decisions? These gains increasingly depend on how well data flows, analytics layers, and decision systems are aligned within the infrastructure.

With a productivity-driven model, we create a more direct connection between technology investment and operational impact. Infrastructure is no longer evaluated by scale, but by how effectively it converts data into timely, high-quality decisions.

It also introduces a more disciplined approach to data. Rather than treating all telemetry equally, organisations

AI is moving from an overlay to a core layer, embedded within pipelines and workflows to deliver consistent, outcome-driven performance.

begin to align data usage with analytical value. The focus moves from ingesting more data to using the right data in the right context to drive better outcomes, optimising both data pipelines and processing costs.

AGENTIC AI AS AN EXECUTION LAYER

Agentic AI builds on this foundation by introducing a more structured, accountable approach to scaling intelligence within the SOC, effectively creating a new execution layer within the security infrastructure.

Instead of functioning as isolated assistants, AI agents operate as part of a coordinated system, capable of handling investigations, enriching context, and supporting decision-making within defined boundaries.

These agents are integrated across data pipelines, analytics layers, and operational workflows, enabling continuity across the stack. These systems are designed to work with analysts, not around them, taking on operational workload while keeping humans in control of critical decisions.

Analysts spend less time stitching together information across tools and more time evaluating well-formed cases. Investigations move faster, with clearer narratives and stronger context. Decision-making becomes more consistent, reducing variability across teams and shifts, as execution is standardised across the infrastructure.

Importantly, this approach also addresses one of the most persistent barriers to AI adoption: governance, by embedding control and traceability within the execution layer itself.

MAKING AI ACCOUNTABLE TO THE BUSINESS

For AI to operate effectively in security, it must be accountable in the same way human decisions are. This means actions must be explainable, auditable, and aligned with organisational policies and risk tolerance, requiring a governance layer embedded within the security infrastructure.

In a productivity-driven, agentic model, governance is not layered on after deployment. It is embedded into how the system operates. AI-assisted actions follow defined

rules, escalation paths are enforced, and decision-making can be reviewed and validated when needed, supported by audit trails, policy engines, and control mechanisms integrated across the stack.

Security leaders can demonstrate not only that AI is being used, but also that it is used responsibly and effectively. Boards gain clearer visibility into how investments translate into outcomes, as governance infrastructure enables traceability and measurable accountability. AI shifts from being a perceived risk to a governed capability.

MEASURING OUTCOMES ACROSS THE STACK

As cybersecurity continues to evolve, the metrics that define success must evolve with it. Activity and volume will always have a place, but they are no longer sufficient on their own.

What matters now is how effectively the SOC converts effort into outcomes. How well it scales analyst capacity. How consistently does it reduce risk? And how clearly it can demonstrate value to the business, through infrastructure that connects data, intelligence, and execution.

A productivity-driven approach, supported by agentic AI, provides a path toward that future. It aligns technology, operations, and economics around a common goal: delivering measurable, accountable security outcomes at scale, enabled by an integrated, AI-driven security infrastructure.

For SOC teams, this means less noise and more focus. For security leaders, it means clearer justification for investment decisions. For boards, it provides the visibility and confidence they have been asking for.

In a landscape defined by complexity and constant change, the organisations that succeed will not be the ones that process more data or deploy more tools. They will be the ones who measure what matters and build their operations around it, re-architecting the SOC as an intelligent, outcome-driven infrastructure layer. 🧠

The author is the Country Director – India and SAARC at Securonix.

feedbackvnd@cybermedia.co.in



Time to measure data centre sustainability claims

As AI and cloud scale data centre demand, sustainability in India must move beyond intent to auditable metrics, real impact, and transparent proof.



BY ANSHUMAN MAGAZINE

For years, sustainability in India's data centre industry existed largely within corporate social responsibility reports and marketing brochures. As India's digital economy expanded, so did the promises of green facilities. But the industry has now reached a critical inflexion point. As data consumption surges—driven by Artificial Intelligence (AI), 5G, and a massive migration to the cloud—the environmental footprint of the infrastructure supporting this growth can no longer be obscured by vague commitments.

The conversation must shift from claims to proof. For Indian enterprises and global hyperscalers operating in the subcontinent, the era of greenwashing is ending. In its place, a new paradigm of radical transparency and measurable impact is emerging.

SUSTAINABILITY MUST BE MEASURABLE

Green is not an objective state but a measurable trajectory, and this remains the fundamental challenge with sustainability claims in the data centre industry. In the

Renewable energy claims often mask reliance on fossil fuels during peak hours, making hourly carbon tracking critical for credible sustainability outcomes.

Water stress across major hubs is reshaping cooling strategies, pushing operators more towards non-potable sources and closed-loop systems.

Indian context, where the grid continues to rely heavily on thermal power and water scarcity is a recurring reality, a data centre cannot simply declare itself sustainable by planting trees or purchasing carbon offsets.

True sustainability is an engineering discipline. It requires a shift from intent to impact—the verifiable reduction of resource consumption. For a CEO or CIO, the focus must shift to a limited set of high-integrity indicators that reflect the facility's physical reality. If a claim cannot be audited, benchmarked, or measured in real time, it is likely to be greenwashing.

DEFINING THE METRICS THAT MATTER

There are several metrics which must be measured and can play an increasingly important role as the industry evolves.

Energy efficiency remains foundational, expressed as annualised power usage effectiveness (PUE), with clearly defined boundaries and metering methodology. In India's bifurcated climates—hot-humid like Mumbai and Chennai, and hot-dry weather of Hyderabad and NCR—cooling challenges vary significantly, as does the temptation to cherry-pick favourable seasonal results.

Weather-normalised PUE provides a more honest assessment, revealing whether a facility has invested in airflow containment, economisation hours, and liquid-cooling readiness for AI workloads, or is simply benefiting from climatic conditions.

Carbon intensity of delivered electricity is equally critical, measured in kgCO₂e per kWh and reported in both location-based and market-based terms. This must be paired with an hourly 24/7 carbon-free energy match. Annual renewable energy certificates can make a facility appear "100% renewable" on paper, while it continues to depend on fossil-heavy power during peak hours.

An hourly lens enforces alignment with clean energy supply and incentivises strategies such as storage, demand flexibility, and firm clean power purchase agreements (PPAs) that reduce emissions when electricity is actually consumed.



IN BRIEF

- Sustainability must move from narrative to measurable outcomes, with auditable metrics defining energy, water, and carbon impact.
- Annualised and weather-normalised PUE exposes real efficiency, avoiding selective reporting driven by seasonal or operational advantages.
- Renewable claims must reflect real-time consumption, with PPAs, storage, and flexible loads replacing certificate-led accounting.
- Water efficiency must include source risk and embedded use, as low WUE can conceal unsustainable freshwater dependency.
- Embodied carbon in materials and infrastructure is emerging as a key footprint, requiring lifecycle transparency and reuse strategies.
- Grid-responsive data centres that shift demand can support renewable integration, making flexibility central to decarbonisation.

Water intensity and source risk form the third pillar. Direct water usage effectiveness (WUE, in litres per kWh of IT load) is only a starting point. Disclosure must extend to embedded water from electricity generation, source mix—whether municipal, borewell, surface, or

As operational emissions decline, embodied carbon in construction and equipment will increasingly define the lifecycle impact of data centres.

treated—and recycling rates, along with contingency plans for drought. Given the water stress across major hubs, using freshwater evaporatively to achieve low WUE may represent a flawed trade-off. Non-potable sources and closed-loop systems must become standard practice.

Embodied carbon per MW built is another crucial dimension. As grids decarbonise over time, emissions embedded in materials such as concrete, steel, batteries, and switchgear, as well as server refresh cycles, will increasingly dominate lifecycle footprints. Buyers should expect lifecycle assessments supported by Environmental Product Declarations, alongside transparent refurbishment and reuse policies.

Finally, grid-friendliness must be considered. Data centres are programmable loads, and facilities capable of shaping or shifting demand—through thermal storage, batteries, or scheduling non-urgent workloads—can support renewable integration and reduce curtailment. In India's evolving power system, flexibility is not optional; it is central to credible decarbonisation.

RENEWABLES, WATER, AND INDIA'S REALITIES

One of the most common forms of greenwashing is the conflation of “renewable intent” with “renewable impact.” Many providers claim to be “100% renewable” by purchasing Renewable Energy Certificates (RECs). While RECs support the global transition, they do not necessarily change the electron mix entering a specific data centre in Mumbai or Chennai at 2:00 AM when the sun is not shining.

In India, “renewable impact” means moving toward power purchase agreements (PPAs) and round-the-clock (RTC) renewables. It involves investing in captive solar or wind farms and, increasingly, exploring battery energy storage systems (BESS) to bridge the intermittency gap. A credible provider must show a clear roadmap for transitioning their actual hourly load to carbon-free sources.

Equally important is the “water constraint.” Major data centre hubs such as Chennai, Mumbai, and Delhi-

NCR face varying degrees of water stress. A facility that achieves low PUE by evaporating excessive water is not sustainable; it merely shifts the burden. Forward-looking providers are adopting zero liquid discharge (ZLD) systems and air-cooled technologies to decouple compute growth from water consumption.

BUYER CHECKLIST FOR CREDIBLE GREEN CLAIMS

A diligent buyer can distinguish progress from narrative with a few disciplined asks. Demand annualised, site-level PUE with boundaries and 95th-percentile data, not just a flattering mean. Ask for both location-based and market-based emissions intensity and the hourly 24/7 carbon-free energy percentage, with the matching method and grid region disclosed.

Probe additionality by naming PPA projects and commercial operation dates to show that your procurement is enabling new capacity, not just reallocating existing certificates. On water, insist on direct WUE, embedded water from electricity generation, source mix, recycling rates, and a drought contingency that does not fall back on stressed aquifers.

Embodied carbon transparency per MW should be supported by EPDs and clear reuse/refurbishment policies. Also, look for third-party assurance and quarterly cadence. Red flags are increasingly evident: snapshot PUEs during cool spells, “100% renewable” claims based purely on unbundled RECs, or “zero water” assertions that shift the burden off-site.

India's digital growth does not need to come at the expense of climate or water security. By anchoring decisions in a small set of verifiable metrics—and insisting on hourly carbon accountability, transparent water use, and lifecycle visibility—the industry can build data centres that are genuinely sustainable in practice, not merely in narrative. That is the standard the next decade will demand. 🌱

The author is the Chairman and CEO for India, South-East Asia, the Middle East, and Africa of CBRE.

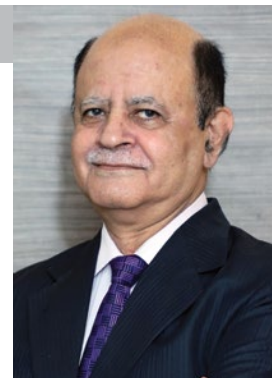
feedbackvnd@cybermedia.co.in



LT. GEN. DR. SP KOCHHAR

CONNECTIVITY AS STRATEGIC INFRASTRUCTURE IN UNCERTAIN TIMES

Recognising telecom as critical infrastructure can unlock protection, priority access, and investment, ensuring continuity, resilience, and security across sectors.



India's digital transformation has reached a point where connectivity is no longer just an enabler of growth but the backbone of national resilience. Telecom today is no longer a standalone vertical but a value-added horizontal supporting every critical function of the state, the economy, and society.

From governance and defence to healthcare, finance, and logistics, all sectors depend on secure, uninterrupted communication networks. However, as the global environment becomes increasingly complex, with rising

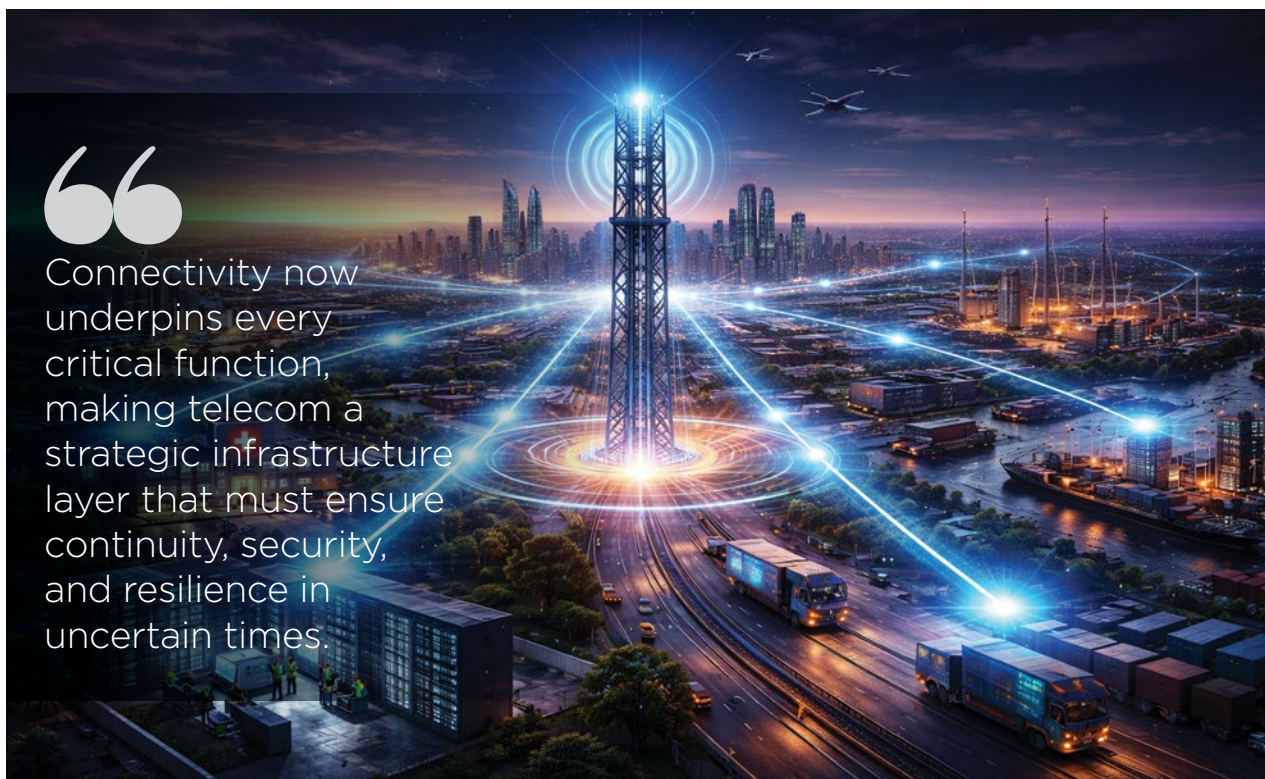
geopolitical tensions, supply chain vulnerabilities, and evolving security considerations, it is important to view telecom through a broader, more strategic lens.

Today, connectivity is no longer merely an enabler of economic activity. It is steadily emerging as critical infrastructure, integral not only to growth but also to resilience, continuity and national preparedness.

As articulated by the Minister of Communications, Jyotiraditya M Scindia, telecom is not a standalone

“

Connectivity now underpins every critical function, making telecom a strategic infrastructure layer that must ensure continuity, security, and resilience in uncertain times.



As geopolitical and cyber risks grow, connectivity is emerging as a strategic asset that enables national preparedness and institutional continuity.

vertical but a “value-added horizontal” that supports and powers every sector of the economy. This framing is particularly relevant in the current context. In an interconnected world, a nation’s ability to sustain its economic and institutional functions, especially during periods of uncertainty, depends fundamentally on the strength and reliability of its communication networks.

ENSURING CONTINUITY AMID GLOBAL RISKS

As conflict evolves beyond traditional battlefields into cyber and hybrid domains, telecom infrastructure must adapt. The focus must shift from enabling growth to ensuring continuity under stress.

Modern economies are deeply dependent on telecom infrastructure. Financial systems rely on real-time connectivity to process transactions and maintain market stability. Similarly, healthcare delivery increasingly depends on digital platforms for consultations, diagnostics and emergency response. Governance frameworks rely on communication networks for service delivery, coordination and citizen engagement. Logistics, transportation and energy systems all depend on uninterrupted connectivity for efficient operations.

In such a scenario, telecom naturally assumes the character of an essential service—one that ensures continuity across sectors and needs to be recognised as such. Telecom must be formally classified as an Essential Service, on par with fuel, electricity and transport, potentially under the Essential Services Maintenance Act.

In crisis or wartime scenarios, communication networks are indispensable for coordination, command and public information. Prioritising telecom in resource allocation, protection frameworks and emergency protocols is critical to maintaining national stability.

India’s digital ecosystem has grown rapidly in both scale and complexity. The widespread adoption of digital services, from payments and e-governance to online education and telemedicine, has created an interconnected environment where data flows continuously across networks. This transformation has been accompanied by the proliferation of devices and systems that collect and transmit data in real time.

Among these, camera systems and sensor-based networks are becoming increasingly embedded across urban infrastructure, industrial facilities and public services. Smart city surveillance systems, traffic management platforms and industrial monitoring solutions all depend on continuous data transmission to centralised platforms. While these systems significantly enhance efficiency and governance, they also underline the importance of ensuring that data flows remain secure, reliable and aligned with national priorities.

BUILDING INDIGENOUS AND TRUSTED LAYERS

Strengthening indigenous capabilities across this ecosystem, from devices and network infrastructure to data processing and storage, can help reduce dependencies and enhance resilience. This does not imply isolation, but rather the development of trusted, self-reliant systems that can operate effectively even under adverse conditions.

