

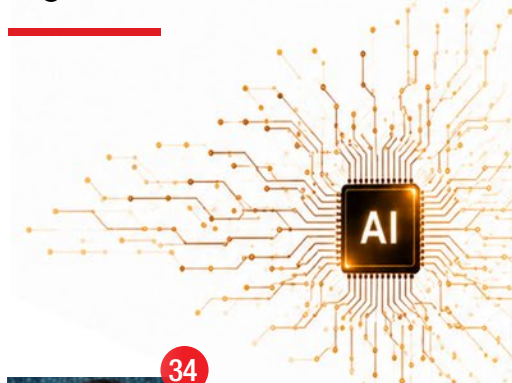
VOICE & DATA

Connecting the Digital World



MAINFRAMES ARE BACK

Quantum risks, AI workloads and data sovereignty are giving the enterprise workhorse a new role across modern digital infrastructure.



34

"One of the biggest constraints for AI is the network"

SAMIR MISHRAManaging Director, Enterprise,
Cisco India & South Asia

48

"AI is pushing security deeper into the network"

David HughesSVP – SASE and Security,
HPE Networking



UGC Recognised
12(B) Status from UGC

Apeejay Stya University

SOHNA, GURUGRAM | Estd. 2010



PROGRAMMES OFFERED

Engineering & Technology | Journalism & Mass Communication | Design & Visual Arts | Biosciences | Education |
Management Sciences | Pharmaceutical Sciences | Legal Studies | Behavioural Sciences | Arts & Sciences

ADMISSION OPEN 2026-27



KEY HIGHLIGHTS

- Liberal Arts Integrated Curriculum
- Cutting-Edge Teaching Methodologies
- AC Transport Facility Across Delhi NCR
- World-Class Technology-Enabled Campus
- Excellent Training, Internships & Placement Support
- Future-Ready Education with Strong Industry Collaboration
- Experiential Learning Through Projects & Practical Exposure
- Industry-Oriented Curriculum Aligned with Emerging Careers
- Among India's Leading Top 100 Universities — IIRF Ranked Indian Institutional Ranking Framework

Empowering Bright Minds with Attractive Merit based Scholarships

(For more details, please refer to the ASU website)

Admission Helpline No:
1800-103-7888



Ranked 3 in the State and 7 in North India among top 100 private universities in India by the Indian Institutional Ranking Framework (IIRF) 2023

For admissions, please contact us:

Apeejay Stya University, Sohna - Palwal Road, Sohna - 122103, Gurugram
Email: admissions@asu.apeejay.edu | Website: university.apeejay.edu

Follow us on:





THE INDIAN NEWSPAPER SOCIETY

VOICE & DATA
Connecting the Digital World

Lies try to
disguise themselves
as the sensational truth.
But we all seek the truth.
That's why every word
we print is corroborated,
verified, and only
then put to paper.
Between these lines,
there is no room
for falsehood.
Here, what's written
and what's true are always
the same thing because

Nothing but the truth.

Ink Doesn't Lie



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

HEAD - AI TRANSFORMATION & CONTENT STUDIO: Sudesh Prasad
VICE PRESIDENT RESEARCH: Anil Chopra

MANAGER CYBERMEDIA LABS: Ashok K Pandey

LARGE BUSINESS CONVENTIONS & PROJECTS
CONFERENCE PRODUCER: Ajay Dhoundiyal

BUSINESS SOLUTIONS & SALES
GM - BUSINESS SOLUTIONS: Rajnish Jamur
SR MANAGER: Ajay Dhoundiyal (North)
SR MANAGER: Sudhir Arora (North, East)
SR. MANAGER: Anita Swamy (South)

MARKETING & ALLIANCES
SR MANAGER: Ajay Dhoundiyal

EVENTS, OPERATIONS & COMMERCIALS
GM, EVENTS & SPECIAL PROJECTS: Ankit Parashar
SR. MANAGER - ONLINE AD OPERATIONS: Suneetha B S
AUDIENCE ACQUISITION & EVENT OPERATIONS: Bibhuti Kumar
EXECUTIVE EVENTS OPERATIONS: Aditya Mishra
CREATIVE DESIGN: Sunali
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: Priyanshi Goyal, Diksha
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 Kuria 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)

August-September 2026

[CONTENTS]

COVER STORY **26**

MAINFRAMES ARE BACK

Quantum risks, AI workloads and data sovereignty are giving the enterprise workhorse a new role across modern digital infrastructure.



INDUSTRY SPEAK

08 India's connectivity future takes a multi-orbit turn

11 Securing OT behind India's telecom and digital infrastructure

14 AI is changing what network observability must deliver

[COMMENTARY]

38 Connected data, not smarter AI, will win healthcare's race

42 Cloud discipline becomes the new currency of digital growth

46 Can Agentic AI crack quantum computing's use-case puzzle?

[TECHNOLOGY]

52 Outside-in testing exposes digital infrastructure blind spots

55 AloT convergence moves intelligence closer to the action

58 Distributed infrastructure puts observability to a new test

60 Beyond GPS, real-time visibility becomes the new standard

REPORT

18 India scales telecom manufacturing but value add stays low

20 Parliament panel seeks BharatNet audit over rollout gaps

TELECOM TALK



22 Right of Way reform holds key to India's digital growth

LT. GEN. DR. SP KOCHHAR

INTERVIEW



34 "One of the biggest constraints for AI is the network"

SAMIR MISHRA



48 "AI is pushing security deeper into the network"

DAVID HUGHES

FOCUS

64 India's defence drone push moves deeper into the tech stack

NEWS ANALYSIS

70 AT&T's trillion-token play rewrites network intelligence

REGULARS

06 Voicemail

07 Opening Note

74 Postscript

[NEXT ISSUE]



JULY 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**.

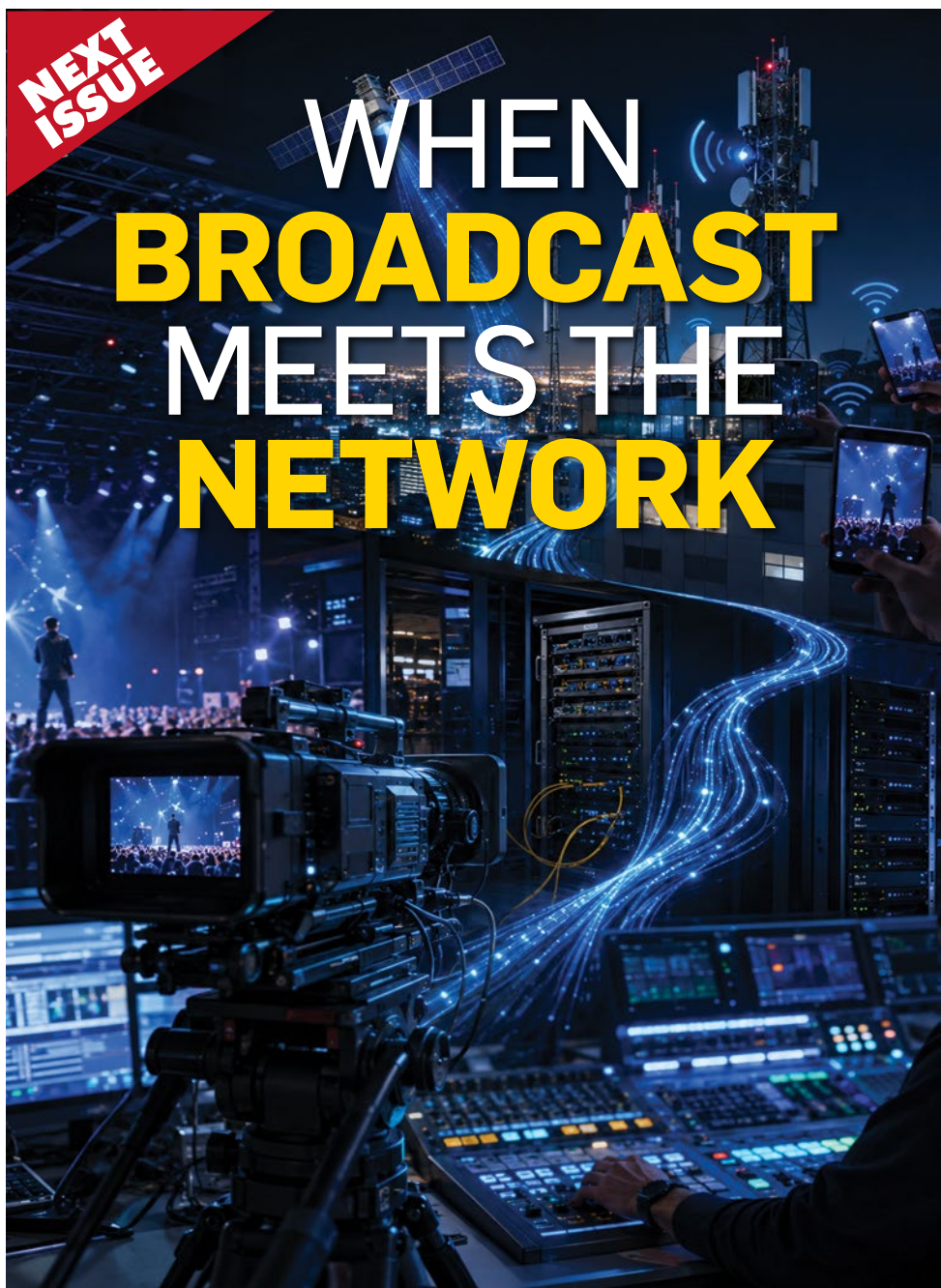
You can also write to
Reader Service Executive, **VOICE&DATA**,
Cyber House, B-35 Sector 32,
Gurgaon-122 003, Haryana
Tel: 9953150474, 7993574118