Another critical layer in this ecosystem is navigation and timing infrastructure. Telecom networks, transportation systems, financial platforms and emergency services all rely on precise positioning and timing signals. While global navigation systems have enabled seamless operations thus far, there is growing recognition of the importance of having robust indigenous alternatives.

In this regard, India’s navigation system, NavIC, represents an important strategic capability. Wider adoption of such indigenous systems across telecom networks and critical infrastructure can enhance reliability and reduce exposure to external dependencies, particularly in sensitive scenarios.

As networks evolve, intelligence is increasingly becoming embedded within them. Artificial intelligence is now playing a growing role in network management, optimisation, security and customer interaction. From detecting spam and fraudulent communications, something that has become particularly relevant in India’s high-volume messaging ecosystem, to enabling predictive maintenance and dynamic resource allocation, AI-driven systems are reshaping how telecom networks operate.

Strategic autonomy in telecom depends on strengthening indigenous capabilities across networks, data, and digital ecosystems.

In this context, developing capabilities within indigenous artificial intelligence ecosystems, including both Large Language Models and Small Language Models, is important. Localised AI systems, trained on relevant datasets and governed by domestic frameworks, can provide greater control, adaptability and security.

SECURING INFRASTRUCTURE ACROSS ALL LAYERS

Closely linked to this is the need for a secure and resilient data infrastructure. Data centres today form the backbone of the digital economy, hosting applications, platforms and services that support millions of users. For example, large-scale digital services such as Aadhaar and the DigiLocker platform depend on robust and secure data infrastructure to ensure uninterrupted access and trust.

As dependence on these systems increases, ensuring their protection becomes critical. Global practices offer useful insights. High-security facilities developed by organisations such as CERN demonstrate the importance of designing infrastructure that is robust, protected and capable of withstanding both physical and cyber risks.

For India, investing in geographically distributed, resilient and secure data centre infrastructure will be an important step toward strengthening digital continuity.

At the same time, it may be useful to adopt a layered approach to communication systems. While digital networks provide scale, speed, and flexibility, complementary systems, such as hardware-supported or offline-capable communication mechanisms, can offer additional resilience. Analogue or semi-analogue fallback systems, though less prominent in everyday operations, can serve as critical backups in the event of disruptions.

Reducing reliance on external dependencies is another important consideration. Elements of global internet infrastructure, including domain name systems governed by organisations such as ICANN, form a foundational layer of digital communication. Ensuring that critical services remain accessible and resilient, even in the face of external disruptions, requires a thoughtful, balanced approach to these dependencies.

Physical connectivity infrastructure also warrants attention. Undersea cables, which carry a significant portion of global data traffic, are essential to international communication networks. These cables traverse sensitive and strategically important regions, including the Strait of Hormuz and the Suez Canal. Given their importance, enhancing the protection, redundancy and monitoring of such infrastructure is increasingly relevant in the context of evolving global dynamics.

These evolving risks also extend to the semiconductor layer, where dependence on globally concentrated chipset supply chains and external design ecosystems can create vulnerabilities, underscoring the need for greater indigenous capabilities in telecom hardware and chip design.

Taken together, these developments suggest the need for a gradual recalibration in how telecom is perceived within policy and regulatory frameworks. Beyond its economic contribution, telecom plays a foundational role in enabling the functioning of multiple sectors and supporting national resilience.

Recognising telecom as critical infrastructure in India can help facilitate access to appropriate support mechanisms, encourage long-term investments and strengthen the overall ecosystem. This includes enabling policies that promote infrastructure expansion, foster innovation and support the development of indigenous capabilities across key technological domains.

India's telecom sector has already demonstrated its ability to connect at scale and support a rapidly growing digital economy. The next phase of this journey may well be defined by how effectively the country enhances the resilience, security, and autonomy of its communication systems while remaining integrated with the global ecosystem. 🌐

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

feedbackvnd@cybermedia.co.in

PCQUEST APRIL 2026 EDITION THE AI PC RECKONING: Why half your enterprise laptops may already be obsolete

ALSO READ MORE ON

- The rise of intelligent desktop: What consumers now expect from a home PC
 - Choosing an AI laptop in 2026: What really matters
 - What nobody tells you about using AI
 - Top 10 Mac games you should be playing
- Trust as a system property: Designing verifiable supply chain platforms with AI
 - REVIEW: Infinix Note Edge 5G | ORAL-B iO9 | Logitech MX Master 4



Scan QR Code
& Subscribe now...

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

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

FOLLOW PCQUEST FOR THE REGULAR
UPDATES ON TECH AND TRENDS

 @pcquest  @pcquest  @pcquest

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

For Subscription queries::

 subscriptions@cybermedia.co.in

 9289870545



THE AI SURGE

CAN INDIA HOLD ITS GROUND?



India's AI infrastructure is expanding at speed, but constraints on power availability, orchestration, and access will determine whether this surge can sustain itself.

BY PRATIMA HARIGUNANI

The journey is tempting. The tracks are being laid out. As India's AI Railroads throb to life, a lot is happening to ensure the tracks are in the right place and ready for the speed and load they will carry.

From the ballasts of data centres, to the sleepers of hardware, to the fishplates of fibre, to all the coal, couplers and axles of the processor muscle that fires up these wagons—everything is coming together, and quite fast and furiously.

Almost every major hyperscaler has either established a presence in India or is in the process of doing so. The country's AI and digital infrastructure landscape is witnessing investments estimated at USD 67.5 billion from hyperscalers, including approximately USD 17 billion from Microsoft, USD 15 billion from Google, a 500 MW data centre planned by Meta, and USD 35 billion announced by Amazon across various AI domains, among others.

Consider Deloitte's TMT Predictions 2026. India's data centre capacity is projected to scale from approximately 1.5 GW in 2025 to around 10 GW by 2030. In parallel, supporting the country's AI trajectory is the rapid expansion of its semiconductor market, which is expected to reach approximately USD 120 billion by 2030 and around USD 300 billion by 2035. This reflects a growth of nearly 20% CAGR, alongside an estimated USD 50 billion in additional capital investment over the next five years.

Facility build costs, excluding IT hardware, are expected to remain in the range of approximately USD 5.5–8.0 million per MW, underscoring India's structural competitiveness in adding new capacity.

AI INFRA SHIFTS FROM SCALE TO CAPABILITY

The current AI infrastructure landscape is transitioning from a phase of capacity build-out to one of capability alignment, observes Gopi Sirineni, Founder and CEO of Axiado, a cybersecurity and semiconductor startup focused on next-generation hardware security in India.

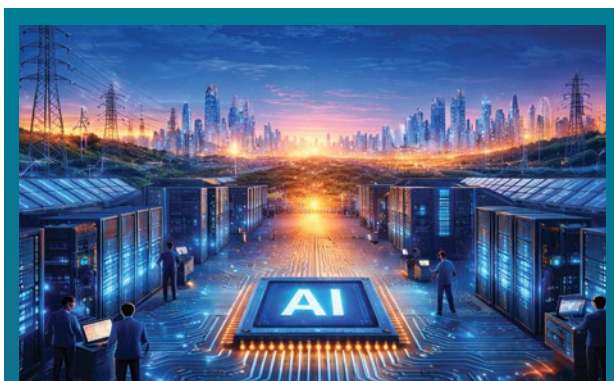
India's AI expansion is reshaping enterprise behaviour, as infrastructure confidence rises and organisations begin committing to production-scale AI deployments.



“India must build sovereign AI capabilities, leveraging its data strength through secure, localised infrastructure to unlock long-term value.”

RANGANATH SADASIVA

CTO, HPE India



IN BRIEF

- India's AI infrastructure is expanding rapidly, but the shift from capacity build-out to capability alignment will define long-term outcomes.
- Data centres are moving to high-density racks of 50–150 kW, increasing pressure on power, cooling, and facility design requirements.
- Hyperscaler investments are accelerating scale, but gaps in orchestration and utilisation are limiting enterprise AI adoption at scale.
- Power availability, water use, and land demand are emerging as structural constraints as AI workloads increase infrastructure intensity.
- The real bottleneck is not compute access but usability, as enterprises struggle with data readiness, integration, and workload orchestration.
- Sovereign AI, local infrastructure, and regulatory shifts are becoming critical as data control and geopolitical factors shape the ecosystem.

“Over the past 12–18 months, there has been visible momentum across AI-ready data centres, GPU cluster deployments, and fibre expansion, driven by both hyperscalers and domestic players. What is changing now is the nature of demand. Enterprises are no longer looking at AI as experimental workloads, but as production systems that require predictable performance, low latency, and secure compute environments.”

Deloitte has predicted that India's technology infrastructure will be defined by rising digital demand and the physical build-out required to support AI-led compute, cloud adoption and data localisation. There will be a rapid expansion of data centre capacity to serve AI and cloud workloads, and a parallel acceleration of the domestic semiconductor ecosystem to reduce reliance on strategic imports and capture more value across the electronics stack.

At present, India has developed two broad categories of data centres, according to Jackie Lee, CEO of Altos Computing. “Many of these facilities have been built domestically with extremely large capacities, and several of them meet global standards in terms of infrastructure and capability.”

Arjun Nagulapally, CTO of AlonOS, assesses India's infrastructure build-out from both supply and demand perspectives. According to him, the ambition on the supply side is undeniable.

“Significant capital is flowing into hyperscale data centre capacity across cities such as Chennai, Mumbai, Hyderabad, and Pune. GPU cluster announcements are becoming increasingly routine. Fibre rollouts under BharatNet, along with expansions by private operators, are materially improving both backbone and last-mile connectivity,” he explains.

Nagulapally further adds: “Power density per rack, a true litmus test of AI readiness, is now emerging as a



“For technology to create a better world, it has to work together, but the software part is lacking, even as infrastructure is moving well.”

SERGIO GAGO
CTO, Cloudera

design-first consideration rather than an afterthought. These developments represent real, structural shifts.”

The need for data sovereignty for the most populous country in the new world order is also a strategic enabler for this, underlines Prof Nityesh Bhatt, Director and Dean (I/C) at the Institute of Management in Nirma University.

He highlights that governments have realised the importance of real-time availability of mission-critical data and innovative AI models for Indian needs. “In the last few years, the Government of India and various state governments have devised progressive policies, financial incentives and regulatory measures for data centres and high-performance computing,” he points out.

Sirineni indicates that AI-ready data centres are increasingly being designed for high-density workloads, with racks optimised for accelerated compute rather than traditional enterprise IT. “GPU clusters are becoming more accessible, but orchestration, utilisation efficiency, and cost management remain key challenges,” he says, adding that fibre expansion is improving interconnectivity. Still, the real shift is towards distributed compute architectures where processing is closer to where data is generated, rather than being centralised.

A key transition is underway toward large-scale GPU clusters and accelerated compute environments, driving a shift from conventional 5–10 kW racks to high-density

deployments of 50–150 kW and beyond, notes CR Srinivasan, Chief Executive Officer, Digital Connexion. “This steep change in density is fundamentally reshaping facility design, requiring advanced power distribution, higher floor loading, and digital infrastructure that can support next-generation compute from the outset.”

Hyperscalers are adding significant sub-ballast to these new railroads.

Hyperscaler investments are accelerating the pace of AI infrastructure development and scaling in India, underscores Sirineni. “They are setting benchmarks for high-density compute, advanced cooling systems, and energy-efficient data centre design. This is pushing the broader ecosystem, including colocation providers, enterprises, and infrastructure partners, to evolve faster and align with these new standards.”

When Microsoft, Google, and AWS make multi-billion-dollar commitments to Indian data centre regions, it does not merely add capacity; it alters the psychology of enterprise AI adoption, as Nagulapally explains. “CIOs who were on the fence about committing to AI at scale are now making decisions with greater confidence, because the question of infrastructure sovereignty risk is being addressed.”

POWER, DENSITY PUSH INFRA TO THE EDGE

There will be many questions, side effects, and derailment



“Concerns have already been raised about the pressure hyperscale facilities place on shared utilities such as electricity and water in several regions globally.”

JACKIE LEE
CEO, Altos Computing



“Enterprises are no longer looking at AI as experimental workloads, but as production systems that require predictable performance and secure compute.”

GOPI SIRINENI

Founder & CEO, Axiado

INDIA'S AI BUILD-OUT: SCALE MEETS STRUCTURE

COMPUTE INFRASTRUCTURE SCALE-UP

IndiaAI Mission has deployed over 38,000 GPUs, with another 20,000 planned, bringing the installed base to over 80,000 GPUs across India.

DATA CENTRE CAPACITY EXPANSION

Operators such as STT GDC, CtrlS, Sify, Nxtra and PDG are expanding capacity across cities to support AI workloads and high-density compute demand.

AI CLOUD ECOSYSTEM BUILD-OUT

GPU cloud providers like Yotta, NxtGen and Neysa are building specialised AI compute platforms, enabling enterprises to access scalable GPU infrastructure.

NATIONAL CAPACITY GROWTH TRAJECTORY

India's data centre capacity is expected to grow from about 2 GW today to 8–9 GW by 2030, reflecting a strong shift towards AI-ready infrastructure.

ENTERPRISE AND STARTUP ADOPTION BASE

India has over 1,800 GCCs, with 500+ focused on AI, while nearly 89% of new startups are integrating AI into their products and services.

POLICY AND PUBLIC INVESTMENT PLANS

The Union Budget 2025–26 allocated Rs 500 crore for an AI Centre of Excellence in Education, signalling sustained focus on capability building.

SEMICONDUCTOR INVESTMENT PUSH

India's semiconductor sector could attract USD 50 B over five years, with USD 30–35 B for fabs and OSAT, and USD 15–20 B for the value chain.

HYPERSCALER INVESTMENT MOMENTUM

Microsoft will invest USD 17.5 B by 2029 to expand its AI infrastructure, while Amazon plans to invest USD 35 B by 2030 to drive AI-led growth and jobs. telecom networks help reduce latency while supporting distributed AI and IoT deployments.

risks as India lays down these expansive and ambitious AI tracks ahead.

For one, this expansion will, as Deloitte warns, intensify demand for land, power, and cooling as AI

workloads increase, raising rack densities and intensifying infrastructure per MW of IT load. This could also drive the sector's electricity demand to approximately 57 TWh by FY2030, increasing data centres' share of global electricity consumption from about 0.8% to nearly 2.5–3%.



“CIOs who were on the fence about committing to AI at scale are now making decisions with greater confidence as infrastructure risk is addressed.”

ARJUN NAGULAPALLY

CTO, AlonOS

Sustainability will not be a footnote but a defining priority as India builds its AI foundations. India's average Power Usage Effectiveness (PUE) could be around 1.9, compared with approximately 1.3 for best-in-class designs. Deloitte identifies this as meaningful headroom to reduce unit energy consumption through liquid-ready architectures, higher-efficiency power trains, and continuous metering and control systems.

Lee explains how, with the rapid growth in CPU- and GPU-driven workloads, particularly those related to AI, the demands on power and water resources for data centres are increasing significantly. “In several regions globally, including parts of the United States, concerns have already been raised about the pressure hyperscale facilities place on shared utilities such as electricity and water. India also faces structural constraints in terms of electricity availability and water resources.”

Pankaj Malik, CEO and Whole-time Director, Invenia-STL Networks, adds that energy is emerging as a strategic design lever. “Leading data centre operators are moving beyond traditional power models to adopt hybrid energy strategies, integrating grid supply with renewable PPAs, on-site solar, and intelligent energy management systems to optimise efficiency and actively reduce carbon intensity at scale. We are also advancing smarter power management and evolving cooling strategies to help operators scale sustainably

without compromising on performance, resilience, or cost efficiency,” he says.

One challenge that demands the government's attention is the substantial water and electricity required to power this infrastructure, Dr Bhatt says. “Without addressing this, it can invite numerous societal confrontations. Rapid skill-building is also the need of the hour.”

Aggregate data centre land requirements are expected to expand by an additional 45–50 million sq. ft. by 2030, up from approximately 13 million sq. ft. in 2023. And as Sirineni avers, the increase in AI compute capacity is also bringing operational challenges.

According to him, “High-performance AI workloads demand significantly more power and generate more heat, making power availability, cooling efficiency, and sustainability critical considerations rather than secondary concerns.” He further notes that the integration of renewable energy is becoming a strategic necessity, not just for compliance but for long-term cost and scalability.”

Malik also addresses how connectivity is becoming mission-critical. “AI workloads generate massive east-west traffic across GPU clusters, storage, and distributed data centres, making high-capacity, low-latency fibre networks a foundational requirement. India is steadily building this digital backbone to support the next phase of AI-led innovation and domestic compute capacity.”



“Leading data centre operators are moving beyond traditional power models to adopt hybrid energy strategies integrating grid supply with renewable PPAs.”

PANKAJ MALIK

CEO, Invenia-STL Networks



“Governments have devised progressive policies, financial incentives and regulatory measures for data centres and high-performance computing.”

PROF. NITYESH BHATT

Director & Dean (I/C), Institute of Management, Nirma University

Nagulapally explains the ripples here. “High-density AI compute, particularly GPU clusters running inference workloads at scale, generates heat loads that older data centre designs simply were not built for. The move toward liquid cooling, immersion cooling, and intelligent thermal management is not optional; it is a prerequisite for running serious AI workloads reliably.”

There are many other bumps on this track as well, and most will only pop up on the radar when the train starts moving.