Share your views at vndedit@cybermedia.co.in

NEXT
ISSUE

WHEN BROADCAST MEETS THE NETWORK



For any query: ajaydh@cybermedia.co.in



SHUBHENDU PARTH [OPENING NOTE]

The ‘Future is for Everyone’ but on whose terms

Imagine an Artificial Intelligence (AI) agent that understands your needs, manages aspects of your finances and health, teaches you new skills, and gives you capabilities once available only to large organisations. Now imagine billions having one. This is the vision Mark Zuckerberg present in his essay *The Future is for Everyone*, built around a compelling proposition: superintelligence should empower individuals rather than remain concentrated with governments, corporations, or a few institutions.

Yet another message runs through the essay. While arguing for decentralising AI power, he makes an explicit case for American leadership. He supports silicon export controls that constrain foreign competitors, wants faster US energy and data centre development, cautions against regulations delaying American model releases, and wants the US and its allies to lead the open-source AI ecosystem.

This is where AI intersects with the infrastructure economy. Intelligence may be delivered as software, but producing it requires semiconductors, compute, data centres, power, cooling, fibre, cloud infrastructure, and telecom networks. With compute remaining finite, countries and companies controlling this infrastructure could influence the economics and availability of AI.

There is nothing unusual about an American technology executive advocating his country's interests. What merits examination is the difference between democratising access to intelligence and democratising control over its foundations. While billions may have access to personal AI agents, will the infrastructure powering those remains concentrated within a handful of companies and countries?

That distinction resonates in India, where Meta and the government are confronting questions around content moderation, algorithmic accountability, intermediary liability, and the applicability of Indian law to global platforms. Facebook's temporary restriction of a video featuring Prime Minister Narendra Modi, for which Meta apologised, has brought platform power into sharper focus.

While his essay should not be interpreted as a response to India's regulatory actions, India certainly provides a useful test for its balance-of-power thesis.

His proposition positions individuals against institutional and government power. The digital ecosystem, however, has another powerful institution: the technology platform. Algorithms already influence what billions see and discover. Personal AI agents capable of advising, deciding, and acting for users could make accountability more consequential.

The equation increasingly involves citizens, platforms, governments, and infrastructure owners. None should possess unchecked power.

For India, the emphasis on American leadership is also a reminder that AI sovereignty cannot be measured merely by access to models. Open models may expand choice, but dependence persists if compute, semiconductors, clouds, and critical infrastructure are controlled elsewhere.

India consequently has an economic opportunity as much as a strategic challenge. Building compute, data centres, power, fibre, telecom networks, semiconductor capabilities, and edge infrastructure can create an AI infrastructure economy while strengthening domestic capacity and reducing critical dependence.

Zuckerberg says the future is for everyone. Perhaps. But as intelligence becomes infrastructure, India must ask not only who gets access to AI, but who builds, owns, and controls what powers it.

shubhendup@cybermedia.co.in

India's connectivity future takes a multi-orbit turn

LEO and GEO bring complementary strengths in latency, coverage and mobility, creating a more adaptable architecture for resilient connectivity.



BY P. J. NATH

India has reached an important point in its digital journey. With more than a billion broadband users and digital public infrastructure operating at population scale, expectations around network reliability and reach have fundamentally shifted. The challenge is increasingly not only to extend connectivity, but to maintain it across different geographies and operating conditions.

India's diverse geography makes that difficult. From the high Himalayas to vast maritime boundaries, terrestrial fibre and towers face structural and economic limits in areas where deployment can be impractical or commercially unviable.

The emerging question, therefore, is how different network layers can complement one another to provide greater continuity. This is where multi-orbit connectivity becomes relevant. Satcom service providers are

integrating Low Earth Orbit (LEO) satellite services into their portfolios and will be able to combine them with existing Geostationary Earth Orbit (GEO) capabilities once commercial LEO services become available in India.

HOW LEO CHANGES THE SATELLITE EQUATION

Globally, LEO constellations are expanding what satellite networks can deliver. Their proximity to Earth enables lower latency, high throughput for data-intensive applications and greater support for mobility and edge connectivity.

But LEO should not be viewed in isolation. India's connectivity requirements vary significantly across geography, industries and applications, and no single network technology can address all of them.

This is the power of 'and'.

The real multi-orbit opportunity is not choosing between LEO and GEO, but assigning each workload the right mix of latency, coverage and resilience it needs.

A hybrid multi-orbit approach can combine emerging LEO capabilities with established GEO networks. LEO can address applications requiring lower latency and responsiveness, while GEO can provide wide-area coverage and connectivity across large geographies. Used together, the two can provide different layers of connectivity according to application and operational requirements.

The opportunity, therefore, is not simply to add another satellite technology. It is to build an architecture in which different orbital layers can complement one another and, where appropriate, work alongside terrestrial networks.

MATCHING ORBITS TO CONNECTIVITY NEEDS

The potential value of such architecture becomes clearer when viewed through different operating environments.

For national digital infrastructure and public services, multi-orbit networks could extend digital services into remote geographies. LEO could support responsive, high-speed access for telehealth, financial inclusion points and mobile governance units, while GEO provides wide-area connectivity for public-service delivery.

Disaster preparedness and emergency response present a different requirement. During floods, cyclones and extreme weather events, lower-latency satellite connectivity could support data feeds, field coordination and situational updates when terrestrial links are damaged. GEO connectivity can provide another layer for early-warning systems, emergency command centres, shelters and medical teams.

National security and border management bring together mobility, difficult terrain and mission-critical communications. In high-altitude and border regions, LEO could support tactical communications, sensor fusion and intelligence, surveillance and reconnaissance data transport for forces on the move. GEO can complement this with wide-area coverage, redundancy and backhaul for forward bases.

The same principle extends into industrial operations. Mines, manufacturing facilities, offshore platforms and



IN BRIEF

- India's connectivity challenge is shifting from extending reach to ensuring continuity where terrestrial networks face practical limits.
- LEO brings lower latency and responsiveness, opening new possibilities for mobile, remote and time-sensitive connectivity across India.
- GEO adds wide-area coverage and continuity, making the opportunity less about choosing an orbit and more about combining strengths.
- From disaster response to defence and industry, different operating needs can use the network layer best suited to each task at hand.
- Software-defined satellites could shift capacity as demand changes, making orbital resources more adaptable across events and emergencies.
- The real promise is seamless handoff across LEO, GEO and terrestrial layers, so applications stay connected as conditions change today.

energy corridors increasingly depend on connected operational technology, remote asset monitoring and data-driven automation. Here, the combination of LEO and GEO could balance responsiveness with wider coverage and business continuity.

A network may eventually hide the orbit from users, shifting across satellite and terrestrial layers while applications simply remain connected to services.

Mobility creates another set of requirements. Aircraft and ships require connectivity across flight paths and oceans where terrestrial networks are unavailable. LEO can support higher-speed inflight and maritime communications, while GEO can provide wider coverage and service continuity.

Agriculture and rural commerce can similarly benefit from connectivity spanning large and often dispersed operating areas. Hybrid networks can support data from sensors, fleets and supply chains while extending connectivity to rural banking networks, agricultural marketplaces and remote operations.

Logistics, retail and fast-moving consumer goods operations bring these requirements closer to the supply chain. LEO could support fleet telematics, cold-chain visibility, railway asset tracking and warehouse operations in locations with limited terrestrial infrastructure. GEO can provide wide-area connectivity for ports, intermodal hubs and distributed field operations.

The common requirement across these applications is not that every workload should use the same orbit. Instead, the network architecture should be able to match different connectivity characteristics with different operational requirements.

ADDING INTELLIGENCE TO MULTI-ORBIT NETWORKS

The evolution of satellite infrastructure is also increasingly about how network resources are managed.

Software-defined satellite systems can dynamically shift capacity according to demand, whether towards a disaster zone, a large sporting event or a busy shipping lane. This ability to respond to changing traffic patterns introduces greater adaptability into satellite networks.

Combined with a multi-orbit approach, such capabilities point towards networks in which connectivity is not tied rigidly to one infrastructure layer. Different satellite resources can address different requirements,

while terrestrial 5G can remain part of the broader connectivity environment.

This makes the handoff between networks important. For users and applications, the objective is not to determine whether connectivity is being provided through LEO, GEO or terrestrial infrastructure at a particular moment. What matters is whether the underlying architecture can maintain the required level of service as operating conditions change.

DESIGNING NETWORKS AROUND CONTINUITY

India's digital ambitions increasingly require infrastructure designed not simply for reach, but for continuity, reliability and adaptability. Multi-orbit connectivity provides an opportunity to combine the different characteristics of LEO and GEO rather than treating them as competing satellite technologies.

The availability of commercial LEO services would add another layer to India's connectivity architecture. Their value will depend on how effectively they can complement existing GEO capabilities and terrestrial networks across applications that have different requirements for latency, coverage, mobility and resilience.

The larger shift is, therefore, from thinking about satellite connectivity in terms of individual technologies to considering how multiple network layers can operate as one architecture. The objective is an 'invisible handoff', where applications can remain connected without the underlying network becoming the user's concern.

India's geography will continue to present connectivity challenges. A multi-orbit approach does not remove those constraints, but it offers a different way of designing around them. In that sense, the future of resilient connectivity will be shaped not by choosing one orbit over another, but by how intelligently different orbits and terrestrial networks can work together. 🌐

The author is the Managing Director and CEO of Nelco.

feedbackvnd@cybermedia.co.in



Securing OT behind India's telecom and digital infrastructure

As India scales 5G, data centres and AI infrastructure, ageing industrial control systems could leave critical power and cooling systems vulnerable to attack.



BY DAVID SEHYEON BAEK

India's digital economy is expanding rapidly. Telecom operators are extending 5G coverage, data centres are multiplying across major cities, and AI services are driving demand for computing power. Yet the physical systems supporting this growth remain less protected than the cloud platforms, applications and enterprise networks built above them.

A campaign against US critical infrastructure illustrates why this matters. In July 2026, US authorities

warned that cyber actors assessed to be affiliated with Iran and linked to the Islamic Revolutionary Guard Corps were exploiting internet-connected programmable logic controllers used in government facilities, water and wastewater systems, and energy installations.

While state attribution in cyber operations is rarely absolute, the operational methods documented in the campaign and the risks they created warrant close attention.

Industrial systems built for isolated networks are increasingly connected for remote management, creating new attack paths across critical infrastructure.

A compromised PLC can keep equipment running while showing operators normal readings, allowing dangerous physical conditions to develop unnoticed.

The actors reportedly targeted PLCs from Rockwell Automation, Schneider Electric and Siemens that were reachable from the public internet. Rather than relying on exotic malware or unknown software flaws, they used legitimate engineering tools designed to configure and manage those devices. Once connected, they downloaded project files containing the logic governing pumps, valves, alarms, shutdown routines and physical processes.

They then modified that logic and redeployed it to the affected controllers. In some cases, the changes preserved enough normal functionality to avoid detection while overriding instructions responsible for safe operating conditions. Alarm and shutdown functions were reportedly disabled, while information shown on HMI and SCADA screens was altered so operators could see normal readings even when the underlying process had become unsafe.

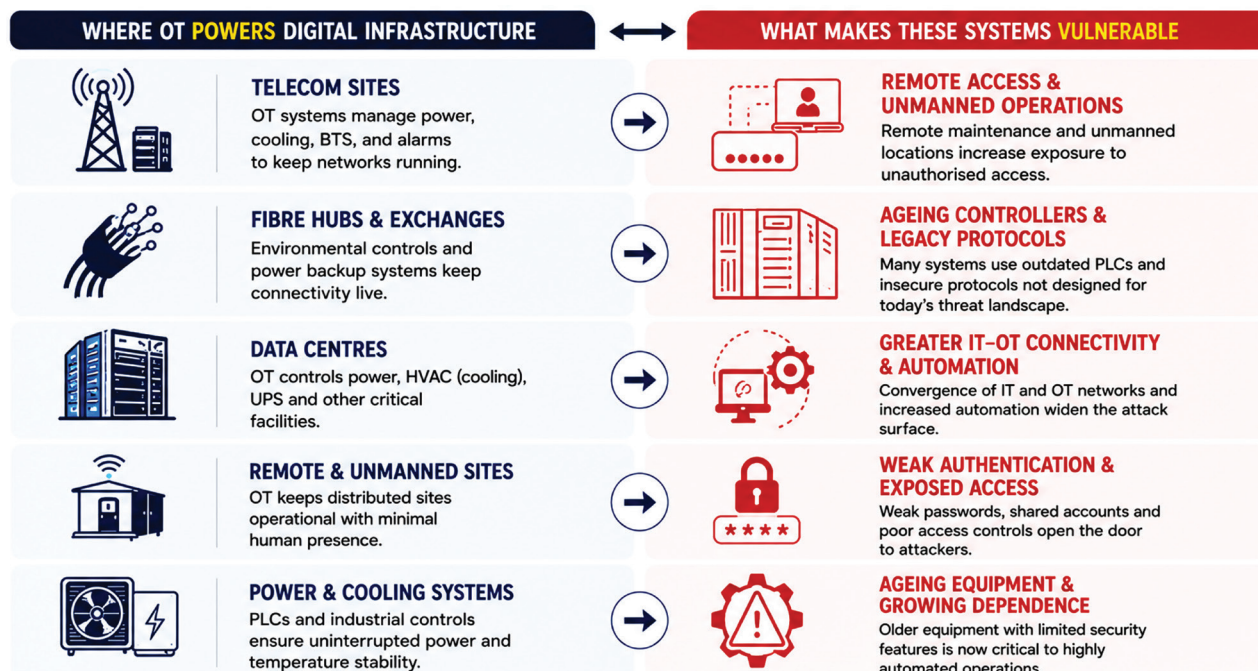
The risk was not merely that a system could stop working. It was that the machine could continue operating while giving its operators false information.

HOW OT ATTACKS TURN INTO PHYSICAL RISK

This distinction is important. Information technology manages data, communications, applications and processes. Operational technology controls physical equipment and industrial processes. A compromised email server can expose confidential information. A compromised PLC can change chemical dosing, shut down cooling, alter power distribution or disable a safety mechanism. The consequences can move from the digital domain into physical damage, service disruption and public safety.

Many PLCs and industrial devices remain vulnerable because they were designed for a different era. Some have been operating for ten, twenty or even thirty years. Their designers assumed they would sit inside isolated industrial networks where only trusted engineers could reach them.

Protocols such as Modbus TCP, BACnet/IP and older implementations of SNMP were built around that assumption. Authentication was weak or absent,



OT incidents cannot be handled by cybersecurity teams alone; engineers who understand physical processes, safety systems and recovery must also be involved.

encryption was uncommon, and logging was not considered essential.

WHY DIGITAL INFRASTRUCTURE IS EXPOSED

The technology may be old, but dependence on it is growing. Telecom networks rely on generator controllers, cooling systems, environmental sensors and remote automation at switching centres, fibre hubs and tower sites. Data centres depend on building management and electrical power management systems to operate chillers, power distribution units, batteries, generators and switchgear.

If these systems are manipulated, the result may be a regional network outage, a data hall shutdown or physical damage.

The harder problem is that operational habits do not change easily. Remote access is convenient. Shared passwords reduce administrative friction. Internet-connected maintenance ports allow contractors to work without travelling to distant sites.