ORCHESTRATION GAPS STALL AI OUTCOMES

The ground reality, as Nagulapally notes, is more complicated. “The bottleneck is rarely raw compute anymore. It is the gap between infrastructure availability and infrastructure usability. Enterprises have access to GPU capacity through cloud providers, co-location, or direct procurement, but most cannot consume it efficiently because their data and integration layers are not ready. A world-class GPU cluster sitting behind a siloed legacy stack does nothing for you.”

Lee argues about the part where utilisation overshadows capacity layouts. “A significant portion of this infrastructure is still not fully accessible to the wider public ecosystem. Researchers, students, and several government-led public applications could benefit far more from these resources if they were made available more broadly.”

A large share of existing data centre capacity remains underutilised for such public and research-driven use cases, contends Lee. “If these high-performance compute facilities were made accessible at more affordable costs to students, research institutions, and public-sector initiatives, the infrastructure already created by private organisations could reach a much wider set of users.”

Sirineni puts the torch on another key aspect. “From a backend perspective, the complexity is not just in scaling compute, but in managing and securing it. As AI infrastructure becomes more distributed and heterogeneous, the control plane becomes critical. This is where we see a gap in the current ecosystem. While compute capacity is expanding, there is a growing need for intelligent, hardware-level control and security mechanisms that can manage AI workloads efficiently and securely across environments.”

Sergio Gago, CTO of Cloudera, reckons that a lot of work is happening in India on AI builds and infrastructure—especially with focus on inclusivity, accessibility and citizen services, where the country is going great. “For technology to create a better world, it has to work together. The software part is lacking. Remember, it is still a four-year-old technology. The solid part is moving impressively well. There is still a lot of work to do—from ground-up decisions to sustainability to accessibility.”



“High-density AI workloads are redefining facility design, requiring advanced power systems, higher floor loading, and AI-ready infrastructure.”

CR SRINIVASAN

CEO, Digital Connexion



“Enterprises are very keen on sovereignty, and we are seeing the emergence of local data centre capabilities beyond superficial compliance.”

DD MISHRA

VP Analyst, Gartner

Nagulapally also underscores the role of software in this transition. “India has the compute. India has the fibre. What we still need to scale is orchestration intelligence—the ability to route AI workloads intelligently, manage cost and latency trade-offs in real time, and govern AI behaviour in production. That is not a hardware problem; it is a software and systems-thinking challenge, and it is where the real competitive differentiation will be won.”

SOVEREIGNTY AND ACCESS DEFINE THE NEXT PHASE

Thankfully, India’s formula is not just about scale. As articulated by the government and reflected in updates on the specially carved Rs 10,300+ crore IndiaAI Mission, the country’s approach emphasises inclusivity and cost-effectiveness.

In many markets, advanced AI infrastructure remains concentrated in the hands of a few corporations, shaping who gets to innovate. India, however, is building a different model—one that expands access and enables responsible AI for the public good. Under the Mission, more than 38,000 high-end GPUs have been made available at Rs 65 per hour, lowering compute barriers for startups, researchers, students, and public institutions.

There is also encouraging momentum in renewable integration. Several large data centre operators in India are committing to green power procurement, which matters both for sustainability goals and for operational cost predictability over a 10-year horizon, notes Nagulapally.

Lee is similarly optimistic that initiatives such as the India AI Mission are enabling these shifts by promoting models of public–private collaboration that can make advanced computing infrastructure more widely available at lower cost. When such resources become genuinely accessible to a broader ecosystem, India is likely to experience a stronger and more widespread AI-driven transformation.

Nagulapally reasons that India’s AI infrastructure foundation is being laid faster than many anticipated. However, the enterprises that will ultimately extract value from it will be those investing equally in their data fabric and AI orchestration layers, rather than focusing solely on compute procurement.

AI and data sovereignty have moved beyond theoretical discussions, notes DD Mishra, VP Analyst at Gartner. “It is an emerging risk at this point in time. Client conversations show that enterprises are very keen on sovereignty, as evidenced by the last few months. The reality is settling in now, and we are seeing the emergence of local data centres and capabilities that go beyond superficial compliance. Regulatory forces and geopolitical dynamics will also influence this space significantly—for example, the Pax Silica agreement.”

Ranganath Sadasiva, CTO, HPE India, reinforces this perspective. “While it is anticipated that hyperscalers and large model developers will leverage a significant share of this capacity, there is a critical need for India to focus on building sovereign AI capabilities. With the nation generating nearly 20% of the world’s data, developing localised, secure, and self-reliant AI infrastructure is essential to unlock its value and ensure data sovereignty fully.”

Data sovereignty is a strategic enabler for India, but it will require sustained effort and a significant long-term resource commitment, as Dr Bhatt encapsulates.

Let us not forget that despite all its power and technological edge, the American steam locomotive Tom Thumb once lost a race to a horse-drawn carriage due to a mechanical failure. Any belt can slip off any blower pulley in today’s AI locomotive as well, especially when the race is no longer with what was, but with what is coming. 🚂

pratimah@cybermedia.co.in



ARUNAV ROY
SVP & Business Unit Head – Connectivity, Cyient

“AI is enabling networks to self-learn and optimise in real time”

Arunav Roy, SVP and Business Unit Head – Connectivity at Cyient, brings over two decades of global experience across telecom, media, and technology, with a strong track record in 5G, network transformation, and next-generation infrastructure strategy. In his current role, he leads Cyient’s connectivity, utilities, and spatial intelligence businesses, driving lifecycle-led engineering and AI-driven network modernisation across global markets.

In this conversation with Shubhendu Parth, he discusses how telecom operators are moving beyond infrastructure build-out towards intelligent, outcome-driven networks. Roy explains Cyient’s approach to embedding intelligence across planning, design, deployment, and operations, the role of open architectures and rApps in enabling network programmability, and why enterprise use cases and automation will define the next phase of telecom monetisation. Excerpts:

Cyient has deep engineering capabilities across connectivity and infrastructure. How are you now aligning this legacy with emerging network transformation demands?

Cyient is a publicly listed company with over 30 years of deep engineering heritage and a strong global presence. We are a 16,000-plus-employee organisation operating across major geographies. Over the years, we have deepened our engineering capabilities and expanded into specific customer segments—connectivity, transportation, energy, mining, utilities, and geospatial. What has really differentiated us is our ability to solve core

engineering problems and build long-term relationships around business outcomes.

From a structure standpoint, we are increasingly aligning ourselves around industry verticals and lifecycle capabilities. In my role, I lead connectivity, utilities and spatial intelligence. The idea is to bring a full-stack, lifecycle view—right from infrastructure and network layers up to AI-driven outcomes—and see how we can create meaningful impact across that value chain.

Analysts argue that incremental upgrades may no longer be sufficient for the next phase of telecom-sector growth. Does the industry now require a deeper network transformation?

If you look at the journey of telecom networks over the last four decades, every eight to ten years there has been a major technology shift—2G to 3G, 3G to 4G, 4G to 5G. But for the first time, we are seeing that cycle stretch out with 5G to 6G.

So instead of jumping to the next generation, telcos are now focusing on extracting outcomes from 5G. The reason is that they have not yet realised even 30–40% of the ROI from those investments. The immediate priority is—how do we solve meaningful use cases and monetise what has already been built?

At the same time, the pace at which AI is coming in is forcing the industry to rethink. It is pushing telcos to assess their infrastructure readiness and how they can

AI has to be made meaningful, not a buzzword, driving intelligent engineering, autonomous networks and cognitive operations across the lifecycle.

create more monetisable assets. That is where open architectures are becoming important.

If you take a global view, telcos are broadly working around three priorities—continuing to build fibre infrastructure, reducing OPEX through AI-led efficiency, and improving monetisation by opening up networks to enterprise use cases.

Many operators still approach network upgrades as technology refresh cycles. What differentiates intelligent network modernisation from traditional upgrade cycles?

Because of our 30-plus years of experience in this domain and our work with tier-one telcos globally, we have come to understand what really matters to them. One thing we realised is that AI has to be made meaningful—it cannot just remain a buzzword. So, we reframed our approach and defined what we call intelligent network modernisation. We look at it in three layers.

The first is intelligent network engineering—how do we use AI to make planning and design cycles more effective, whether for fibre or wireless deployments, and how do we optimise infrastructure?

The second is autonomous networks—how do we define a roadmap for L3 and L4 autonomy, what kind of RIC ecosystem is needed, and how we work with OEMs like Ericsson, Nokia, Samsung and others. This is also where rApps and xApps come into play. This space itself is trending towards a USD 700–800 million opportunity.

The third is cognitive operations. This is where everything comes together—our global delivery footprint, our IP, and platforms like WISMO AI. The focus here is on outcomes—energy efficiency, configuration management, and fault detection and resolution.

We also bring in vendor-agnostic capabilities, a strong data foundation, and our own LLM layer on top. So, it is not just a technology refresh—it is a lifecycle-led, outcome-driven transformation.

Cyient is positioning intelligence across the entire network lifecycle. How does embedding AI across the network lifecycle change the way networks are built and managed?

Fundamentally, the biggest shift has been from closed ecosystems to open ones.

Earlier, telecom networks were largely controlled by one or two vendors. Now, architectures are becoming more open, APIs are exposed—it is almost like a marketplace. That is where innovation is happening, and monetisation can happen on top of it. This openness allows multiple players to come in and apply AI across different layers of the network.

Also, for a long time, telcos were essentially communication backbones. Now, enterprise use cases are becoming central to how networks are designed and monetised. When you embed AI across the lifecycle—from planning and design to operations—you move towards networks that can monitor themselves, optimise themselves, and increasingly take decisions in real time.

Despite rapid deployment, 5G monetisation remains challenging for many operators. Is it a transition phase before the real impact of 6G?

That is a very interesting point of view. But at the end of the day, from an end-user standpoint, what is the real difference you have experienced? 4G already gave us the bandwidth we needed, and the device has largely remained the smartphone. So, from that lens, the impact has not been very visible.

But from an industry standpoint, 5G has always been about enabling future use cases—holography, digital twins, AI-driven workloads. Today, even a single AI query is generating a huge amount of data, and the backbone is still not fully tuned to handle that scale.

So, slowly and steadily, we are moving in that direction. Enterprises are beginning to use these capabilities—autonomous vehicles, remote engineering, real-time cross-domain operations, and simulation models for diagnostics. These use cases will pick up momentum over time.

Can these interventions improve monetisation for telecom operators?

If you look at it from an efficiency and cost-saving standpoint, yes, this is definitely a strong play. But there is another dimension to this. I was recently at the Mobile World Congress, and one thing that was clearly emerging is that while data has been the foundation layer and cloud has enabled distributed infrastructure, as AI adoption increases, a clear use case will be for more secure and reliable networks.

Autonomous networks are evolving through rApps, open architectures and AI, enabling continuous optimisation, faster deployment and real-time operations.

It is a slightly different way of looking at it. There have always been concerns around cybersecurity, but if you have AI agents continuously working on the network—crawling it, monitoring it—that actually strengthens resilience at the core.

As far as ARPU is concerned, the real impact comes from monetisation. Open network architectures allow telcos to embrace newer use cases. It is about opening up the pipe for enterprises, and that is where the overall revenue return comes from.

What structural shifts are required to unlock new revenue streams? Where do you play in that value chain?

This is really an ecosystem play. Companies are working on infrastructure—data centres, network infrastructure. Players are coming in with application-level interventions. Others are working on services, and then there are companies that are focusing on operations. We play across the services and operations stack, focusing on helping telcos stitch the network fabric sooner, faster, better, more reliably, and more future-ready.

The second dimension is how we drive tangible outcomes—efficiency on the network side, efficiency in rollout, and greater autonomy. How do we help them monitor and optimise their networks in real time through our platforms and the IP we have built over the years? And how do we align that to a three-to-five-year outlook?

Earlier, we were operating on more discrete building blocks. Now, we are trying to augment the entire value chain—especially on the wireless side—through platforms like WISMO, Cyient's AI-led wireless network operations stack, and a lifecycle-driven approach.

How are rApps and xApps reshaping service innovation and the developer ecosystem?

This is where the industry is heading, and it ties directly into the autonomous networks play. We are working closely in accordance with the TM Forum guidelines. Not all telcos are at the same level—some are at L2.5, some

are moving towards L3—but the journey from L1 to L4 is clearly being defined.

If you peel the layer, what has really changed is that OEMs have started opening up their stacks. Ericsson, Nokia, Samsung—they all now allow third parties to build on their platforms. There was even an announcement that Ericsson and Nokia will support each other's rApps. That has fundamentally changed the play—it is now an open ecosystem.

That is where we are also playing. We have identified around 20 rApps, but we are very focused—prioritising the most pressing use cases in network assurance, configuration management, fault management, and energy efficiency.

What practical steps must operators take to move from pilots to autonomous networks?

The shift is already underway. Looking at the last couple of years, there was a lot of hype. But now, especially at MWC, you could clearly see a shift towards demonstrable use cases and measurable outcomes. The transition has already started. Implementations are happening globally.

Tier-one telcos are taking different approaches. Some are going with a focused single-vendor strategy and building ecosystems around that. Others are going multi-vendor, where they need a vendor-agnostic layer to stitch everything together. Also, SMO interoperability is becoming critical. Network-as-a-product is enabling new models, such as network slicing, that can drive enterprise monetisation.

Another important thing—we have to recognise that AI is enabling networks to self-learn. It is like an agent working 24/7 across the system. So, the pace of change is no longer in years or months—it is happening much faster, possibly in days. That is where we are heading. 🧠

To **read and listen** to the complete interview, **click** <https://bit.ly/4tyD5gz>.

shubhendup@cybermedia.co.in



VIJAYAKUMAR ARUMUGA NADAR
Chief AI Officer, NeevCloud

“Orbital data centres are the next evolution of AI infrastructure”

India's AI ambitions are increasingly tied to infrastructure—compute, data centres, and the networks that bind them. Yet, as AI workloads grow denser and more latency-sensitive, terrestrial constraints around power, cooling, and geography are becoming harder to ignore.

Vijayakumar Arumuga Nadar, Chief AI Officer, NeevCloud, is at the forefront of exploring what could become India's first orbital AI data centre, in partnership with Agnikul Cosmos. In this conversation with Pratima Harigunani, he sheds light on the architectural thinking behind space-based AI infrastructure, the realities of latency and sovereignty, and the engineering and regulatory challenges that lie ahead. Excerpts:

What is driving the idea of a data centre in space? How does it differ from terrestrial infrastructure?

An orbital data centre represents a long-term evolution of AI infrastructure architecture. AI workloads are increasingly power-dense and thermally intensive. Terrestrial data centres face constraints related to land availability, grid dependency, cooling resources, and carbon intensity.

Space offers potential advantages such as continuous solar exposure, depending on the orbit, and physical isolation for highly sensitive workloads.

From a design perspective, what does such an orbital data centre look like?

From a technical perspective, there are many aspects. The power architecture would rely primarily on solar generation, supported by energy storage systems. Cooling would use radiative heat rejection instead of air or water-based systems.

Hardware would need to be optimised for radiation tolerance and autonomous operations. Software would require high fault tolerance and intelligent remote orchestration capabilities.

Traditional terrestrial PUE metrics may not directly translate to orbital environments, so efficiency will be measured differently. Early systems would be modular and designed for resilience rather than routine in-orbit hardware replacement.

We are currently evaluating feasibility models and phased deployment pathways, beginning with feasibility, payload engineering, and regulatory coordination.

Are there any global precedents or benchmarks you are studying?

At this stage, there is no known large-scale AI-optimised data centre operating in orbit, either in India or globally.

An indigenous orbital compute layer could reduce reliance on foreign hyperscale infrastructure and provide jurisdictional control over sensitive workloads.

Low latency is important, but the broader goal is to explore globally distributed, secure AI inference nodes that are independent of terrestrial constraints.

Some experimental edge-compute capabilities have been explored, but this remains an emerging frontier. While experimental edge-compute capabilities have been explored globally, this remains an emerging frontier for both space and AI infrastructure.

What role does Agnikul Cosmos play in this initiative?

Our collaboration with Agnikul Cosmos is focused on launch capability and indigenous access to space. Their role relates to launch and orbital deployment expertise. Data centre compute architecture, AI infrastructure design, and software intelligent orchestration remain within our domain at NeevCloud.

Low latency is often cited as a key benefit. How critical is it in this context, and what use cases are emerging?

Low latency is an important dimension, but it is not the only value proposition. Latency itself depends on orbit selection and the ground infrastructure topology. The broader objective is to explore globally distributed, secure AI inference nodes that are independent of terrestrial constraints. At this stage, we are in exploratory discussions across sectors such as defence, satellite data analytics, and sovereign AI workloads. Specific deployments and customer engagements will follow once formal agreements are in place.

What regulatory and environmental considerations come into play for such infrastructure?

Space infrastructure operates under strict regulatory frameworks. This includes national space authorisation and oversight, orbital debris mitigation planning, end-of-life deorbit strategies, and insurance and risk management compliance.

On environmental aspects, sustainability considerations—including debris mitigation and responsible orbital management—are central to our planning.

How does this initiative contribute to AI sovereignty?

AI sovereignty is about operational independence

and strategic control over compute infrastructure. An indigenous orbital compute layer could reduce reliance on foreign hyperscale infrastructure, provide jurisdictional control over sensitive workloads, ensure operational continuity during terrestrial disruptions, and support national strategic and defence use cases.

Sovereignty does not mean isolation alone; it means the ability to operate independently with full control as required.

What are the biggest challenges you anticipate in making this viable?

We fully recognise this is a complex, frontier initiative. NeevCloud's deep-tech focus enables us to approach such challenges with long-horizon engineering discipline and systems-level thinking.