Similarly, legacy equipment may be too costly or disruptive to replace. Operators may also fear that new security controls could interfere with uptime, which remains their primary responsibility. These decisions are understandable individually, but together they create a national attack surface.

India faces the same structural pressures. Its telecom footprint spans thousands of dispersed and often unmanned locations. Data-centre capacity is growing rapidly, while industrial automation is expanding across factories, logistics hubs, energy systems and smart-city infrastructure.

As these environments become more connected, the boundary between IT and OT becomes less clear. A stolen engineering credential, infected maintenance laptop, exposed cellular modem or weak jump server can become the bridge from an ordinary intrusion into a physical control environment.

HOW INDIA CAN STRENGTHEN OT SECURITY

India should therefore treat OT security as part of national digital infrastructure policy, not as a narrow technical issue left to individual facilities. Critical operators need accurate inventories of PLCs, modems, engineering workstations, remote access paths and exposed industrial services.

Direct internet access to controllers should be eliminated wherever possible, with remote maintenance routed through controlled gateways that enforce strong authentication, restricted privileges, logging and time-limited access.

Regulators should establish minimum OT security requirements for telecom, data-centre, energy and other nationally significant facilities. These should cover network segmentation, unique credentials, secure vendor access, protected engineering workstations, verified backups and regular integrity checks of PLC project files.

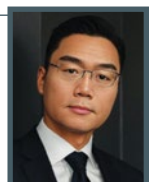
Similarly, procurement rules should require manufacturers to provide secure defaults, long-term support, audit capability and modern authentication without treating basic security as a premium option.

The country will also need sector-specific incident response capacity. OT incidents cannot be managed by IT security teams alone. Engineers who understand the physical process, safety systems and recovery sequence must be involved. Smaller operators and regional service providers will require practical support, shared expertise and specialist assistance.

India's digital ambitions depend on more than software, cloud platforms and connectivity. They depend on the machines that keep networks powered, cooled and operational. Protecting those machines is now a condition of national digital resilience. 🌱

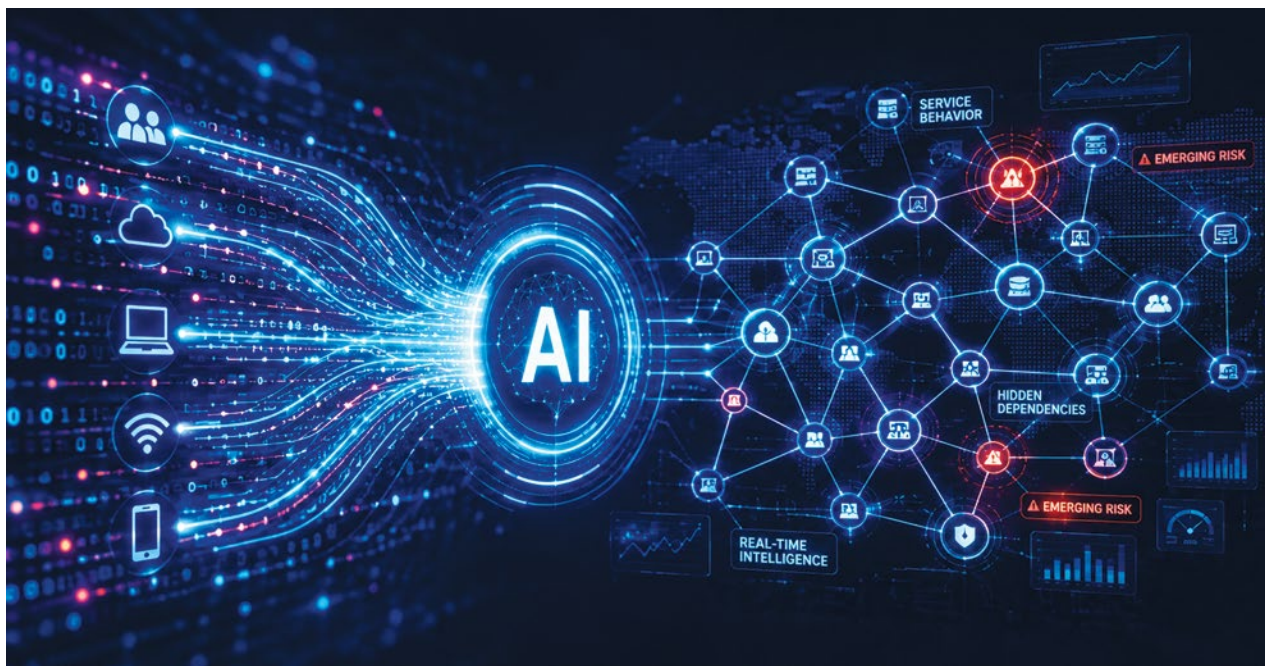
The author is the Founder and CEO of Pygmalion Global. He collaborates with multiple cybersecurity companies, including NPCore in South Korea, and engages with government agencies and conglomerates across Asia.

feedbackvnd@cybermedia.co.in



AI is changing what network observability must deliver

As AI moves into operations, live network traffic must yield high-fidelity intelligence to expose service behaviour, emerging risks and hidden dependencies.



BY GAURAV MOHAN

Artificial Intelligence (AI) is becoming integral to enterprise operations by automating routine tasks, providing insights for informed decision-making, and supporting innovation. Generative AI, Agentic AI, and intelligent automation are increasingly influencing IT operations, cybersecurity, service delivery, and customer experiences, shaping the next phase of enterprise transformation.

This evolution raises the importance of enterprise data. When AI recommends or automates an action, incomplete or inaccurate information can lead to poor decisions, service disruptions, operational risks, and unreliable outcomes.

The next wave of enterprise AI will depend less on the volume of data an organisation possesses and more

on whether that data delivers high-fidelity, real-time operational intelligence that provides a complete view of how its digital environment is performing.

WHY BETTER TELEMETRY BEATS MORE DATA

Early observability strategies were based on the idea that collecting every metric, event, log, and trace (MELT) in a central repository would improve troubleshooting. In practice, however, this often introduced greater complexity.

Although data tiering and observability pipelines helped reduce data volumes and control costs, filtering sometimes removed critical performance and security indicators needed to understand real-time network and service behaviour.

As a result, organisations are placing greater emphasis on improving data quality rather than

Collecting every metric, event, log and trace can add complexity, making enriched telemetry and operational context more valuable than sheer data volume.

simply collecting more data. One approach is to enrich telemetry at the source with protocol-aware metadata and operational context. This preserves essential information while providing clearer, more actionable insights that improve signal quality and accelerate root-cause analysis, enabling faster and more accurate downstream decisions.

WHEN DASHBOARDS STOP BEING ENOUGH

Traditional observability platforms have centred on dashboards, alerts, and reports. While these tools indicate that a problem exists, they often lack the ability to correlate information across systems or identify the underlying cause.

Observability and security platforms are evolving beyond monitoring to become AI-driven systems capable of understanding natural language, supporting business continuity, and extracting actionable insights from complex datasets.

These capabilities combine long-context models, retrieval-augmented generation (RAG), and reasoning engines to deliver conversational interfaces that guide users through multi-step investigations. Long-context models help preserve operational continuity, retrieval pipelines surface relevant information from tickets, configurations, and telemetry, while reasoning layers reduce alert noise and improve decision-making.

Moving from dashboards to predictive intelligence can improve the user experience, accelerate mean time to knowledge, shorten root-cause analysis, and support faster remediation. However, these capabilities remain dependent on the quality of the underlying data. AI systems require accurate, contextual, and high-fidelity operational intelligence to deliver reliable conclusions that organisations can trust.

EDGE COMPUTING AND REAL-TIME ANALYTICS

Edge computing is expanding beyond remote offices and branch locations to factory floors and wide area network (WAN) perimeters. Physical AI systems, robotics, autonomous devices, and connected technologies are generating workloads that cannot always be processed efficiently in distant cloud environments.



IN BRIEF

- High-fidelity telemetry enriches network data with operational context, improving signal quality and accelerating root-cause analysis.
- AI-driven observability combines long-context models, RAG and reasoning engines to correlate data and support complex investigations.
- Edge inference moves analytics closer to connected devices, enabling low-latency decisions and resilience when connectivity becomes unstable.
- AI governance requires stronger visibility across prompts, inference behaviour, encrypted traffic and east-west data movement.
- Shadow AI can create hidden dependencies, move sensitive data outside governance and automate processes without adequate IT oversight.
- Balancing edge inference with centralised training and analysis can improve availability and resilience across distributed environments.