Some key challenges include launch economics and payload optimisation, radiation-tolerant system design, autonomous fault management, insurance and regulatory frameworks, and long-term economic viability models for orbital inference.

We are approaching this with a phased roadmap, ensuring careful and responsible engineering validation at each step.

What excites you most about this frontier, and do you see spillover effects on terrestrial cloud and data centre markets?

What excites us most is the possibility of extending AI infrastructure beyond terrestrial boundaries, purpose-built for advanced AI inferencing workloads.

By exploring orbital edge inferencing, we aim to evaluate models that could support sovereign, distributed AI execution and, in certain high-sensitivity use cases, ultra-low latency responsiveness. 🌐

pratimah@cybermedia.co.in

Networks shift from connectivity to intelligence at scale

As AI, edge, and digital platforms scale, networks are evolving into deterministic, secure, programmable systems enabling real-time, high-reliability operations.



BY GP. CAPT. CS KRISHNADAS

India's telecom and enterprise networks are entering a phase where connectivity is no longer the primary benchmark of progress. As the country moves into 2026, infrastructure is evolving into systems that are secure, autonomous and programmable, capable of supporting context-aware operations and predictable performance across environments.

This transition is being driven by the scale of digital platforms, the expansion of artificial intelligence (AI) workloads beyond centralised data centres, policy focus on domestic technology capabilities, and the maturity of the global technology ecosystem aligned with India's requirements.

Training and inference workloads are no longer restricted to hyperscale environments. Across sectors such as manufacturing, logistics, healthcare and mobility, edge computing and multi-access edge computing (MEC)

are being deployed for applications including computer vision, telemetry and safety systems. These use cases require low-latency, lossless transport and local data breakout to ensure real-time responsiveness and minimise dependency on centralised backhaul networks.

EDGE AI RESHAPES NETWORK TRAFFIC FLOWS

The shift of AI workloads towards the edge is changing how networks are designed and operated. Instead of transporting large volumes of data to central clouds, processing is increasingly occurring closer to where data is generated. This reduces latency and enables immediate decision-making in environments where delays are not acceptable.

Factories, ports and logistics hubs are integrating edge inference systems that rely on deterministic network behaviour. These systems must support consistent throughput and minimal packet loss to maintain operational continuity. As a result, networks are being

Networks are being redesigned for assured performance, with latency, throughput, and reliability engineered parameters rather than variable outcomes.

required to deliver assured performance rather than best-effort connectivity.

At the same time, the demand for local breakout capabilities is increasing. This allows data to be processed within proximity to the source, avoiding unnecessary routing through distant data centres. The combination of edge computing and deterministic transport is becoming central to enterprise network architectures.

DIGITAL PLATFORMS DRIVE SCALE AND TRUST

India's digital public infrastructure is contributing significantly to network demand. Platforms such as Aadhaar, Unified Payments Interface (UPI), DigiLocker, Ayushman Bharat Health Account (ABHA), and Open Network for Digital Commerce (ONDC) operate at a population scale, generating continuous traffic and requiring high reliability.

These systems are associated with identity verification, financial transactions, healthcare records, and digital commerce, all of which demand secure, real-time network performance.

Use cases are emerging that place additional requirements on network capabilities. For instance, live commerce applications require consistent video quality, while digital health records require strong encryption and secure access frameworks. This combination of scale and sensitivity is pushing networks to incorporate trust mechanisms by design.

The requirement for deterministic connectivity is also expanding into sectors such as connected mobility and operational technology (OT) networks. These environments depend on predictable performance and policy-driven network behaviour. Identity-based segmentation and assured quality of service (QoS) are becoming essential to ensure that applications function within defined parameters.

ACCESS NETWORKS EVOLVE FOR PERFORMANCE NEEDS

Changes at the access layer are enabling new performance benchmarks. Wi-Fi 7 operating in the 6GHz band is expected to deliver multi-link capabilities that improve

indoor performance consistency. In parallel, private 5G deployments are being adopted in industrial environments to provide controlled and predictable outdoor coverage.

Fibre access technologies are also progressing towards higher capacities. Architectures such as 50-gigabit passive optical network (50G-PON) are being introduced with capabilities that support coexistence and bounded latency. These developments enable fibre networks to handle converged workloads, including backhaul for wireless systems, video analytics and supervisory control and data acquisition (SCADA) systems.

In addition, 5G fixed wireless access (FWA) continues to play a role in extending connectivity to locations where fibre deployment is limited. This includes rural areas and buildings where fibre infrastructure is not yet available. The combination of fibre, wireless and private networks is creating a hybrid access environment designed to meet diverse requirements.

TRANSPORT AND DATA CENTRES ADAPT TO AI

Beyond the access layer, transport networks and data centre infrastructure are undergoing significant changes. At the transport level, coherent optical technologies are advancing, with higher-capacity pluggables such as 800G ZR and ZR+ being introduced at the IP edge. These systems are supported by telemetry capabilities that enable monitoring, optimisation and automated path adjustments.

In data centres, the requirements of distributed AI workloads are influencing network design. Lossless Ethernet using remote direct memory access over converged Ethernet version 2 (RoCEv2) is being deployed to reduce packet loss between compute nodes, improving the efficiency of training processes. Network infrastructure is being optimised to handle east-west traffic patterns characteristic of AI workloads.

Cloud-native principles are also shaping telecom core networks. 5G SA cores are transitioning towards containerised network functions operating on service-based architecture. These systems support automation across deployment and operations, enabling scalability and flexible service delivery.

Edge computing is reshaping traffic flows, bringing compute closer to data sources and enabling faster, context-aware decision-making across industries.

The use of network APIs is expanding, allowing operators to expose capabilities such as identity verification, device status, and quality-of-service controls to enterprises. This enables new service models in which network functions can be consumed programmatically.

Routing and switching platforms are evolving towards software-defined architectures. Network operating systems are adopting container-based models, supported by orchestration systems that manage operations across different lifecycle stages, including day-0, day-1, and day-2. Telemetry and analytics are being integrated to enable continuous optimisation of network performance.

Hardware platforms are also advancing, with higher interface speeds such as 800GbE and emerging 1.6T capacities, supported by (224) serialiser-deserialiser (SerDes) technologies and advanced digital signal processors. These developments support granular traffic management, enabling networks to handle diverse workloads efficiently.

SECURITY FRAMEWORKS INTEGRATE INTO NETWORKS

Security is becoming an embedded component of network infrastructure rather than an overlay. Approaches such as Zero Trust Network Architecture (ZTNA) are being integrated into network elements, enabling granular segmentation and policy enforcement. This reduces the potential impact of security incidents by limiting lateral movement within networks.

At the same time, Secure Access Service Edge (SASE) frameworks are combining connectivity and security functions into unified architectures. These models integrate software-defined wide area networking (SD-WAN) with cloud-delivered security services, supported by real-time monitoring and analytics.

The need to protect long-lived data is also driving the adoption of post-quantum cryptography strategies. Hybrid approaches are being considered to ensure that sensitive information remains secure against future threats.

Policy frameworks in India are influencing the direction of technology development. Initiatives related to trusted

sources and domestic manufacturing are encouraging the development of intellectual property across hardware, software and firmware. This includes areas such as semiconductor packaging, optical technologies and secure system design.

Sustainability is also becoming a consideration in infrastructure planning. Data centres and transport networks are adopting technologies to reduce energy consumption, including advanced cooling methods such as liquid cooling and more efficient optical systems.

To support this transition, several priorities are emerging for operators and policymakers. Deterministic connectivity is expected to be offered through defined service tiers, allowing enterprises to request specific performance characteristics. Transport networks are being upgraded to support higher capacity and to accommodate AI-driven traffic patterns.

The migration to cloud-native architectures is continuing, with a focus on automation and operational efficiency. Security frameworks are being strengthened through integrated approaches that combine network and security functions. At the same time, networks are extending beyond terrestrial boundaries, with non-terrestrial networks such as Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) satellite systems being considered to enhance coverage in remote and underserved areas.

Industrial wireless environments are adopting hybrid models that combine different access technologies, supported by edge computing, to meet latency requirements. Efforts to build domestic capabilities and improve energy efficiency are also shaping the sector's long-term direction.

India's network infrastructure is therefore moving towards a model in which programmability, reliability, and security are integral. The focus is shifting from expanding connectivity to enabling systems that can support complex, real-time and large-scale digital operations. 🌐

*The author is an Indian Air Force veteran and CEO of Umiya Buildcon.
feedbackvnd@cybermedia.co.in*



AI in networks: Speed up front, strain beneath the hood

Behind automation and predictive gains, AI in networks demands deep data integration, orchestration, and infrastructure upgrades to scale reliably.



BY PRATIMA HARIGUNANI

We thought it was a snowman, but it turned into a snowball. It is staggering how fast the glacial forces of Artificial Intelligence (AI) have melted and reached the farthest corners of the modern world's plains and islands. It was only reasonable to expect this force to flow into networks as well.

AI in networks is projected to reach USD 46.87 billion by 2029, according to MarketsandMarkets. Grand View Research estimates it will grow further to USD 60.60 billion by 2030. Nokia's recent global traffic report, produced with Bell Labs Consulting, adds another layer of insight. Even though 70% of global WAN traffic will still come from non-AI sources by 2034, AI traffic will represent the largest area of growth, expanding at 23% CAGR compared to 15% for non-AI traffic.

AI TRAFFIC SURGE AND DATA FLOW SHIFTS

The growing volume of AI-driven autonomous activity signals that 37% of total network AI traffic will be machine-generated by 2034. When combined with other traffic sources, this can easily trigger a threefold increase in inter-datacentre traffic. The addition of generative AI to this mix further intensifies the trend, as AI-enabled IoT systems amplify uplink traffic by continuously transmitting video streams and sensor data.

A GSMA Intelligence report from March 2025 observed that AI is making networks more intelligent, efficient, and cost-effective. Its role has evolved from task automation to optimising entire systems. Network operations, predictive maintenance, self-healing capabilities, and intelligent traffic management are already reducing downtime and improving cost efficiencies.



“AI is shifting networks from reactive fixes to predictive operations, improving uptime, lowering costs, and enabling autonomous network management at scale.”

SUMIT SARAWGI

India Head, Oliver Wyman

AI-driven capabilities such as dynamic traffic routing, intelligent load balancing, and automated congestion management are helping optimise performance while maintaining service quality.

The report also highlights AI's impact on the complex and costly domain of RAN management. The RAN, widely regarded as the most energy-intensive component of telecom infrastructure, accounting for 80–85% of total consumption, benefits significantly from AI-powered RAN Intelligent Controllers and traffic steering.

These capabilities enhance resource allocation, automate fault detection, and support sustainability efforts by reducing power consumption in network operations. Integrating AI into RAN operations also helps unlock downstream energy efficiencies.

AI RESHAPING NETWORK OPERATIONS AT SCALE

Sumit Sarawgi, India head of Oliver Wyman, echoes these directions: “As highlighted in Oliver Wyman's recent report, AI is already reshaping core network operations, from predictive maintenance and network optimisation to automated root cause analysis and increasingly autonomous network operations centres.”

These use cases are helping operators move from reactive to preventive network management, with tangible impact such as faster incident resolution, improved network uptime, and 20–40% optimisation in network capex and opex.

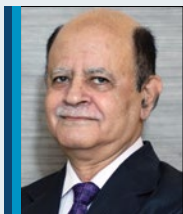
AI is also creating significant value by transforming telecom networks into what Lt Gen Dr SP Kochhar (Retd), Director General, COAI, describes as a “value-added horizontal” that enables innovation across sectors.

“In this framework, telecom networks act as the foundational layer over which AI-led applications across governance, healthcare, agriculture, education, and industry are delivered at scale. Within network operations,



IN BRIEF

- AI traffic is set to outpace traditional flows, driven by machine-generated data and GenAI-led workloads across networks and data centres.
- AI is shifting networks from reactive operations to predictive and autonomous systems, improving uptime, efficiency, and incident response cycles.
- RAN optimisation through AI can reduce energy consumption while improving resource allocation, making networks more sustainable and cost-efficient.
- The real bottleneck is not AI models or compute, but fragmented data layers and a lack of orchestration across network systems and workflows.
- Scaling AI across the network lifecycle requires strong data foundations, measurable outcomes, and a careful balance between automation and oversight. Mission-critical networks demand explainable AI, auditability, and human override, shifting focus from capability to accountability in deployment.



“Telecom networks are evolving into a value-added horizontal, enabling AI-led applications across sectors and strengthening their role as digital infrastructure.”

LT. GEN. DR. SP KOCHHAR
Director General, COAI



NUMBERS BENEATH AI'S RISE

- 53% of operators believe generative AI will have the greatest impact on network planning and optimisation
- 80% of operators are prioritising revenue-generating activities over cost-centric approaches
- Improving customer experience and enabling new services outweigh opex and capex savings by a four-to-one margin
- 15% of operators expect increased data traffic to be the most immediate network impact of generative AI
- 63% of operators are investing in AI-led workforce upskilling, closely followed by 62% focusing on network capacity expansion

AI is already being used for predictive maintenance, intelligent network planning, and rollout optimisation, enabling operators to anticipate lapses, enhance uptime, and manage growing data traffic more efficiently,” he says.

From a practitioner’s perspective, the future is not distant. Arjun Nagulapally, CTO, AlonOS, points out that while AI in networks is often framed as a future state, the reality is that it already exists in production

environments. “Everyone talks about AI in networks as a future state. From my perspective, building systems that actually operate in production across complex network environments, the future is already here, it is just unevenly distributed and, frankly, unevenly understood.”

FROM EFFICIENCY GAINS TO STRATEGIC ROLE

AI’s advantages extend beyond operational efficiency. It allows telecom infrastructure to support new digital business models and sectoral transformation, thereby reinforcing its role as an economic multiplier rather than merely a connectivity utility. Kochhar further notes, “AI-led optimisation of telecom networks can improve spectral efficiency by about 10%, potentially helping operators manage congestion without additional airwaves.”

The long-term vision of autonomous networks is also taking shape. Abdu Mudesir, Member of the Board of Management, Deutsche Telekom (DT), Product and Technology, notes, “AI will transform networks to be more proactive and have a rapid response, increase its resilience and reduce exposure to outages and faults. We combine an approach to tackle high-value use cases and, in parallel, transform complete business processes to maximise the value return.”

There is more than mere efficiency and money that come along with AI—it strengthens trust and security at the network level. Kochhar explains, “AI is also strengthening trust and security at the network level. AI-enabled systems can detect fraudulent activity, spam and anomalous traffic patterns in near real time, protecting consumers and improving confidence in digital services.”

To take this forward, the Department of Telecommunications has developed an indigenous AI and Big Data Analytics tool, ASTR, to identify SIMs issued to the same person under different names. Based on ASTR, a large number of mobile connections have been disconnected due to non-verification. “As AI adoption deepens across industries, telecom networks



“AI will make networks more proactive, resilient, and responsive, while transforming business processes to maximise value from network operations.”

ABDU MUDESIR

Former Member – Board of Management, Deutsche Telekom (Product & Technology)

are evolving into a strategic national infrastructure that enables inclusive digital growth,” Kochhar adds.

Mudesir provides a practical example of this transformation: “Our RAN Guardian Agent, powered by Gemini, is already supporting teams in DT’s live mobile network in Germany for a better customer experience. During high-impact events or sudden traffic surges, it continuously monitors network behaviour, identifies emerging performance issues, and autonomously triggers corrective actions within minutes”. In live operations, it has reduced the time needed to manage major events from hours to around a minute, a more than 95% improvement.

AI IN NETWORKS: THE CLOGGED PARTS

The journey is not entirely smooth, nor is it free of obstacles. AI in networks may solve long-standing problems, but it also introduces new challenges.

Sarawgi points out that much of this value remains concentrated in isolated use cases. “The real challenge for telecom operators is scaling AI across the network value chain; from planning and build to operations and field maintenance, while ensuring robust data foundations and clear performance measurement.”

He further explains that as AI becomes embedded in mission-critical network infrastructure, operators will need to carefully balance automation with human oversight and address risks related to reliability, security, and governance.

Nagulapally highlights another critical factor: “What separates deployments that succeed from those that stall is rarely the sophistication of the model. It is whether someone made the unglamorous decision to fix the data layer first, connecting operational systems that had been running in silos for years, so the AI is finally working from a single, coherent picture of the network rather than fragments of one.”

According to him, mission-critical networks add an entirely different dimension. When the stakes are high enough, including emergency infrastructure, financial networks, and defence-grade connectivity, the conversation stops being about capability and starts being about accountability. “Can you explain every decision the AI made? Can you audit it, challenge it, override it with confidence? That is a systems design question as much as an AI question, and it is one most vendors are not answering seriously enough yet,” he notes.

The GSMA report also indicates that the industry is moving towards new operational realities, where enabling AI at scale will require sustained investment in network capacity expansion, workload resilience, and orchestration across cloud and edge environments.

Nagulapally underscores this gap: “The truth is that most organisations are underinvesting in exactly the layer that determines whether their AI initiatives succeed or stall, not the models, not the compute, but the integration and orchestration fabric that ties it all together.”

Kochhar reinforces the need for sustained infrastructure investment when he says, “Sustained investments in fibre, spectrum, edge computing and data infrastructure will therefore be critical to fully realise the value-added horizontal potential of AI-driven telecom ecosystems in India.”

He augurs that, as networks become more complex with the rapid expansion of 5G and the future transition to AI-native 6G architectures, AI-driven automation will be essential to ensure resilience, performance optimisation, and cost efficiencies.

AI may have begun as a massive snowball, but for now, the snowbirds are still dealing with some snow-bunnies. ❄️

pratimah@cybermedia.co.in

Mesh vs extenders: Rethinking home Wi-Fi design

As Indian homes grow in size and device density, Wi-Fi is shifting from patch fixes to a core digital infrastructure layer, shaping coverage, resilience, and performance.



BY DR. SARATH KUMAR

Walk into any Indian home today, and the reliance on Wi-Fi is immediately clear. It powers office calls, virtual lessons, streaming, payments, and what appears to be a seemingly endless queue of connected devices. But dead spots remain a common irritant. Most families use extenders, which amp up a router's signal, but these tend to be temporary solutions rather than long-term fixes.

Mesh systems, however, are designed to deliver rock-solid, consistent Wi-Fi throughout the home. They can cover up to 1200+ square feet at a consistent speed, support up to 200 devices in higher-end models, and be expanded as needed. Extenders, by contrast, are better suited for targeting singular dead zones.

With Indian cities becoming smarter and multi-story homes the norm, the choice between extenders and mesh

is no longer a technical decision but a practical one that determines how homes are ready for the digital age and how families get connected.

SIGNAL EXTENSION VS DISTRIBUTED TOPOLOGY

The crucial distinction begins with how these systems work. A Wi-Fi extender is a device that receives the signal from your main router and rebroadcasts it to hard-to-reach areas of your home.

Most households use extenders to target one or two stubborn dead zones—a bedroom far from the router, or a balcony surrounded by concrete. However, extenders support multiple network names, so manual switching is required when roaming between rooms, and their grouped bandwidth can degrade performance under heavy use.

The shift from routers to distributed systems marks a turning point where home Wi-Fi begins to resemble structured network design.

Mesh Wi-Fi, however, forms a network of interconnected nodes placed around your property. Each node communicates with others, logically routing traffic to the strongest connection available, ensuring consistent speeds from the front door to the back door and right to the last room upstairs.

Users do not have to manually switch networks, and speed loss is minimised through dedicated node-to-node channels. Indian homes—with thick walls, rooms tucked behind stairwells, and growing numbers of smart devices—stand to gain maximum benefit from mesh systems that prioritise coverage, stability, and ease of use.

COVERAGE ENGINEERING FOR DENSE LAYOUTS

The choice between mesh and extenders is not binary; it is context-driven. Extenders excel in small apartments or homes facing one or two dead spots. For example, a family living in a compact Mumbai high-rise might only need an extender if the bedroom on the other side of their router experiences slow speeds.

Extenders work best when the goal is simple—stretch the signal a short distance at minimal cost—especially for less-demanding households or single rooms divided by a single wall.

Mesh networks shine in multi-storey homes, villas, and residences packed with connected devices—think large families streaming in every room, video calls, gaming sessions, and a parade of smart sensors. In Indian houses built with concrete partitions, mesh nodes brilliantly sidestep the headaches of patchy signals. Those living in duplex flats, serviced apartments, or even homes with shared courtyards find mesh invaluable, as it blankets wide spaces and navigates structural obstacles without manual adjustments.

THROUGHPUT, ROAMING AND LATENCY TRADE-OFFS

Many homeowners worry that mesh is overkill or that extenders are a fix-all. The truth is more nuanced. Mesh does not just serve tech-savvy users or luxury homes. Affordable mesh options are now plentiful, and setting up a network is often as simple as plugging in a few nodes and connecting to an app.

Likewise, extenders are not obsolete; they still fit scenarios where budget, space, and the number of devices are limited. The real myth is that one solution applies to all. Wall-thickness issues, floor plans, and rising expectations in Indian homes necessitate a tailored approach to maximise yields.

Extenders are better suited to addressing specific weaknesses. However, users in larger homes may experience reduced speeds or need to switch networks when roaming. Mesh systems are designed to provide balanced coverage across larger or more complex spaces and adapt automatically as additional smart devices are installed. Each solution suits different applications, depending on the size of the home, its layout, and internet usage patterns.

FROM HOME WI-FI TO DIGITAL INFRASTRUCTURE

The mesh debate now extends beyond individual homes into city-scale connectivity projects across India. Urbanisation is driving strong demand for wireless mesh networks in smart city infrastructure—everything from public Wi-Fi in parks to security cameras and intelligent traffic management.

Government-backed mesh deployments are bridging the digital divide by providing reliable connections where wired networks cannot. Indian telcos and private builders are also heavily investing, as mesh enables real-time IoT data exchange that lies at the core of smart city aspirations.

For everyday Indians, mesh Wi-Fi has become a technology luxury that is now a pragmatic reality. With a proliferation of smart devices in workspaces, bedrooms, and kitchens, mesh delivers the flexibility, speed, and convenience demanded by modern life. Extenders, convenient as they are, should remain for spot solutions. The conversation is no longer about which device is flashier, but which solution makes homes—and India itself—smarter, more connected, and ready for what comes next. 🌐

The author is the Chief Technology Officer of ACT Fibernet.

feedbackvnd@cybermedia.co.in



Networks rule the battlefield

From sensing to strike, integrated digital networks now shape combat outcomes, making resilience, trust, and speed central to operational advantage.



BY SHUBHENDU PARTH

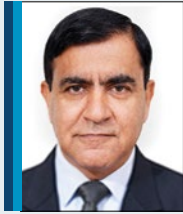
For much of modern military history, the logic of warfare was anchored in platforms. The side with superior aircraft, more advanced missile systems, or larger armoured formations held the advantage. Command structures were hierarchical, information flowed in defined tiers, and combat effectiveness depended on the concentration of force at decisive points.

This model also shaped India's early warfighting doctrines, where platform superiority and force concentration defined operational outcomes across theatres.

That logic is now undergoing a structural shift. Across recent conflicts—from Eastern Europe to West Asia—the decisive advantage is increasingly shaped not by the number of platforms deployed, but by how effectively they are connected. Warfare is no longer defined by platforms alone, but by the resilience, integrity, and speed of the networks that connect them.

Defence capability today is less about individual systems and more about integrating sensors, communication networks, and decision frameworks into a real-time operational fabric.

Electronic and cyber disruptions are redefining conflict, turning data flows and signal integrity into primary targets in modern warfare.



“Shared situational awareness and self-synchronisation now define combat, where dispersed forces act coherently without continuous central direction.

LT. GEN. RAJEEV SABHERWAL

Former Signal Officer-in-Chief, Indian Army

At its core, this transformation marks the emergence of a digital infrastructure stack for warfare—spanning fibre backbones, satellite communication layers, edge and cloud compute, AI-driven analytics, and secure data pipelines. What is now contested is not just physical space, but the integrity of the network that binds the battlefield together.

NETWORK-CENTRIC WARFARE: STRUCTURAL SHIFT

The transition from platform-centric to network-centric warfare is not merely technological. Rather, it is deeply structured and rooted in how militaries organise information, authority and action.

Explaining this shift towards an information-driven battlespace, Lt Gen Rajeev Sabherwal (Retd), former Signal Officer-in-Chief with the Indian Army, highlights that the combination of networked connectivity and smart entities has fundamentally changed the character of warfare.

“For the first time, it became possible to generate shared situational awareness, a common operating picture across echelons and services, and even self-synchronisation where dispersed elements could act coherently without continuous central direction,” he points out.

This is not just about linking systems, but creating a shared cognitive layer across the force. A common operating picture transforms command, enabling

distributed forces to act coherently without continuous central direction.

India’s own systems, such as the Integrated Air Command and Control System (IACCS), illustrate this shift by integrating civil and military radar feeds into a unified grid that supports coordinated responses across geographies. In such architectures, sensors, shooters, and decision-makers are no longer tightly bound to platforms or locations but operate as distributed, loosely coupled nodes within a shared battlespace.

This transformation fundamentally alters the nature of command. As Lt Gen Sabherwal further notes, “In a network-centric environment, combat effectiveness is directly proportional to network integrity... a sensor disconnected from the grid is reduced to a local observer.”

Cdr Aditya Varma (Retd), Leader – Public Sector, Security (India & SAARC) at Cisco, frames modern warfare as a unified operational stack. “A radar, tactical data link, fibre backbone, Satcom hop, and battle-management application must now be treated as parts of one warfighting stack... if the network is trusted, the force can fight coherently; if degraded, even advanced systems lose value,” he says.

Cdr Vipul Manocha (Retd), Founder of LAWA Global Innovations, describes this shift as the emergence of “combat cloud” architectures, where platforms operate as nodes within a shared battlespace network.



“Modern warfare runs on combat cloud architectures where communication, compute, and cybersecurity converge into one integrated operational framework.”

CDR. VIPUL MANOCHA

Ex Indian Navy & Founder, LAWA Global Innovations



“If you disrupt radios, satellite links, or secure data pipes, the command chain collapses, making communication networks the first target in conflict.”

COL. SANTANU DAS

Ex Indian Army & Head – Regulatory, Altius

As Cdr Manocha explains, “These systems are tightly integrated into multi-layered digital architectures... each platform operates as a node within a larger combat cloud,” reflecting a shift toward data-centric, algorithm-driven warfare where communication, compute, and cybersecurity converge into a unified framework.

At a systems level, this architecture spans multiple interdependent layers—sensing, network, compute, decision, and actuation—each dependent on the integrity of the others. The battlespace is no longer defined by platforms, but by the coherence of the system that connects them.

COUNTER-NETWORK OPS: NEW CENTRE OF GRAVITY

If networks define combat effectiveness, they are also becoming the primary target. Recent conflicts indicate a clear shift in targeting philosophy, where adversaries aim to degrade sensing, disrupt communication, and fragment decision-making rather than focus solely on destroying platforms.

Col Santanu Das (Retd), Head – Regulatory at Altius, explains that modern wars increasingly target communication infrastructure because it forms the “heart” and “nerves” of combat systems, noting that “If you knock out radios, satellite links, or secure data pipes, the whole command chain starts stumbling.”

Electronic warfare and cyber operations are central to this approach. As Col Das observes, “Jamming radar, spoofing GPS, or hacking command links can delay or mislead the system... even a few seconds of confusion can let a missile slip through.” In the Indian context, reliance on fibre grids, satellite communication, and tactical radio networks makes these layers prime targets, effectively turning communication infrastructure into the first line of attack.

Warfare is shifting from physical destruction to decision disruption, where delaying or degrading decisions becomes

decisive. This dynamic is amplified by saturation attacks, which involve coordinated waves of drones, missiles, and electronic interference designed to overwhelm systems and compress response timelines.

Gp Capt Dr Ashok Kumar (Retd), Member of the Board of Advisors of CyberAI Commune, highlights that “the timeline from detection to engagement... might be in the range of 30–40 seconds depending on the threat,” leaving little room for error. He also points to a deeper operational constraint, noting that “The biggest constraint in today’s battlefield is being an emitter... if you emit you will be detected—and with detection begins the kill chain.”

KILL WEB DYNAMICS: TIME AND TRUST LAYERS

The increasing complexity of threats has transformed the traditional kill chain into a distributed kill web, where multiple sensors, command nodes, and engagement systems interact dynamically across domains. This reflects the convergence of cyber, telecom, cloud, and electronic warfare into a unified combat system, where mission assurance depends on trusted data flows.

Sensor fusion lies at the core of this transformation, combining inputs from radar, electro-optical systems, RF intelligence, and space-based assets into a unified operational picture. As Lt Gen Sabherwal explains, “network integrity preserves situational truth, while decision speed ensures its timely exploitation,” underscoring the dual importance of accuracy and speed in modern operations.

From an operational perspective, Gp Capt Dr Kumar notes that “the sensor-to-shooter kill chain is always stressed... the requirement is to detect, identify, classify, prioritise and engage multiple threats simultaneously.”

This compression of timelines is often understood through the lens of the OODA loop—observe, orient, decide and act—where the side that can cycle faster gains a decisive advantage. In modern missile defence



“LEO constellations are transforming battlefield connectivity, enabling secure, reliable communication across dispersed and contested environments.”

DR. SIDHARTH SHUKLA

Ex Indian Army and Telecom & Satellite Consultant

scenarios, even marginal gains in this loop can determine whether an incoming threat is intercepted.

At this level of speed and complexity, human decision-making alone is no longer sufficient. AI is increasingly integral—shaping prioritisation, filtering noise, and recommending engagement decisions within compressed timelines. This introduces new challenges around control, accountability and fail-safe mechanisms in autonomous or semi-autonomous systems.

Cdr Manocha links this to decision tempo, observing that “this enables faster decision cycles... enhancing the probability of successful engagement in high-speed threat environments.” Yet speed alone is insufficient without trust.

Cdr Varma highlights that the defining vulnerability of such systems is not just loss of connectivity, but loss of confidence in data integrity. As he warns, “The greatest risk is not merely loss of availability, but the loss of confidence in sensing, identity, timing and data provenance... a false track or corrupted data stream can be as damaging as a physical strike.”

SPACE AND SATCOM AS THE RESILIENCE LAYER

As terrestrial networks become increasingly contested, space is emerging as both a sensing layer and a resilience layer. Lt Gen (Retd) AK Bhatt, Director General, Indian Space Association (ISpA), describes space-based systems as the “eye from the sky,” noting that “space... acts as the eye from the sky... enabling detection, tracking and characterisation of threats across large geographies.”

Lt Gen Bhatt further emphasises the dual role of space, stating that “space is increasingly becoming both the first line of sensing and the last line of resilience,” ensuring continuity of communication and situational awareness when terrestrial systems are degraded.

Dr Sidharth Shukla, an Army veteran and Telecom and Satellite Consultant, reinforces this perspective by

highlighting the enduring role of satellite communication, noting that “satellite communication has always been the redundant layer... its reach to remote areas is a win-win situation.” He also points to the future trajectory, explaining that “LEO constellations are the present and future for broadband satellite communication... enabling reliable and secure communication to the tactical and strategic battlefields.”

The expansion of LEO constellations and non-terrestrial networks (NTN) is likely to further strengthen this layer, making space an integral component of future defence architectures. “NTN technology onboard the LEO satellites can enable handsets to communicate with satellites directly, eliminating the need for bulky satphones. Also, NBIoT communication for all devices in the battlefield will be a game changer,” Dr Shukla says.

If space is emerging as both the first line of sensing and the last line of resilience, it also completes the shift in how combat systems are structured. What connects fibre backbones, satellite constellations, tactical radios, edge compute, and AI-driven decision systems is not technology alone, but their role as a unified operational infrastructure. In effect, warfare is no longer built around platforms, but around networks that make them relevant. This reframes combat power itself.

Interceptors may deliver the visible effect, but their effectiveness is shaped earlier—at the level of sensing, communication, and decision-making. The decisive advantage now lies in the ability to sustain network integrity under disruption, preserve trust in data, and maintain decision tempo under pressure.

Modern warfare is no longer a contest of platforms, but of systems—and in that contest, the side that sustains its digital and network infrastructure fights better and defines the battlefield. 🧠

shubhendup@cybermedia.co.in

“SPACE IS BECOMING THE FIRST LINE OF SENSING AND DEFENCE”

LT. GEN. AK BHATT

Ex Indian Army & DG, Indian Space Association (ISpA)



How is space emerging as a critical layer in modern defence systems, particularly for sensing and communication?

Space has emerged as a new domain of war. There are three critical aspects: the land, air and sea. Space is now emerging as a new critical dimension for warfare. The space segment provides an additional layer of data, which acts as an eye from the sky. Data recorded in real time, in formats such as satellite imagery and radar data, can detect enemy movements for vigilance.

They enable detection, tracking, and characterisation of threats across large geographies, feeding actionable intelligence into command systems. Additionally, Satcom enables space segment intelligence to be instantly communicated to all operational units, without dependence, while ensuring secrecy through encryption.

What role do Intelligence, Surveillance, Reconnaissance (ISR) satellites and Satcom play in enabling real-time targeting and coordination?

ISR satellites provide real-time awareness, capturing high-resolution data. This data enables allied forces to detect and track enemy movements across geographies that would otherwise be inaccessible. ISR and Satcom create a seamless loop, reducing decision timelines and enabling coordinated, precision operations even in highly dynamic combat scenarios.

How are adversaries leveraging space assets to enhance battlefield awareness and operations?

Adversaries are also increasingly investing in multi-layered space capabilities, including high-revisit ISR constellations, electronic intelligence satellites, and resilient communication networks.

ISR and Satcom create a seamless loop, reducing decision timelines and enabling coordinated, precision operations in highly dynamic combat scenarios.

The convergence of space, AI, edge computing and communication networks will define the next generation of defence systems and operational capabilities.

Adversaries of India have heavily invested in developing infrastructure, including a fleet of satellites and high-resolution data for surveillance, GIS, PNT, SSA, and SSD capabilities. China has invested additional resources to enhance its capabilities. Our other adversary, though, lacks similar resources or infrastructure, but can gain access to these capabilities through China, which is a matter of concern.

How do you see the integration of space, AI, and communication networks evolving?

The convergence of space, AI, edge computing and advanced communication networks will define the next generation of defence systems. AI will play a critical role in processing vast volumes of satellite data, enabling real-time analytics, anomaly detection, and predictive decision-making.

Edge computing allows raw sensor data to be filtered, prioritised, and transformed into actionable intelligence before transmission, ensuring that only mission-relevant insights are communicated through high-speed, secure networks.