Instead, analytics and AI inference are moving closer to where data is created, enabling real-time intelligence and faster decision-making. Synthetic data is also being used to strengthen edge AI models by recreating conditions

Moving beyond dashboards to predictive intelligence can shorten root-cause analysis, but reliable conclusions still depend on accurate contextual data.

that are difficult to capture consistently across remote and highly variable environments.

As distributed environments continue to grow, organisations must decide which functions should be executed locally and which should remain centrally managed. Immediate inference for sensors and connected devices, low-latency decision-making, and resilience during periods of unstable connectivity are well suited to edge environments. Large-scale model training, historical analysis, and compute-intensive workloads can remain centralised.

This balance helps organisations maintain service availability, operational resilience, and a consistent customer experience across increasingly distributed digital environments.

AI NEEDS GOVERNANCE BEFORE SCALE

AI-driven applications are introducing new traffic patterns and expanding the enterprise attack surface. These risks increase with prompt manipulation, data leakage, or changes in model behaviour. The challenge can be greater at remote locations where devices are more vulnerable to tampering or distributed denial-of-service (DDoS) attacks that disrupt local operations. Browsers and other local environments operating outside traditional monitoring frameworks can also create additional exposure.

To address these challenges, organisations are strengthening AI governance by validating training pipelines, implementing stronger controls over prompts, inputs, and outputs, continuously monitoring inference behaviour, and expanding visibility across encrypted and east-west traffic.

As AI becomes more deeply integrated into enterprise operations, governance provides greater visibility into data movement and unusual activity, enabling security teams to investigate threats more quickly and maintain stronger operational oversight.

THE HIDDEN COST OF SHADOW AI

The rapid adoption of AI is also contributing to the growth of Shadow AI. Whether described as AI sprawl,

uncontrolled AI adoption, or the convergence of Shadow IT and Shadow AI, the challenge remains the same: applications deployed outside organisational governance.

When employees or business units adopt AI tools independently, those systems can influence decisions, generate unverifiable outputs, or automate processes without IT oversight. This increases operational risk, particularly when sensitive or operational data bypasses established telemetry pipelines.

Although Shadow AI and Shadow IT present different risks, they also overlap. External chatbots, large language models (LLMs), and AI plug-ins can generate unverifiable outputs and unsupported automation, while unapproved software-as-a-service (SaaS) applications, browser extensions, and other Shadow IT tools create hidden dependencies, move data outside governance, and reduce organisational visibility.

Greater visibility into unknown applications, communication patterns, and data movement can help organisations support responsible AI adoption without compromising security, operational control, or digital trust.

AI is becoming embedded in everyday enterprise operations, but its value ultimately depends on the quality of the data that supports it. Organisations may possess vast amounts of information yet still lack a complete understanding of how their services behave. Making a poor decision more quickly through AI remains a poor decision.

By converting live network traffic into high-fidelity operational intelligence, organisations can gain a clearer understanding of service interactions, identify emerging issues earlier, and detect indicators of risk before they escalate. This creates a stronger foundation for AI-driven initiatives and supports more reliable decision-making across increasingly complex enterprise environments. 🧩

The author is Vice President of Sales for SAARC and the Middle East at Netscout. feedbackvnd@cybermedia.co.in





**IF
EVERYTHING
IS INSIGHT,
NOTHING IS.**

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

**A constant stream of unobserved update
overwhelms Judgement.**

**Editing and curating Information converts it
into insight.**

READ LESS. KNOW MORE.

"An Initiative by Association of Indian Magazines"

India scales telecom manufacturing but value add stays low

NITI Aayog points to low domestic value addition, import dependence, and higher costs as hurdles to building a competitive telecom equipment ecosystem.



BY SHUBHENDU PARTH

India's Telecom and Network Equipment (TANE) manufacturing remains largely concentrated in low-value assembly, with domestic value addition often below 20% despite the country's push to expand local production, according to NITI Aayog's Report on Key Sectors to Position India as a Global Manufacturing Hub.

The report indicates that manufacturers continue to import high-cost sub-assemblies and components for final integration and packaging in India, while critical capabilities in product design, research and development, and core component fabrication remain primarily overseas.

China accounts for a significant part of that exposure. India imports around USD 4–5 billion of telecom and network equipment annually, with more than 80% sourced from China for critical components such as 4G/5G antennas and signal processors, according to the report.

The report warned that the dependence exposes India to supply-chain vulnerabilities, geopolitical risks and currency fluctuations, adding a strategic dimension to the challenge of increasing domestic value addition.

The dependence on imported components also carries a cost penalty. The report estimates that Indian telecom equipment manufacturers face costs 10–15% higher than global original equipment manufacturers (OEMs) because of reliance on imported inputs such as printed circuit boards, antennas and radio frequency modules.

Processors and integrated circuits are among components for which the report identifies no domestic availability, while import dependence remains high for static converters, diodes and transistors. China is listed as the leading supplier across each of these component categories.

India's USD 25 billion domestic equipment market could double by 2032, but scale at home will mean little without much deeper local component capabilities.

The findings highlight the challenge facing India as it seeks to convert the scale of its domestic telecom market and network deployments into deeper manufacturing capabilities and a larger position in global equipment supply chains.

DEEPENING LOCALISATION BEYOND ASSEMBLY

Against this backdrop, the report proposes a localisation-linked incentive framework to reduce import dependence by encouraging manufacturers to progressively source a greater proportion of their bill-of-material components domestically.

It recommends initially focusing on non-semiconductor, plastic, insulation and electro-mechanical components before extending localisation efforts to higher-value components.

Such a shift would mark a move from encouraging primarily equipment production and assembly towards increasing the share of components and value created within India.

The report also advocates joint ventures between global OEMs and Indian companies to facilitate technology transfer and develop local capabilities, such as the Reliance Jio-Sanmina partnership.

The report also recommends developing cluster-based telecom manufacturing ecosystems to create economies of scale, improve supplier integration and strengthen innovation networks, citing Madhya Pradesh's Telecom Manufacturing Zone as a potential template.

TURNING GLOBAL DEMAND INTO EXPORT SCALE

Exports are another area where the report sees significant headroom. It identifies antennas, remote radio heads, baseband units, optical fibre cables and microwave apparatus as high-potential segments that India could target for export promotion.

Global imports of antennas, remote radio heads and baseband units alone exceeded USD 219 billion in 2024, compared with Indian exports of less than USD 1 billion in these categories, according to the report.

India also has a growing domestic market on which manufacturers could potentially build scale. The country's TANE market is estimated at nearly USD 25 billion in fiscal 2025 and is projected to reach USD 50 billion by 2032, representing annual growth of around 10%. The report expects 5G deployment and the adoption of enterprise services, IoT, smart-city infrastructure, industrial automation, mission-critical communications and other emerging applications to sustain equipment demand.

BREAKING THE MARKET-ACCESS BARRIER

Building manufacturing capacity, however, does not automatically translate into access to India's telecom equipment market.

Nearly 98% of telecom equipment demand originates from private telecom service providers, according to the report. These operators continue to prefer established global OEMs because of their technological maturity, scalability and certification standards.

That presents a second challenge for domestic manufacturers: alongside increasing local value addition and reducing component costs, they must establish the technology credentials, product reliability and scale needed to compete with established international suppliers.

The report recommends centralised testing facilities and internationally aligned certification systems to strengthen product credibility. It also calls for closer industry-academia partnerships to improve workforce readiness and innovation capabilities.

India's telecom equipment opportunity therefore extends beyond increasing the number of products assembled domestically. The report's recommendations point towards building capabilities across components, technology and product development while creating domestic vendors capable of competing for operator orders and addressing global markets. 🌐

shubhendup@cybermedia.co.in

Parliament panel seeks BharatNet audit over rollout gaps

Despite extensive fibre deployment, uneven upgrades and last-mile use raise questions about whether rural broadband can deliver connectivity at scale.



BY SHUBHENDU PARTH

The Parliamentary Committee on Communications and Information Technology in India has called for a state-wise and implementation model-wise performance audit of BharatNet, saying its rollout remains uneven despite substantial infrastructure creation and funding for the rural broadband programme.

The Standing Committee made the recommendation in its 32nd Report on schemes and projects under Digital Bharat Nidhi (DBN), presented to the Lok Sabha on 6 August 2026. The committee said substantial infrastructure had been created, but the number of operational gram panchayats (GPs) remained below envisaged universal coverage, with implementation varying across states and models.

Under the Amended BharatNet Program (ABP), 23,414 GPs had been upgraded as of 31 July 2026,

according to the DBN dashboard. The programme had laid 49,439 km of optical fibre cable (OFC) and recorded 261,995 net fibre-to-the-home (FTTH) connections by the end of July.

Separately, cumulative BharatNet deployment stood at 731,066 km of OFC, while 961,811 FTTH connections had been commissioned under the programme, according to DBN data. The July figures of 49,439 km of OFC and 261,995 net FTTH connections relate specifically to implementation under ABP.

BharatNet is the government's rural broadband programme aimed at providing high-speed connectivity to gram panchayats and villages across India. Its infrastructure is available to telecom and Internet service providers on a non-discriminatory basis for services including FTTH, Wi-Fi hotspots and leased-line connectivity.

BharatNet has deployed more than 731,000 km of fibre, but the parliamentary panel wants audits to determine how effectively that infrastructure is being used.

The Amended BharatNet Program or ABP extends the network to villages while upgrading existing infrastructure and supporting last-mile connectivity.

PANEL SEEKS ACTION ON BHARATNET DELAYS

The committee asked the Department of Telecommunications (DoT) to conduct a comprehensive model-wise and state-wise performance audit of BharatNet to identify and address implementation bottlenecks.

For ABP, it sought faster finalisation of pending packages and state-led strategies, stronger co-ordination between Bharat Sanchar Nigam Limited (BSNL), states, and implementing agencies, and milestone-based monitoring for each package. The panel said the measures were needed to complete connectivity to all GPs and targeted villages within defined timelines.

The government plans to upgrade 265,014 GPs under ABP. Of these, 214,912 had been connected under the earlier BharatNet Phase I and Phase II, while 13,494 had been upgraded under ABP as of June 2026, according to government data. The DBN dashboard put the number of upgraded GPs at 23,414 by 31 July, including 9,920 upgraded during July.

The committee recommended stronger preproject appraisal and realistic costing for public sector undertakings involved in DBN and ABP projects. It called for adherence to timelines and contractual obligations, performance-linked incentives and disincentives, and a unified framework to monitor the progress and completion of DBN and BharatNet projects.

FTTH UPTAKE TRAILS NETWORK POTENTIAL

The parliamentary committee called for greater utilisation of BharatNet infrastructure, with a focus on increasing FTTH connections and extending connectivity across rural and remote areas. It also recommended that DBN funding be used in a targeted and outcome-oriented manner.

ABP recorded 261,995 net FTTH connections as of 31 July 2026, including 20,196 added during July, according to the DBN dashboard. The Digital Bharat

Nidhi also supporting the provision of 15 million FTTH connections through the BharatNet Udyami model. Under the programme, eligible new rural connections are provided without an installation charge, while users pay the applicable monthly subscription.

On network performance, the committee called for standardised guidelines for technology selection and deployment, timely approvals for alternative technologies in difficult areas, and mechanisms to monitor network reliability and minimum assured speeds.

It said the measures should enable the benefits of BharatNet's Internet Protocol-Multiprotocol Label Switching (IP-MPLS) architecture and multi-technology approach to extend across GPs and connected villages.

AUDIT TARGETS OUTAGES AND COVERAGE GAPS

The panel recommended strengthening third-party audits, including time-bound compliance with audit observations by telecom service providers (TSPs), and greater support for BharatNet Udyamis (BNUs) to sustain last-mile connectivity.

It asked the DoT to co-ordinate with state governments and security agencies to address field-level issues affecting infrastructure deployment and telecom services in rural and remote areas. The committee also sought action on audit findings involving data outages, coverage gaps, weak signals, and infrastructure duplication.

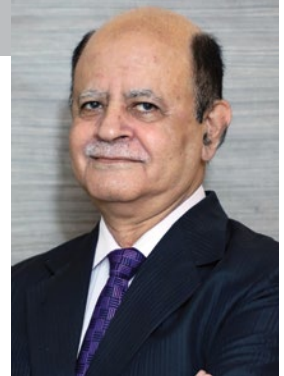
The committee has separately asked the DoT to strengthen scheme-wise monitoring of mobile connectivity projects and ensure adherence to timelines, with priority for the 4G Saturation Scheme and BOP/BIP scheme.

DBN data showed 25,085 mobile towers had been commissioned and 35,367 villages covered as of 31 July 2026. During July, 301 towers were commissioned and 345 additional villages were covered. 🏡

shubhendup@cybermedia.co.in

LT. GEN. DR. S.P. KOCHHAR

RIGHT OF WAY REFORM HOLDS KEY TO INDIA'S DIGITAL GROWTH



Faster, uniform approvals for towers, fibre and small cells can cut deployment delays while improving connectivity, public safety and network resilience.

India's digital economy rests on a simple but often overlooked foundation: physical infrastructure. Every video call, digital payment, telemedicine consultation, online class, enterprise application, public service and emergency alert depends on telecom towers, optical fibre, small cells, ducts, poles and backhaul. While digital services appear seamless to consumers, the infrastructure behind them must be planned, approved, built, maintained and continuously upgraded.

As India moves deeper into 5G, prepares for 5G-Advanced and looks ahead to 6G, the speed and predictability of telecom infrastructure approvals will determine how quickly digital connectivity reaches citizens and institutions. Spectrum and technology are important, but without timely permissions for towers, small cells and fibre, networks cannot expand at the pace required by the digital economy.

This is why streamlining Right of Way (RoW) approvals is not merely an industry issue, but a national infrastructure priority.

ROW REFORMS LAY A STRONGER FOUNDATION

The Government of India has taken important steps in this direction. The Department of Telecommunications' (DoT) e-services portal has created a centralised platform through which Telecom Service Providers (TSPs) and Infrastructure Providers (IP-Is) can apply for RoW permissions for optical fibre and mobile towers across States, Union Territories and local bodies, while improving transparency in pendency monitoring.

The Telecommunications Act, 2023 strengthened the legal basis for telecom infrastructure by recognising Right of Way, the non-discriminatory and non-exclusive grant of RoW, and the distinction between a telecom network and the property on which it is installed. The Telecommunications



Digital India cannot be built only in data centres, applications and smartphones. It must also be built on roadsides, rooftops, poles, ducts and towers.



Telecom infrastructure needs to become part of city design, with fibre pathways and utility corridors planned alongside roads, water and electricity.

(Right of Way) Rules, 2024, effective from 1 January 2025, seek to provide a uniform framework for approvals, clear timelines, dispute resolution and shared infrastructure.

The results demonstrate the value of process reform. According to the Department of Telecommunications, the centralised RoW portal reduced approval time from 448 days in 2019 to approximately 34 days as of November 2025, with around 25% of applications disposed of within 15 days. DoT has also stated that 3.81 lakh tower and optical fibre applications have been disposed of so far.

However, India's ambition requires the next phase to be sharper. The challenge is no longer only to have rules and portals, but to ensure that the framework operates uniformly and predictably across every State, municipality, development authority, public works agency, industrial estate, transport authority and public entity.

MAKING APPROVALS FASTER AND UNIFORM

A truly functional single-window system is essential. A single portal should mean one application, one set of documents, one defined process, one payment mechanism, one tracking dashboard and one digitally signed approval. Applicants should not be required to pursue parallel physical approvals or submit the same information to multiple agencies. Digitisation must reduce friction, not merely shift paperwork online.

Approval timelines must also be enforceable. Time-bound approvals are essential because telecom roll-out is interdependent. A delay in one fibre route can affect multiple towers, while a delay at one tower site can affect coverage for an entire locality. Similarly, delays in small cell permissions can affect capacity in dense urban areas. Where applications are complete and no valid objection is raised within the prescribed period, deemed approval mechanisms should be implemented in letter and spirit.

RoW policies must be harmonised across ministries and government departments. Permissions relating to forest land, roads and highways, petroleum and natural gas corridors, railways, urban development and other public infrastructure are often governed by separate laws, policies and procedures.

These should be aligned, to the greatest extent possible, with the RoW Rules, 2024 so that procedures, timelines, documentation and charges are consistent. A coordinated, whole-of-government approach would significantly reduce project delays, administrative burden and costs while accelerating broadband, 5G and future digital infrastructure.