This distributed intelligence enhances resilience, particularly in contested or communication-denied environments, where continuous connectivity cannot be guaranteed. When integrated with high-speed, secure communication networks, this creates an ecosystem of autonomous or semi-autonomous operations in which systems can respond faster than human decision cycles in certain scenarios.

This integration will move defence architectures toward intelligent, adaptive, and self-healing networks, capable of operating effectively even under contested conditions.

With increasing reliance on ISR satellites and Satcom, do you see space emerging as the first line of sensing and the last line of resilience in defence networks?

Space is increasingly becoming both the first line of

sensing and the last line of resilience. Space-based sensors often provide the earliest indication of threats, whether through missile launch detection, movement tracking, or electronic signatures. If terrestrial and airborne systems are disrupted, the space domain can step in to maintain communication and situational awareness.

How should India strengthen its space-based defence capabilities to support integrated and network-centric warfare?

India's approach should move towards distributed satellite constellations rather than relying on a few high-value assets. This would improve redundancy and survivability, ensuring that the loss of individual systems does not compromise the overall capabilities.

At the same time, it is important to leverage India's growing capabilities in the private space sector. Organisations such as ISpA can play a key role in accelerating innovation, reducing costs and enabling faster scaling of space-based capabilities.

There is also a need to develop unified frameworks that integrate space-based data with air, land, sea, cyber and electronic warfare domains. This integration is essential to enable true multi-domain operations and ensure seamless coordination across different layers of defence.

In addition, government investments in indigenous ISR, secure Satcom and space situational awareness capabilities will be critical to maintaining strategic autonomy.

Finally, India will need to work towards a combined Geostationary Earth Orbit (GEO), Medium Earth Orbit (MEO), and Low Earth Orbit (LEO) constellation for Satcom as a strategic necessity. The Navigation with Indian Constellation (NavIC) system, India's independent regional satellite navigation system, is currently facing challenges and will also need to be fully functional at the earliest. 🌐

Shubhendu Parth
shubhendup@cybermedia.co.in

“THE TRADITIONAL KILL CHAIN HAS EVOLVED INTO A KILL WEB”

GP. CAPT. DR. ASHOK KUMAR

Ex Indian Air Force & Member – Board of Advisors,
CyberAI Commune



In an actual air defence scenario, how does the timeline unfold from detection to interception, and where do the key constraints arise?

In the present environment, air defence systems are networked and layered, with long-range surveillance, tracking and engagement radars forming the primary detection layers. Adversaries increasingly attempt to delay detection, as this directly impacts subsequent layers, including sensor-to-shooter linkages. This delay is achieved through stealth aircraft, hypersonic weapons and unmanned systems with very low radar cross-sections, making detection more difficult.

The timeline from detection to engagement is extremely tight, often measured in seconds. For example, Arleigh Burke-class destroyers of the US Navy, equipped with the Aegis Combat System, can detect, classify,

evaluate, engage and guide interceptors to neutralise incoming threats within seconds. In such scenarios, the time between detection and impact may be as little as 30 to 40 seconds, depending on the threat's parameters.

With the proliferation of small and slow unmanned aerial systems, these timelines are becoming even more compressed, as conventional radars are often unable to detect them at longer ranges.

In today's war, the evolution and proliferation of technology itself are a constraint. New and emerging methods of warfare are adding layers of complexity. The biggest constraint in today's battlefield is being an emitter of any kind in the electromagnetic domain. If you emit, you will be detected, and with detection, the kill chain begins.

As threats scale in speed and volume, systems shift to kill webs, integrating sensors, command nodes and shooters into a coordinated, adaptive architecture.

Detection delays are now engineered through stealth, hypersonics, and low-radar-cross-section drones, compressing timelines and stressing sensor-to-shooter networks.

From an operator's perspective, how effectively does the sensor-to-shooter chain function under real-world conditions, especially during multiple simultaneous threats?

In real-world conditions, the sensor-to-shooter kill chain is always under stress, as threat vectors continue to evolve. With the advent and continuous refinement of both kinetic and non-kinetic threats, including electronic warfare enabled by software-defined radios (SDRs), the kill chain has been significantly compressed.

The requirement is to detect, identify, classify, prioritise and engage multiple threats in the most effective manner, while ensuring minimal disruption to own operations and avoiding collateral damage. As a result, the traditional kill chain has evolved into what is now described as a kill web.

Accordingly, air defence sensor-to-shooter links are designed with low-latency and high-bandwidth systems, supported by multiple layers of redundancy. Increasingly, AI-enabled systems are assisting across the entire cycle, from detection to engagement and neutralisation, particularly in scenarios involving multiple simultaneous threats, which have now become the norm in modern battlefields.

Operation Sindoor in June 2025 serves as an illustrative example. The threat vectors included simulated attacks by manned 3.5th- to 4th-generation fighter aircraft launching guided munitions against both aerial and ground targets. These were complemented by waves of unmanned aerial vehicles—drones—of varying sizes intended to overwhelm air defence sensor-to-shooter links, followed by ground-launched short-range ballistic rockets and missiles.

All these threats were neutralised by a layered air defence architecture comprising Airborne Early Warning and Control System (AEW&CS), S-400 systems, the

Akash missile system, and point air defence systems, including legacy gun systems.

Threats were seamlessly handed off from sensors to Command & Control nodes to shooters while coordinating ongoing offensive operations. In essence, it is a multidimensional chess game, where actions at one level create cascading effects across others.

So, how do modern air defence systems cope with high-volume or swarm attacks designed to overwhelm interception capacity?

Modern air defence systems cope with swarm attacks by harnessing advanced technologies, particularly AI-enabled detection, identification and classification, followed by decision support that matches the optimal weapon system to incoming threats. Most unmanned aerial threats are detected by ground-based radars relatively late due to their small or negligible radar cross-section (RCS), which depends on the size and speed of the unmanned aerial vehicle.

For example, the now well-known Shahed-136 loitering munition has an RCS that is often filtered out by traditional radars as clutter. As a result, detection relies on a combination of techniques and technologies, including AI-powered fingerprinting of radar signals and acoustic signatures for initial detection and identification. These are then handed off to engagement systems, which may employ thermal sensors paired with passive RF sensors to engage the swarm.

At this stage, key considerations include achieving the lowest possible cost per engagement while minimising collateral damage, particularly from debris.

Overall, AI-enabled systems are increasingly being integrated across each stage of the sensor-to-shooter kill chain, providing timely decision support to the man-in-the-loop and enabling more effective responses to high-volume threats.

AI-led detection, classification and engagement are reshaping air defence, enabling faster response and optimal weapon allocation against swarm attacks.

How critical are network reliability and decision speed during active engagements, particularly when response windows are extremely compressed?

Network reliability is vital for the success of the entire sensor-to-shooter kill web. Low-latency and high-bandwidth networks form the backbone of the system. During hostilities, the effectiveness of air defence systems is often tested in scenarios that were not fully envisaged during the initial design and deployment phases.

The robustness and redundancy built from concept through design to execution, along with inherent adaptability, determine the effectiveness of any air defence network. The addition of plug-and-play architectures further enables the integration of a large number of sensors and shooters, enhancing overall system capability.

In today's complex and dynamic air threat environment, network reliability and decision speed can be the difference between being overwhelmed and achieving overmatch.

This can be understood in the context of the near-continuous targeting of Ukrainian power generation and distribution infrastructure by Russian forces. Without power, networks degrade, increasing the probability of success for swarm attacks involving unmanned aerial vehicles combined with cruise and ballistic missiles.

With increasing automation, how do you see the balance evolving between human judgement and AI-assisted decision-making in air defence?

The evolution of the balance between human judgement and AI is no longer a future debate. As of 2026, it has become a core design philosophy for air defence architecture at both operational and national levels. The shift is from a "human-in-the-loop" model to a "human-on-the-loop" framework, where AI functions as an agentic partner rather than merely a computational tool.

In the emerging battlefield, the central challenge will be momentum, driven by mass and velocity. Either speed

will increase, as seen with hypersonic weapon systems, or mass will increase through swarms of low-cost unmanned systems. In most scenarios, a combination of both will be applied. This will require not only AI assistance but, in certain cases, AI-led engagements. While AI manages the "how," the human commander remains the sole arbiter of the "why."

How would you assess India's readiness in handling multi-layered, high-intensity aerial threats, and what operational gaps still need attention?

India has modernised significantly and developed novel solutions into a multi-layered, robust and redundant air defence kill web, as demonstrated during Operation Sindoor in early June 2025.

However, this kill web needs to be constantly updated, upgraded and enhanced through the adoption of newer technologies and more capable systems. As the threat landscape evolves and technology boundaries blur, air defence systems must become more agile in discovering, detecting and identifying emerging threats.

A key gap is the dependence on foreign systems, which can limit or delay full integration across the kill web. Addressing this will require greater involvement of private industry in research, development and production of cutting-edge solutions across both software and hardware domains. Another critical area is reducing the cost per engagement. This can be addressed through a mix of Directed Energy Weapons and soft-kill methods based on target allocations by MOTL kill webs.

There is also an urgent need to expand airborne early warning and control capabilities. India requires a scalable, indigenous AEW&C system to effectively counter the range and volume of threats likely to emerge during hostilities. 🌟

(Lt. Col. Varun Pathak provided research inputs for the responses)

Shubhendu Parth
shubhendup@cybermedia.co.in

“MISSILES DELIVER IMPACT, NETWORKS DECIDE TIMING AND EFFECT”

CDR. ADITYA VARMA

Ex Indian Navy & Leader – Public Sector,
Security (India & SAARC), Cisco



How is the convergence of cybersecurity, telecom and defence networks reshaping warfare?

Modern warfare is no longer platform-centric; it is network-centric and increasingly data-centric. The decisive edge now lies in how quickly a force can sense, fuse, decide and act across air, land, sea, undersea, space and cyber, while preserving trust in the network carrying that data. Integrated air and missile defence, along with joint all-domain command and control, now depend on rapid detection, distributed decision-making, resilient communications and secure data sharing, rather than on any single “best” platform.

In operational terms, cybersecurity, tactical communications, cloud, edge computing, electronic warfare (EW) resilience and command-and-control have converged into a single combat system. A radar, tactical data link, fibre backbone, Satcom hop and battle management application

must now be treated as parts of one warfighting stack. If the network is trusted, the force can manoeuvre and fight coherently; if the network is degraded, even advanced kinetic systems lose much of their combat value.

What are the biggest cybersecurity risks to integrated defence networks?

The greatest risk is not merely the loss of availability, but the loss of confidence in sensing, identity, timing, command integrity and data provenance. Integrated defence networks can be degraded through jamming and spoofing of radio frequency (RF), Global Navigation Satellite System/Positioning, Navigation and Timing (GNSS/PNT) and satellite communication (Satcom) links.

These include network management systems or ground stations, malware propagation across converged IT-OT environments, firmware or component tampering

Cloud and edge together enable distributed decision-making, ensuring low-latency response at the tactical edge while maintaining broader orchestration.

Denied, disrupted, intermittent and limited, the D-DIL-ready architectures must be built with edge autonomy and rapid re-synchronisation capabilities.

in the supply chain, and manipulation of data streams that feed the common operational picture.

As networks become more software-defined and increasingly interconnected, the attack surface expands across cloud layers, fielded nodes, maintenance channels and vendor dependencies. This also means the commander's challenge is no longer limited to cyber defence in the traditional IT sense. Rather, it is about mission assurance across the entire digital kill chain.

A false track, a corrupted time source, an untrusted device identity or a compromised software update can be as operationally damaging as a physical strike on a radar or relay node.

How can defence systems ensure secure, trusted data exchange across distributed nodes?

Secure exchange across distributed nodes requires an identity-first, zero-trust model, rather than implicit trust based on location, enclave or network segment.

In practice, this means establishing strong cryptographic identities for users, devices, and workloads, along with mutual authentication, signed software and firmware, continuous policy enforcement, data labelling, and need-to-know access control, and secure cross-domain transfer across classification boundaries.

Defence networks should also be designed with communications diversity and graceful degradation in mind. Fibre, RF and Satcom links should form protected alternate, contingency and emergency paths, rather than acting as single points of failure.

Equally important is the need for crypto-agility. Sensitive traffic captured today may be targeted for decryption at a later stage, so long-life strategic networks require a migration path towards post-quantum cryptography. This may also involve selective evaluation of quantum-safe overlays or Quantum Key Distribution (QKD) for the most critical sovereign links, where operational circumstances justify it.

How do cloud-edge architectures enable distributed processing and decision-making in defence communications?

Cloud and edge are complementary layers of the same military digital architecture. Cloud provides elasticity, common services, storage, model training, collaboration and force-wide application hosting. Edge provides low-latency processing, local autonomy, sensor fusion and continuity of operations at the tactical point of need.

The US Department of Defense cloud guidance makes the case for hybrid and fit-for-purpose models, especially for distributed environments and the tactical edge. In defence communications, this means that data need not always travel back to a distant core before action can be taken.

Threat evaluation, local AI inference, video analytics, battle management updates and degraded-mode command support should happen as far forward as operationally feasible, that is, as close to the tactical edge as possible. At the same time, cloud layers support broader orchestration, historical analytics, software lifecycle management and multi-echelon common operating pictures.

The real design challenge is not cloud versus edge, but ensuring secure synchronisation, authority, resilience, and data governance across both, particularly under contested, disconnected, or bandwidth-constrained conditions.

Will network survivability under cyber and electronic attack determine kinetic effectiveness in future conflicts?

Kinetic capability will remain indispensable, but secure and sustainable networks will increasingly determine whether kinetic capability can be employed effectively, at speed and at scale. Integrated air and missile defence already demonstrates this logic—detection, threat prioritisation, interceptor assignment and mid-course updates all depend on resilient digital architecture.



The biggest risk is not an outage, but the loss of trust—compromised data, identity, or timing can disrupt operations as severely as physical attacks.

In other words, missiles and interceptors may deliver the physical effect, but networks decide whether that effect is timely, coordinated and proportionate. India's own experience with networked air defence integration, including the publicly highlighted role of Akashteer, reinforces the same lesson—sensor fusion, command networks and real-time situational awareness multiply the effectiveness of hard-kill systems.

In future conflicts, network survivability under cyberattack, EW and saturation pressure will often be the precondition for kinetic success. The side that keeps its network trusted, adaptive and available is more likely to preserve decision advantage, reduce fratricide and use scarce munitions more intelligently.

So, how can India harden its defence network architecture against cyber and hybrid threats?

India should pursue a mission-assurance model built around six priorities. It needs to move from perimeter-based security to zero-trust enforcement across defence IT, OT and weapon-support environments. Also, the communications infrastructure must be hardened end-to-end. Tactical RF, fibre, microwave, undersea and satellite segments should be designed with redundancy, authentication, anti-jam resilience and secure management planes, especially given the

strategic importance of protecting both satellite and ground segments.

In fact, CERT-In's latest space security guidance underscores the strategic importance of protecting satellites and the ground segment.

There is also a need to institutionalise continuous cyber validation through red, blue and purple teaming, along with joint exercises. Initiatives such as the Defence Cyber Agency's Cyber Suraksha reflect the right operating model in this direction. Supply-chain assurance must also be strengthened, with strict signed-update discipline and clear hardware and software provenance for both indigenous and imported systems.

Denied, disrupted, intermittent and limited, the D-DIL-ready architectures must be built with edge autonomy and rapid re-synchronisation capabilities.

Finally, India needs to begin a deliberate migration towards quantum-safe cryptography for long-life strategic networks and sensitive traffic, aligned with its broader roadmap in this area. 🌟

Shubhendu Parth
shubhendup@cybermedia.co.in

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

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

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



Book Digital Subscription Now!

Yes! I want to subscribe to Voice&Data



Scan QR Code
& Subscribe now...

Subscribe to Digital Edition @ ₹735/-

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

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

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

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

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

Name [•]: Mr/ Ms _____ Date of Birth:

Organisation: _____ Designation: _____

Delivery Address: _____

City: _____ State: _____ Postal Code:

Mob [•]: Tel: Email [•]: _____

GST No. [•]: PAN No. [•]:

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

Payable at (specify bank and city) _____

OR

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

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

[•] Essential fields

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

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

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

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

For Subscription queries:

9289870545

Terms & Conditions: _____

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

Quantum threats test India's cybersecurity doctrine shift

India must rethink legal and regulatory frameworks as quantum risks expose gaps in encryption, compliance timelines, and long-term data protection norms.



BY GAURAV SAHAY

The rapid evolution of digital infrastructure, artificial intelligence, and data-driven economies has significantly altered the contours of risk, trust, and sovereignty in cyberspace.

India, as one of the fastest-growing digital economies globally, has made notable strides in establishing a foundational cybersecurity framework through statutes, sectoral regulations, and executive advisories issued by agencies such as CERT-In. However, the emergence of quantum computing represents a paradigmatic shift that challenges the very assumptions underpinning existing cybersecurity architectures.

In this context, India must transition from a classical cybersecurity paradigm, premised on computational hardness, to a forward-looking quantum security framework that anticipates the vulnerabilities introduced by quantum capabilities. This transition is not merely

technological: it is fundamentally legal, regulatory, and strategic.

At its core, quantum computing does not just challenge cybersecurity policy—it threatens the cryptographic infrastructure that underpins networks, data centres, and digital systems.

LEGACY CYBER LAWS FACE QUANTUM LIMITS

India's cybersecurity regime was conceived in an era where cryptographic systems such as RSA and Elliptic Curve Cryptography were considered secure against feasible computational attacks. These frameworks primarily focus on unauthorised access, data breaches, intermediary liability, and digital signatures.

Supplementary frameworks introduced obligations around data fiduciaries, consent, purpose limitation, and reasonable security safeguards. Additionally, sectoral

Quantum computing shifts cybersecurity from a present-risk model to a time-layered threat, where today's encrypted data may be tomorrow's breach.

regulators such as RBI, SEBI and IRDAI have prescribed cybersecurity and data protection standards tailored to their respective domains.

While these frameworks collectively establish a reasonably robust compliance architecture for current threats, they remain inherently reactive and technologically neutral, without explicit contemplation of quantum-induced vulnerabilities.

Quantum computing fundamentally disrupts this equilibrium by rendering widely used public key cryptographic systems potentially obsolete. Algorithms theoretically enable the efficient factorisation of large integers and the solving of discrete logarithm problems, thereby compromising encryption mechanisms that secure financial systems, government communications, defence infrastructure, and critical information systems.

This introduces the “harvest now, decrypt later” risk, in which adversaries may collect encrypted data today with the intent to decrypt it once quantum capabilities mature. From a legal standpoint, this raises profound questions regarding the adequacy of “reasonable security practices” under Indian law.

If encryption standards considered reasonable today become vulnerable tomorrow, the temporal dimension of compliance becomes uncertain, potentially exposing organisations to retrospective liability.

REGULATORY GAPS IN QUANTUM READINESS

India's existing legal framework does not explicitly mandate quantum-resilient cryptography or prescribe standards for post-quantum cryptographic adoption. The absence of such mandates creates a regulatory lacuna, particularly when juxtaposed against global developments.

In countries like the USA, initiatives led by the NIST are actively standardising PQC algorithms, while the EU is integrating quantum considerations into its cybersecurity and digital sovereignty strategies. India has demonstrated strategic intent through initiatives such as the National Mission on Quantum Technologies and Applications (NM-QTA).

However, this intent has yet to translate into binding legal or regulatory frameworks that govern the deployment, transition, and audit of quantum-safe systems.

REDEFINING REASONABLE SECURITY NORMS

A critical aspect of rethinking India's legal framework lies in redefining the concept of “reasonable security practices and procedures”. Currently, compliance is often benchmarked against standards such as ISO/IEC 27001 or sector-specific guidelines.

In a quantum context, these standards may need to be supplemented or reinterpreted to include quantum resilience benchmarks. This would necessitate regulatory guidance, potentially through amendments to existing rules or the issuance of new subordinate legislation, mandating a phased migration to PQC algorithms for critical sectors such as banking, telecommunications, defence, and energy.

Such a mandate would also need to account for interoperability challenges, legacy systems, and the significant costs associated with the cryptographic transition.

The DPDP Act introduces obligations on data fiduciaries to implement “reasonable security safeguards” to prevent personal data breaches. In a quantum threat scenario, the interpretation of these safeguards must evolve to include forward secrecy, quantum-resistant encryption, and enhanced key management practices. Failure to anticipate quantum risks may constitute negligence, particularly for entities that handle sensitive personal data or critical infrastructure information.

This raises the possibility of regulatory enforcement actions and civil liability in cases where data breaches result from foreseeable quantum vulnerabilities. Accordingly, regulators may need to issue clarificatory guidance or codes of practice that explicitly incorporate quantum risk assessments into data protection compliance frameworks.

Another dimension that warrants attention is the intersection of quantum security with national security and critical information infrastructure protection.

Legal ambiguity around “reasonable security” could expose organisations to retrospective liability as encryption standards fail in a quantum future.

PROTECTING CRITICAL SYSTEMS IN QUANTUM ERA

In India, the government has the authority to designate “protected systems” and impose stringent security requirements. In a quantum era, the criteria for such designation may need to be expanded to include systems that rely on cryptographic integrity for their operation.

Additionally, agencies such as the NCIIPC would need to develop quantum threat models and prescribe sector-specific transition roadmaps. This would likely involve a combination of regulatory mandates, public-private partnerships, and capacity-building initiatives to foster indigenous expertise in quantum-safe technologies.

CROSS-BORDER RISKS AND QUANTUM STANDARDS

Cross-border data flows and international cooperation also acquire new significance in the context of quantum security. As India integrates more deeply into global digital supply chains, the security of data transmitted across jurisdictions becomes contingent on the weakest link in the cryptographic chain. The specific provision of law on cross-border data transfers, coupled with potential future adequacy assessments, may need to incorporate quantum security considerations.

This could lead to the emergence of “quantum adequacy” standards, wherein jurisdictions are evaluated based on their adoption of PQC and quantum-safe infrastructure. For Indian entities operating globally, this would necessitate alignment with international standards and participation in multilateral efforts to harmonise quantum security protocols.

From a policy perspective, the transition to quantum security also raises issues of standard-setting, certification, and liability allocation. The BIS and other standard-setting bodies would need to collaborate with global institutions to develop and adopt PQC standards tailored to Indian requirements. Certification frameworks for quantum-safe products and services would become essential to ensure trust and interoperability.

Moreover, contractual frameworks, particularly in sectors such as cloud computing, telecommunications,

and fintech, would need to evolve to allocate risks associated with quantum vulnerabilities. This may include representations and warranties regarding the use of quantum-resistant encryption, indemnities for cryptographic failures, and obligations to upgrade systems in line with evolving standards.

PHASED TRANSITION AND POLICY SAFEGUARDS

The transition to quantum security must be approached in a phased and risk-sensitive manner. Immediate, wholesale replacement of existing cryptographic systems is neither feasible nor economically viable. Instead, a tiered approach that prioritises critical sectors and high-risk data categories would be more pragmatic.

Legal frameworks must therefore provide clarity on timelines, transitional arrangements, and safe harbours for entities that demonstrate good-faith efforts toward compliance. This would mitigate the risk of regulatory overreach while incentivising organisations to address quantum threats proactively.

The advent of quantum computing necessitates a fundamental rethinking of India’s cybersecurity legal framework. While existing laws provide a foundation for addressing current threats, they are insufficient to contend with the disruptive potential of quantum technologies.

India must move toward a quantum-aware legal architecture that integrates technological foresight with regulatory clarity, balancing innovation with risk mitigation. This will require coordinated action across legislative, regulatory, and industry stakeholders, underpinned by a clear national strategy on quantum security.

Failure to act in a timely and structured manner could expose India’s digital economy to systemic vulnerabilities, undermining trust, competitiveness, and national security in the quantum age. 🌟

*The author is the Founding Partner of
Arthashastra Legal.*

feedbackvnd@cybermedia.co.in



India's hyperscale push raises stakes for power quality

As India's data centre capacity surges, next-gen UPS systems can ensure uptime by stabilising power quality and insulating critical loads from grid variability.



BY VIKAS SRIVASTAVA

India's data centre story has moved well past potential. The country is on course to scale from approximately 1.4 GW of installed IT capacity today to over 9 GW by 2030—a trajectory that places it among the fastest-growing data centre markets globally.

Today, hyperscalers, global colocation operators, and domestic cloud providers are committing significant capital to build large-scale campuses across Mumbai, Chennai, Hyderabad, and increasingly, emerging corridors in Pune, Kolkata, and secondary cities.

Beneath this ambition, however, lies a challenge that does not always receive the attention it deserves: India's power grid, for all its improvement, was not built with hyperscale data centres in mind.

GRID VARIABILITY MEETS HYPERSCALE DEMAND

India's national grid has undergone a significant transformation over the past decade. Yet the reality on the ground is of voltage fluctuations, frequency deviations, harmonic disturbances, and intermittent outages that remain far more common than in comparable markets.

India's hyperscale ambition is outpacing grid readiness, making power conditioning infrastructure a non-negotiable layer for uptime assurance.

UPS systems are no longer backup assets; they operate continuously to filter disturbances and maintain clean, stable power for critical loads.

Seasonal demand spikes, monsoon-related transmission disruptions, and the uneven integration of renewable energy into state grids create a genuinely unpredictable power environment.

For a conventional industrial consumer, these variations are an inconvenience. For a hyperscale data centre operating under stringent SLA commitments, they are an existential risk. A voltage sag lasting milliseconds can corrupt transactions across thousands of concurrent workloads.

Similarly, a brief frequency excursion can cause hardware faults in high-density GPU clusters running AI inference at scale. As India's data centres assume increasingly critical functions such as cloud services, financial infrastructure, and national AI platforms, the tolerance for power-related disruptions is effectively zero.

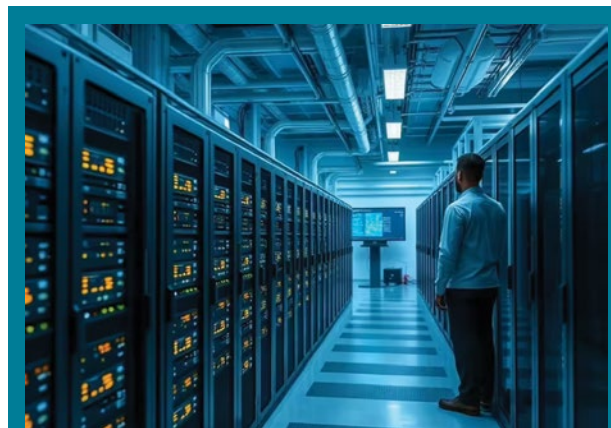
Compounding this is the sharp rise in rack power density. Where standard deployments once operated at 8–12 kW per rack, AI and high-performance computing workloads are routinely demanding 40–80 kW, with next-generation configurations pushing beyond 100 kW. At these densities, the impact of any power-quality event is significantly amplified.

UPS EVOLVES INTO A CORE INFRA LAYER

The conventional framing of UPS systems as backup power devices that activate when the grid fails significantly understates their function in today's hyperscale environment. A modern UPS system is, in effect, a continuous power conditioning and management layer.

In double-conversion online architecture, incoming utility power is rectified to DC and then inverted back to clean AC, ensuring the IT load is always powered from a fully conditioned, grid-isolated supply. Every grid disturbance, including sag, swell, harmonic, or outage, is absorbed before it can reach the load.

This architecture is particularly well-suited to India's grid conditions. The UPS operates as a permanent buffer,



IN BRIEF

- India's data centre capacity is set to expand from 1.4 GW to over 9 GW by 2030, placing unprecedented demands on power reliability.
- Grid variability, from voltage sags to frequency swings, poses systemic risks to hyperscale facilities operating under strict uptime SLAs.
- High-density AI workloads, reaching 40–100 kW per rack, intensify the impact of even minor power quality disturbances.
- Next-gen UPS systems act as continuous power conditioning layers, isolating IT infrastructure from grid inconsistencies.
- Lithium-ion batteries are improving lifecycle economics and resilience, especially under India's high ambient temperature conditions.
- Intelligent UPS platforms enable predictive maintenance and energy optimisation, turning power systems into active infrastructure assets.

not an emergency switch, which means grid variability becomes operationally irrelevant to the IT infrastructure it protects.

Modular UPS designs align with phased data centre builds, enabling efficient scaling without compromising redundancy or performance.

Equally important for India's phased hyperscale build model is the modular UPS architecture. Most large campus developments in India are deployed in tranches, initial capacity followed by incremental expansion as demand is secured. Modular systems allow power capacity to be added incrementally, with each module operating at its optimal efficiency range.

This eliminates the cost and efficiency penalty of oversized fixed-capacity systems in early deployment phases, and enables hot-swappable redundancy at the module level. It is a meaningful operational advantage in a market where service response times can vary by geography.

LITHIUM-ION REDEFINES BATTERY STRATEGY

The transition from traditional valve-regulated lead-acid batteries to lithium-ion technology is reshaping the UPS landscape for Indian data centres. In India's tropical climate, battery room ambient temperatures are a persistent operational challenge.

Lithium-ion chemistries offer a wider safe operating temperature range, higher energy density, which means a reduced physical footprint for equivalent capacity, and a significantly longer cycle life, typically exceeding 10 years compared to 3–5 years for legacy alternatives.

From a total cost of ownership perspective, the extended lifespan fundamentally alters the financial model for large facilities. When combined with sophisticated Battery Management Systems that enable condition-based monitoring, operators can move from scheduled replacement cycles to predictive interventions, reducing both planned downtime and the risk of unexpected failure.

INTELLIGENCE POWERS ENERGY OPTIMISATION

Hardware architecture alone is no longer the differentiator. The competitive frontier for UPS platforms today lies in control intelligence. Advanced monitoring systems continuously track battery impedance, capacitor health, thermal performance, and module output characteristics, enabling predictive maintenance that identifies degradation weeks before it manifests as a failure.

For data centre operators managing distributed facilities across India from Mumbai campuses to emerging hubs in secondary cities, this early visibility is operationally critical, particularly where skilled service resources may not be immediately accessible.

Beyond maintenance, next-generation UPS platforms are increasingly being designed to participate in broader energy management strategies. India's evolving Time-of-Day tariff structures and Open Access frameworks create real opportunities for large power consumers to optimise electricity procurement costs.

UPS systems with grid-interactive capability can discharge stored energy during peak tariff windows and recharge during off-peak periods, functioning as active energy management assets rather than passive protection devices.

POWER BACKBONE FOR GIGAWATT EXPANSION

India's hyperscale build-out will require the deployment of UPS-grade power protection across hundreds of gigawatts of IT capacity over the next decade. This is not an incremental upgrade but a foundational infrastructure investment that will underpin the country's digital economy, cloud sovereignty ambitions, and national AI capabilities for a generation.

While the country's grid will continue to improve, the pace of data centre growth will outrun grid development for the foreseeable future, and the inherent variability of power delivery across a subcontinent of this scale will not be engineered away quickly. The UPS layer can serve as the critical interface between grid reality and the zero-tolerance uptime requirements of mission-critical infrastructure.

The gigawatt growth is here. Securing it demands power infrastructure equal to the ambition driving it. 🌟

The author is Director of Product Management, Product Development, and Engineering at Vertiv.

feedbackvnd@cybermedia.co.in



Power, not proximity, redrawing data centre maps

As metro constraints grow, power availability, cost, and resilience are driving new location choices, reshaping data centre expansion into a distributed model.



BY PRATIMA HARIGUNANI

History is filled with people who left cities to seek something different in remote, unfamiliar places. From writers and artists to modern-day explorers, the journey into the wilderness has always been about finding new possibilities beyond crowded urban life.

That instinct is visible even today. As Ben Fogle's journeys show, life away from cities is not easy, but it

offers a different kind of value shaped by adaptation and resilience.

A similar shift is now playing out in India's data centre landscape. Long anchored in major metro hubs, the industry is now extending into less obvious locations. The "wild" is no longer just a metaphor. Data centres are steadily expanding beyond Mumbai, Delhi, and Bengaluru into new territories.

Expansion beyond metros is no longer opportunistic but driven by power, cost, and resilience, redefining how data centre capacity is distributed.



“Moving inland cuts TCO by up to 40%, while delivering scalable power, reduced congestion, and stronger resilience against metro-centric infrastructure risks.”

NARENDRA SEN

Founder & CEO, RackBank

The question is no longer whether this shift will occur, but how far and how fast it will scale.

CAPACITY FINDS NEW GROUND BEYOND METROS

India's data centre expansion is extending beyond established metros, with operators and investors evaluating Tier 2 and Tier 3 cities to address capacity, latency, and resource constraints.

NeevCloud has identified Indore SEZ-2 and the Pithampur Industrial Area in Madhya Pradesh's Dhar district as primary locations for its AI data centres. CtrlS has selected Bhopal, where it opened a facility in 2025 at Badwai IT Park, with an investment commitment of Rs 500 crore (USD 59 million) on a five-acre site. Its expansion pipeline includes Patna, Lucknow, GIFT City in Ahmedabad, Bhubaneswar, and Guwahati.

RackBank has also announced an 80MW data centre in Indore, while cloud services provider Dinclix GroundWorks is based in the same city, indicating the emergence of a regional cluster. Techno Digital, the digital infrastructure arm of TEECL, is building 102 edge data centres across 23 states and has partnered with RailTel to support the rollout.

The company commissioned a 36MW AI-ready hyperscale facility at SIPCOT IT Park, Siruseri, in August 2025. Large-scale investments continue alongside this distributed expansion. The Adani Group has also outlined plans to invest up to USD 5 billion in a Google

AI data centre project in Visakhapatnam, while Reliance Industries is developing a USD 30 billion, 3 GW AI campus in Jamnagar.

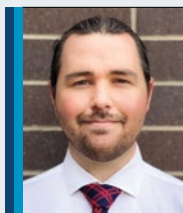
Industry reports indicate a structural shift. According to Mordor Intelligence, cities such as Pune, Jaipur, Kochi, and Bhubaneswar are hosting edge nodes designed to reduce latency for OTT and IoT applications. The IndiaAI Mission's plan to establish 27 regional labs in cities including Gorakhpur, Shimla, and Patna is also contributing to distributed capacity growth.

Savills Research projects expansion in emerging markets, with Kolkata expected to grow by 48%, supported by its role as a gateway to eastern and northeastern regions and proximity to a planned subsea cable landing station expected by 2026. Hyderabad is projected to grow by 47%, driven by IT, ITeS, and manufacturing expansion.

CLUSTERS GIVE WAY TO DISTRIBUTED BUILDOUTS

Despite this shift, capacity remains concentrated. According to a KPMG report, Mumbai and Chennai together account for over 70% of India's installed data centre capacity. This concentration is driven by subsea cable connectivity and established ecosystems.