Fees and charges should be transparent and aligned with the RoW Rules. Telecom infrastructure, being a value-added horizontal, provides public value by improving connectivity, enabling digital services and supporting economic activity. Excessive charges increase deployment costs, can slow expansion and make services unaffordable, particularly for wireline access and last-mile services.

Public infrastructure must also be made available to Telecom Service Providers on fair, non-discriminatory and non-exclusive terms. Government buildings, street furniture, electric poles, airports, metro corridors, highways, railway land, bus shelters, ducts and other public assets can play an important role in densifying networks. This is particularly important for 5G, where small cells and fibre backhaul are critical.

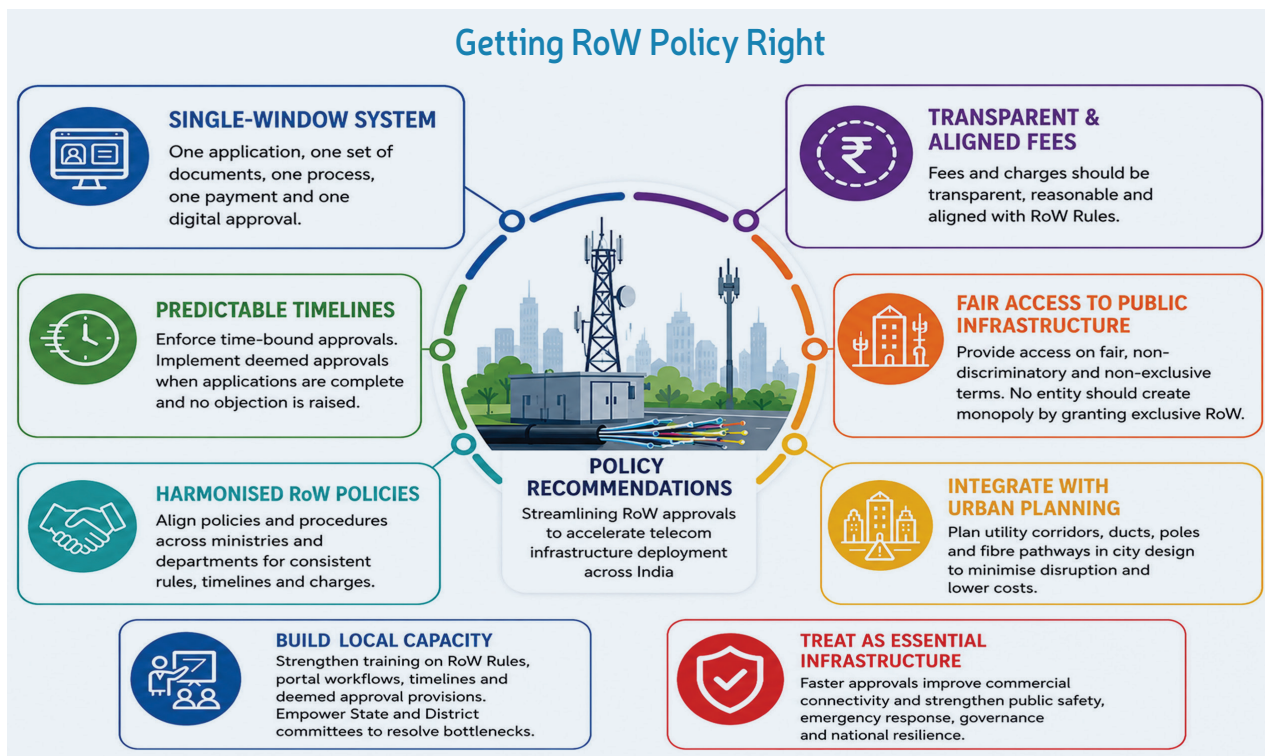
No public entity operating or controlling public infrastructure should be allowed to create a monopoly over access by granting exclusive RoW to any one infrastructure provider or TSP, including its own affiliated entities, as is being done by some entities vested with the operation and control of airports, such as Adani Airport and GMR Airport.

BUILDING CONNECTIVITY INTO URBAN PLANNING

Telecom infrastructure must be integrated into urban planning from the outset. India's cities are being reshaped through smart city projects, transit-oriented development, road widening, urban rejuvenation, utility modernisation and expansion of civic infrastructure. Digital connectivity is now an essential utility, akin to roads, water and electricity.

Dedicated utility corridors, access chambers, pole infrastructure and designated pathways for underground as well as overhead fibre, especially in the distribution segment, should therefore be incorporated into city design standards and redevelopment projects. Such planning would minimise repeated excavation, reduce disruption,

Approval delays often stem from implementation gaps, making stronger local capacity and coordination vital to translating RoW reforms into deployment.



lower deployment costs and improve connectivity to homes, businesses, institutions and digital services.

However, municipal authorities, local bodies, builders and other public entities must not themselves create sub-optimal infrastructure and force TSPs or ISPs to procure it from them instead of granting RoW permission.

Local capacity building is equally essential. Many approval delays arise not from policy intent but from uncertainty at the implementation level. Local officials, municipal bodies, public works departments and field agencies need regular orientation on the RoW Rules, portal workflows, standard documentation, charges, timelines and deemed approval provisions. Strong State Broadband Committee and District Level Telecom Committee mechanisms can help resolve recurring bottlenecks.

Telecom infrastructure must also be viewed as essential infrastructure. During disasters, public emergencies, large public events and periods of high network demand, resilient telecom networks are critical for citizens and authorities alike. Faster tower and fibre approvals therefore support

not only commercial connectivity but also public safety, emergency response, governance and national resilience.

The Central Government has created a progressive legal and digital framework. States, local bodies and sectoral authorities are now key to its success. Industry, too, must continue to ensure quality applications, responsible restoration after digging, safety compliance, community engagement and coordination with authorities.

Digital India cannot be built only in data centres, applications and smartphones. It must also be built on roadsides, rooftops, poles, ducts, towers and fibre routes. The faster we approve and deploy this infrastructure, the faster India can deliver reliable connectivity, better quality of service and inclusive digital growth to every citizen. 🌐

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 presently the Director General of the Cellular Operators Association of India (COAI).

feedbackvnd@cybermedia.co.in

PCQUEST AUGUST 2026 EDITION INDIA'S SEMICONDUCTOR STORY

ALSO READ MORE ON

- India's real chip test starts after design
- Why trusted identities are becoming harder to trust
 - Practical AI adoption for every business
 - Can India build a fair mobile esports ladder
- Forgot your Windows password? This command can reset it in seconds
- REVIEW: Intex Roar 1000 | EvoFox Ronin X75



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

QUANTUM ERA PUTS MAINFRAMES BACK IN THE INFRASTRUCTURE RACE



As quantum-era risks reshape security priorities, mainframes gain fresh relevance across hybrid infrastructure, critical workloads and sensitive data anew.

BY PRATIMA HARIGUNANI

Nothing occupies an Internet-free afternoon on an airplane better than the hypothetical question: Who would win between T-Rex and I-Rex? There is a reason this question came as both a relief and a twist in one of those movies, adding a real nail-biter to an already cliff-hanging edge. Both are theropods. Both weigh tonnes. Both carry a brute force that only the other can match. Both can fight.

Except that one is primal, does not wobble when it comes to its centre of gravity, and is an apex giant trained through years and years of survival in raw conditions. The other has better claws, more intelligence and has been created in a hybrid lab, but lacks the balance that one needs with all that weight.

Everyone had almost forgotten T-Rex after the first movie. Until I-Rex, a sort of Frankensteinish creature, became too dangerous for humans to fight. Who could have thought that T-Rex would arrive just when we

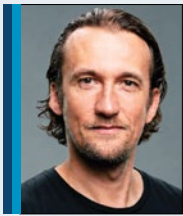
needed it! Who could have thought that mainframes, of all the pieces long forgotten in IT backyards, would become the most plausible answer when humans start confronting the flip side of quantum computing advancements: the security nightmare!

And yet, the plot twist comes. Turns out that mainframes may actually have an edge in the future landscape of cybersecurity. They are a quantum-proof species, as many perceive and argue. And that is why it might be wise to bring them back or hold on to them, beyond all the nostalgia or legacy IT reasons.