Operators are, however, increasingly deploying smaller, modular facilities in Tier 2 and Tier 3 cities to support low-latency services such as 4K streaming, online gaming, and IoT workloads.



“The shift toward tier-2 and tier-3 markets is driven primarily by power availability and greater latency tolerance for certain workloads.”

DOUGLAS DONNELLAN

Research Analyst, Uptime Institute



“Operators are prioritising cities that can offer reliable power, strong fibre backbones, and the ability to scale over time.”

DEEPTI SEKHRI

Practice Director, Everest Group

ResearchAndMarkets estimates the Indian data centre market will grow from USD 9.79 billion in 2025 to USD 21.03 billion by 2031. Key cities such as Mumbai, Navi Mumbai, Hyderabad, Chennai, and Pune continue to attract investment from providers such as ST Telemedia, NTT Data, and Equinix. At the same time, constraints are becoming more visible. Water availability is emerging as a critical constraint, with a 1 MW data centre requiring an estimated 25.5 million litres annually.

Mumbai accounts for nearly 40% of operational capacity, followed by Chennai at around 20%. Both benefit from subsea cable landings but face land and cost pressures. Mordor Intelligence indicates that 15 of India's 17 active subsea cables land along Mumbai's Versova coast, where land availability is limited and expensive.

Operators such as Colt Data Centre Services have faced delays assembling contiguous parcels in Navi Mumbai, while similar constraints exist along Chennai's IT corridor, compounded by environmental clearances for backup systems.

This raises a key question: can Tier 2 and Tier 3 cities provide a viable pathway for expanding existing footprints and establishing new data centre capacity?

POWER RESHAPES DATA CENTRE LOCATION LOGIC

Deepti Sekhri, Practice Director at Everest Group, describes expansion into Tier 2 and Tier 3 cities as a structural shift in India's data centre landscape, driven by evolving demand and improving infrastructure maturity. “While Tier 1 cities continue to anchor large-scale and latency-sensitive deployments, additional cities are emerging as viable options as power availability, network connectivity, land access, and policy support improve. This shift supports broader digital growth while helping balance capacity across geographies.”

Douglas Donnellan, Research Analyst at Uptime Institute, attributes this shift primarily to power availability, along with lower land costs, policy incentives, and greater tolerance for latency in select workloads. These locations also enable faster permitting and access to dedicated power capacity, easing constraints in Tier 1 markets.

A real estate consultant highlights the cost advantages. Selling prices range between Rs 15,000 and Rs 25,000 per sq ft in Gurgaon, compared with Rs 9,000 to Rs 14,000 per sq ft in Jaipur. Office rentals show a similar gap, at Rs 90–120 per sq ft in Gurgaon versus Rs 40–65 per sq ft in Jaipur.

From an operator perspective, the shift reflects a strategic recalibration. Narendra Sen, Founder and CEO of RackBank and NeevCloud, says cities such as Raipur and Indore offer scalable power, lower network congestion, and proximity to users. “They also help de-risk operations from metro-centric outages and infrastructure saturation.”

He adds that land costs in Mumbai can reach Rs 30 crore per acre, while land in inland locations is more economical. “By moving inland, we reduce the total cost of ownership by up to 40%. These locations are geologically stable, offer surplus power, and maintain lower ambient temperatures for much of the year.”

Sanjay Agrawal, Head Presales and Chief Technology Officer at Hitachi Vantara India and SAARC, notes that as Tier 1 capacity matures, expansion is extending into adjacent corridors and emerging cities. “These locations are becoming integral to a distributed digital architecture, bringing data platforms closer to where data is generated and consumed, while maintaining consistent standards of security and resilience,” he says.

Investment is being driven by colocation providers, hyperscalers, infrastructure developers, and state



“Future data centres will increasingly favour regions with stronger energy access, natural cooling potential, green power options, and structurally lower land costs.”

VINEET MITTAL

Senior Vice President, Ziroh Labs

governments. Sekhri notes that state governments are positioning data centres as strategic infrastructure to attract digital ecosystems, while hyperscalers are exploring these markets to support regional workloads, improve latency, and enhance resilience rather than replace Tier 1 hubs.

Mordor Intelligence estimates medium-sized facilities will grow at a CAGR of 19.22%, driven by edge deployments in Tier 2 cities that reduce latency for OTT services and support Internet of Things use cases. This points to a distributed model where mid-sized facilities complement large campuses, with AI workloads split between central hubs and regional nodes.

Vineet Mittal, Senior Vice President at Ziroh Labs, says future facilities may shift towards regions offering natural cooling and lower land costs. “India is attracting hyperscale data centres due to lower land and service costs, potential for green energy, and strong global connectivity through subsea cables.” He also highlights the need for energy-efficient micro data centre models.

Amit Agrawal, President at Techno Digital, says emerging cities are becoming integral to the national data centre footprint. “Tier 2 and Tier 3 locations are becoming an important part of the national data centre footprint. This is where edge infrastructure becomes critical,” he says, citing deployments across 102 cities in partnership with RailTel.

However, this transition is not a direct replication of metro models.

INLAND SCALE DEMANDS NEW OPERATING MODELS

Operators are recalibrating expansion strategies to balance land costs, grid access, and latency targets. Large campus developers are favouring coastal or power-rich inland corridors, where subsea connectivity or renewable energy clusters support long-term resilience.

Medium-scale deployments are increasingly centred on brownfield sites with strong fibre backbones that can be deployed within 12 to 18 months. Sustainability is also influencing design, as water-efficient cooling and on-site solar scale more predictably in the 20–50 MW range. These factors are shaping a two-tier deployment strategy, anchoring capacity in major hubs while extending smaller nodes into consumption zones, as outlined in the Mordor Intelligence.

According to S&P Global estimates from June 2025, key hubs such as Maharashtra, Telangana, and Karnataka account for nearly 70% of India’s operational data centre capacity. These regions offer incentives, including capital and operational expenditure subsidies, land and building concessions, single-window clearances, electricity duty waivers, and assured power supply with backup options. These advantages have driven concentration in Tier 1 cities and will need to be sustained as expansion continues.

However, this model holds only where grid reliability, skilled labour, and network redundancy are firmly in place, making it a selective rather than universal approach, as Donnellan cautions. A corporate real estate consultant adds that Tier 2 and Tier 3 cities, despite cost advantages, still face gaps in workforce, network depth, and supporting infrastructure.

Mittal argues that the transition depends on extending high-capacity and reliable grid infrastructure into these regions, making grid availability the key enabler rather than land or cooling. Without this, the shift may slow despite favourable economics.

While the appeal of newer locations may be strong, but operating in these environments requires careful planning and resilience. 🌱

pratimah@cybermedia.co.in

Global 5G IoT market to touch USD 85 billion by 2036

Enterprises are scaling 5G IoT beyond trials to cut downtime, improve efficiency and gain real-time supply chain visibility, reshaping industry operations.

BY V&D BUREAU

The global 5G Internet of Things (IoT) market is projected to grow from USD 8.1 billion in 2026 to USD 85 billion by 2036, expanding at a compound annual growth rate of 26.5%, driven by enterprise adoption of Industry 4.0 technologies, according to Fact.MR report.

The growth reflects a shift from pilot deployments to large-scale commercial adoption, as enterprises integrate 5G connectivity into industrial operations to improve efficiency, enable predictive maintenance, and enhance supply chain visibility.

The report identifies manufacturing as the primary driver of demand, with companies embedding sensors across production systems to monitor performance and detect faults in advance. This approach is helping reduce unplanned downtime by up to 30%, the report noted.

Besides, the expansion of 5G IoT is enabled by improvements in network capabilities over legacy technologies such as 4G and Wi-Fi.

The report highlighted that ultra-reliable low-latency communication is supporting applications that require near real-time responsiveness, including remote healthcare procedures, autonomous mining operations, and industrial robotics.

Smart city deployments are also contributing to market growth, with connected systems being used for traffic management, utility networks, and public safety. The ability of 5G networks to support high device density is enabling real-time monitoring and control of urban infrastructure.

connectivity currently dominates the market, accounting for 74% of deployments. However, it also pointed to a shift towards wide-area connectivity, supported by technologies such as network slicing. This allows operators to create dedicated network segments for specific enterprise applications, ensuring reliability for critical infrastructure.

The report identified edge computing as an emerging trend, with enterprises combining 5G connectivity with local data processing capabilities. This reduces latency and supports faster decision-making for applications such as autonomous systems and industrial automation.

In terms of regional dynamics, China is projected to record a compound annual growth rate of 27.6% through 2036, supported by extensive 5G infrastructure deployment.

The United States holds a 24.5% share of the North American market, driven by adoption in healthcare IoT and logistics. Germany and Japan are seeing increased deployment of private 5G networks, particularly in automotive and electronics manufacturing.

The competitive landscape includes telecom and technology companies such as Ericsson, Nokia, Huawei, AT&T, Verizon, Cisco, Qualcomm, Intel, Samsung, and Sierra Wireless. The report noted that vendors are increasingly focusing on integrated offerings that combine connectivity, hardware, and cloud capabilities.

The report indicates that 5G IoT will form a core layer of global digital infrastructure by 2036, as enterprises scale connected systems across industries. 🌐

NETWORK EVOLUTION AND REGIONAL TRENDS

The Fact.MR report highlights that short-range IoT

feedbackvnd@cybermedia.co.in

DATAQUEST APRIL 2026 EDITION: THE RISE OF THE AUTONOMOUS ENTERPRISE Where digital labour meets human wisdom

ALSO READ MORE ON

- AI Without Subtitles: For how long? Why explainability still matters
 - Forget the Genie, Read The AI Bottle's Label - D D Mishra
 - Horse-Whisperers Win. Cat-Herders Lose - Madhu Murty Ronanki
- The Doorman may open the gates for AI, but he never leaves - Nikhil Dev
 - The Marketing Team of Tomorrow Is Being Built Today
 - Are You Ready for Sovereign AI?



Scan QR Code
& Subscribe now...

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

<https://shorturl.at/vn6tN>

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



Dataquest



dataquestindia

Leverage Dataquest platform & network

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



#ImpactingICTfor4Decades

For Subscription queries:

subscriptions@cybermedia.co.in

9289870545

India turns to AI infrastructure for data-driven governance

AI integration across platforms is enabling real-time querying, automated analysis, and improved decision-making across India's public data ecosystem.



BY SHUBHENDU PARTH

India is expanding the use of artificial intelligence (AI) across national data platforms, statistical systems, and public service delivery, as part of a broader effort to improve data access, analysis, and governance. The developments indicate a transition from data access platforms to AI-driven systems that support querying, analysis, and decision-making.

Recent initiatives by NITI Aayog and the Ministry of Statistics and Programme Implementation (MoSPI) reflect the adoption of AI-based interfaces for natural language search, direct querying, and context-based information access.

According to a PIB report, key initiatives include AI-enabled search, chatbot interfaces, and machine learning tools integrated into platforms such as e-Sankhyiki and the National Data and Analytics Platform (NDAP). Similarly, the National Statistics Office introduced a Model Context Protocol server on the e-Sankhyiki portal in February 2026, enabling users to query datasets directly using AI tools without downloading large files.

The system provides access to 21 statistical products and supports automated reporting and data integration across systems. AI-based semantic search and chatbot

India's public data ecosystem is evolving into an AI infrastructure, where models, platforms, and pipelines work together to enable real-time intelligence at scale.

features have also been deployed to improve user interaction with official statistics.

These tools enable natural language queries and context-based responses, reducing the complexity of accessing government datasets. NDAP, which integrates datasets across 52 ministries and 31 sectors, is being upgraded in its next phase with AI-driven analytics, visualisation tools, and search capabilities.

Beyond access, AI is being used to improve statistical operations. An AI-based classification tool for National Industrial Classification codes uses natural language processing to generate relevant category suggestions, reducing manual effort and improving survey accuracy.

Government organisations are also deploying systems that enable intelligent search across official documents. At the same time, separate tools extract legacy data from formats such as PDFs and images and store it in structured databases for analysis.

AI ADOPTION ACROSS SECTORS

Sectoral deployments indicate wider adoption of AI across public services. In healthcare, the Benchmarking Open Data Platform for Health AI (BODH), launched in February 2026, supports the evaluation of AI models using anonymised datasets under the Ayushman Bharat Digital Mission framework. Similarly, the Strategy for AI in Healthcare for India (SAHI) provides a governance framework for the safe and compliant deployment of AI in healthcare.

In agriculture, Bharat-VISTAAR and the National Pest Surveillance System are being used for advisory services and crop monitoring, while Kisan e-Mitra provides multilingual support for farmer queries.

In meteorology and disaster management, the India Meteorological Department and institutions under the Ministry of Earth Sciences are applying AI-based systems for weather and climate forecasting. These include tools for cyclone intensity estimation, precipitation modelling, and early warning systems, as

well as applications in fog forecasting, lightning alerts, and fire prediction, the PIB report stated.

At the infrastructure level, BharatGen, a multilingual large language model supporting 22 Indian languages, is being developed to support public and developmental use cases.

AI IN DIGITAL IDENTITY AND AADHAAR

The Unique Identification Authority of India (UIDAI) introduced an AI-based biometric deduplication and document verification platform in February 2026 as part of its digital identity infrastructure. The platform is designed to improve enrolment and update accuracy by strengthening biometric matching across fingerprint, face, and iris modalities.

UIDAI has completed enhanced deduplication rollouts in several states and is expanding deployment nationwide. It has also initiated a broader technology roadmap under the Aadhaar Vision 2032 framework, which includes integrating artificial intelligence, blockchain, quantum computing, and advanced encryption systems to enhance scalability and data security.

INSTITUTIONAL CAPACITY AND AI ECOSYSTEM

Institutional frameworks are being expanded to support AI adoption across government systems. The Data Innovation Lab is supporting experimentation, partnerships, and deployment of AI use cases across statistical and data platforms, with 17 memorandums of understanding signed and multiple applications under development.

Capacity-building programmes under Mission Karmayogi and training initiatives at the National Statistical System Training Academy are being expanded to equip officials with skills in AI, machine learning, and data analytics.

These initiatives reflect a shift from data availability to "intelligent data usability", with AI emerging as a foundational layer across India's digital public infrastructure. 🌐

shubhendup@cybermedia.co.in

Nvidia expands AI Grid focus for telco networks

AI Grid pushes telcos beyond AI RAN, shifting to edge models to cut costs, control data, and test new revenue streams.

Nvidia has expanded its telecom strategy beyond AI-RAN to an AI Grid model aimed at distributed infrastructure, as outlined at GTC 2026, with operators and vendors outlining deployments and use cases.

The company is building a partner ecosystem that includes SoftBank, T-Mobile and Comcast, alongside vendors, to support AI workloads at the network edge. Operators cited revenue opportunities linked to edge-based AI services.

The AI Grid model shifts processing from cell sites to distributed edge nodes to reduce cost per token and improve utilisation. Several operators, including AT&T,

Spectrum and Indosat Ooredoo Hutchison, outlined plans to deploy AI Grid infrastructure.

Agentic AI formed a central theme. Nvidia's Nemotron-based large telco model is being used by operators including Cassava Technologies, NTT Data and Telenor to train AI agents for network optimisation, including traffic management and security. The model has 30 billion parameters and is open source, which could affect vendor-led solutions.

Partnerships with Nokia, Ericsson and Samsung formed part of a broader ecosystem across cloud, data and edge infrastructure. Nvidia is also engaging in early discussions on 6G network design.

Geopolitical factors are influencing infrastructure deployment, with operators in regions including Canada, Saudi Arabia and Singapore focusing on sovereign infrastructure.

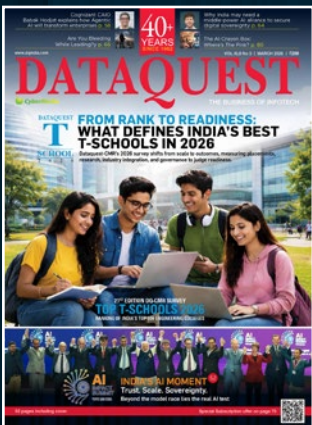
Operators presented edge-based use cases including AI assistants, smart city video analytics and distributed media processing. Comcast outlined applications such as small business AI tools, advertising and low-latency gaming using small language models at the edge.

The adoption of AI Grid will depend on whether operators can generate revenue from these deployments.



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

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



DATAQUEST
Enterprise &
Tech Leadership



PCQUEST
CIOs, Tech
Influencers & SMBs



VOICE&DATA
Telco & Digital
Infra Leaders



DQCHANNELS
ICT Partners &
Channel Decision Makers

OUR BESPOKE B2B MARKETING PROGRAMMES BUILD, ENGAGE AND SCALE COMMUNITIES

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

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

DELIVER INFLUENCE AND OUTCOMES WITH CYBERMEDIA

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

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

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

Partnerships & Advertising Enquiries

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



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

Affiliated to I.K Gujral Punjab Technical University (IKG-PTU), Kapurthala
Approved by AICTE, MOE | NAAC Accredited | Recognised by UGC under 2(f)



REGISTRATIONS OPEN 2026

Build a successful career with **AIMETC**

PROGRAMMES OFFERED



MANAGEMENT

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



COMPUTER APPLICATION

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



ENGINEERING & TECHNOLOGY

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

SOME OF OUR KEY RECRUITERS



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

Scan for website



For more details, please contact us:

Apeejay Institute of Management & Engineering Technical Campus, Rama Mandi,
Hoshiarpur Road, Jalandhar - 144007

Email: aim.jln@apj.edu | Phone: +91-9569-181-181