WHEN THE QUANTUM SECURITY PUZZLE AWAKENS

For decades, enterprises, especially in verticals such as BFSI, have counted on the impenetrability of encryption walls such as RSA, the public-key cryptographic system and Elliptic Curve Cryptography or ECC, because these walls were too huge and too strong for small hammers. Well, not so much when the giant forces of quantum breakthroughs start hitting them.

The quantum challenge is fundamentally a cryptography issue, making post-quantum migration across applications, networks and platforms the real test ahead.



“The reputation for resilience of mainframes comes from decades of closed, tightly controlled architecture, not from any special resistance to quantum computing.”

SERGEY LOZHKIN

Head – Kaspersky Global Research & Analysis Team, META & APAC

Where classical computers flinch, quantum computers stride ahead. In the quantum age, Shor’s algorithm can solve large mathematical computations in a blink. Massive calculations would become a sport for quantum machines, especially Cryptographically Relevant Quantum Computers, or CRQCs. And that is why hackers are already investing in Harvest Now, Decrypt Later (HNDL) exploits. The cybersecurity world would need someone as strong and as brute as these quantum machines to stand tall against this new threat landscape. And these threats are quite brute.

According to the Quantum Threat Timeline Report 2025 by the Global Risk Institute, the quantum threat is expected to become imminent, with a CRQC quite possible (28–49%) within the next 10 years and likely (51–70%) within the next 15 years. A recent study by QNu Labs revealed that 87% of organisations strongly believe quantum computers will break RSA, ECC and legacy security protocols before 2030. Illustratively enough, 21% of surveyed organisations confirmed a cyberattack in the past two years.

Add HNDL to this mix and the path gets even more slippery. HNDL can kick in the moment encrypted data is collected; it does not have to wait until quantum computers become capable of decrypting it.

The 2026 Unit 42 Global Incident Response Report noted that the fastest quartile of intrusions reached data exfiltration in 72 minutes in 2025, compared with 285 minutes in 2024. The share of incidents reaching exfiltration in under one hour also increased from 19% in 2024 to 22% in 2025. Turns out that attackers are exfiltrating data earlier in the attack process and rapidly collecting large volumes of information before sorting through it later.

The State of Quantum Computing report 2026 by Forrester also echoes these fears: quantum computers can break mainstream public-key cryptography such as

RSA-2048 by 2030. It cited a demonstration showing that 1,399 logical qubits could factor RSA-2028 in under a week.

In short, quantum, along with all the new leaps it promises, also brings quantum security questions. Which leads us to the next question.

CAN MAINFRAMES MEET THE QUANTUM TEST?

Yes, mainframes mostly leverage open frameworks, and this gives them a security-from-scratch approach, affirms Shivaling Salakki, Program Director, CySecK, Karnataka State’s CoE in Cybersecurity.

While acknowledging the potential capabilities of quantum computing in the emerging era, it is important to consider sectors such as banking, aviation, healthcare, insurance and large-format retail, says Manoj Gupta, Vice President, IT, Restaurant Brands Asia.

“Let us especially talk about hospitals because we know healthcare data is incredibly sensitive, including patients’ medical records and other relevant information. Therefore, security is extremely critical for the business, and the security structure of the mainframe provides us with multiple layers of security features, such as built-in cryptographic cards, which help to enhance security and make it very difficult for hackers to decipher.”

Gupta adds, “This is just one layer; it has multilayer protection working together, making it nearly impossible to compromise. Furthermore, these systems are continuously updated with state-of-the-art threat detection software.”

Quantum does introduce an important dimension, avers Rahul Rao, Distinguished Engineer, IBM India Systems Development Lab (ISDL). “Preparing for quantum-safe cryptography is a multi-year journey that requires long-term infrastructure decisions today. Security can no longer be an afterthought or an overlay;



“Instead of becoming obsolete, Mainframes will evolve as secure, high-performance transaction engines that work alongside cloud, Edge and AI ecosystems at scale.”

MANOJ GUPTA

Vice President –IT, Restaurant Brands Asia

it must be built into the platform from the processor and operating system through to applications and data management. Enterprises are therefore looking for systems that can help them strengthen resilience against both current and future threats. Mainframes, in fact, are among the most forward-prepared infrastructure.”

He cites how IBM has built quantum-safe capabilities directly into the hardware layer through on-chip accelerators that handle the heavy mathematical computation of quantum-resistant algorithms, and hardware security modules that natively support post-quantum cryptographic standards finalised by NIST. Security remains a key differentiator, Rao underscores.

Quantum computing is a double-edged sword, as Kamal Matta, AVP of Information Technology and Security at Sonic Biochem Extractions, frames it. “While true quantum advantage is still scaling up, the security threat of ‘harvest now, decrypt later’ is already a board-level concern for regulated industries. Mainframes have adapted by becoming the first enterprise systems to integrate hardware-level, NIST-standardised ‘quantum-safe cryptography’. Instead of being threatened by the post-quantum world, they are positioning themselves as the only infrastructure secure enough to survive it.”

Ross Tisnovsky, Partner, Everest Group, throws in a thought here: z16 was the first IBM server shipped with embedded quantum-safe technology at the firmware layer. “That, however, does not mean legacy apps running on mainframes are ready, but do not blame the machine for the laziness of humans.”

Let us explore the other side of the wall now.

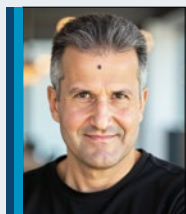
MAINFRAMES MATTER, BUT NOT IN ISOLATION

According to experts, mainframes have long been trusted in banking, telecom and government sectors because of their resilience, scalability and ability to process mission-critical transactions.



IN BRIEF

- Quantum-era security risks are prompting enterprises to reassess the role of mainframes across mission-critical digital infrastructure.
- Mainframes are not inherently quantum-proof, but their hardware security can support enterprise migration towards post-quantum cryptography.
- HNDL attacks put long-lived sensitive data at risk today, increasing pressure on enterprises to build crypto-agility across infrastructure.
- AI is expanding the mainframe’s role from transaction processing to real-time fraud detection, risk analysis and operational intelligence.
- Data sovereignty is strengthening demand for greater control over sensitive information across increasingly complex hybrid IT environments.
- Mainframes are evolving to work alongside cloud, edge and AI rather than compete with them across increasingly hybrid IT environments.



“If you evaluate Quantum Computing by traditional computing metrics, like cost per raw operation, it is more expensive and much slower than classical computing.”

ROSS TISNOVSKY

Partner, Everest Group

However, the quantum challenge is not fundamentally a mainframe issue; it is a cryptography issue. The institutions that will be best positioned for a post-quantum future are those that can rapidly adopt quantum-safe encryption and maintain crypto-agility across their entire environment, including mainframes, cloud platforms, networks, and applications.

In that context, mainframes remain highly relevant, but not because they are inherently quantum-proof. Their value comes from supporting secure, large-scale modernisation and migration to post-quantum cryptography.

Sergey Lozhkin, Head of Kaspersky Global Research and Analysis Team for META and APAC, also clarifies that the idea that mainframes are inherently quantum-proof is often misunderstood. “Their reputation for resilience comes from decades of closed, tightly controlled architecture, and not from any special resistance to quantum computing. Most still rely on widely used encryption methods such as RSA and ECC, which the industry is gradually replacing with post-quantum cryptography.”

Databases and the latest updates can still pose security challenges, echoes Salakki. “Ensuring coding for security and right testing will harden mainframes even more from a security perspective.”

The greater consideration, as Lozhkin points out, lies in the nature of the data these systems protect.

“Enterprises operating mainframes, particularly across banking, insurance and government, manage some of the world’s most sensitive and long-lived data, making them high-value targets for ‘harvest now, decrypt later’ attacks, where adversaries capture encrypted data today with the intention of decrypting it once quantum computing becomes sufficiently advanced.”

Their legacy architecture can also make cryptographic upgrades more complex and time-consuming than on modern systems, he adds. At the same time, Kaspersky’s analysis highlights that even post-quantum deployments on modern, agile infrastructure require careful planning to address interoperability and performance challenges.

The relevance of security also has the AI context to take into account. Mainframes are recognised for their robust data-processing capabilities, which align with the substantial data requirements of AI, Gupta opines. “Therefore, I posit that mainframes and AI are not mutually exclusive but rather complementary technologies. Indeed, numerous financial institutions are leveraging AI on mainframes to execute real-time fraud detection with exceptional accuracy.”

Mainframes are not becoming more relevant because they are quantum-proof, concludes Lozhkin. “They remain relevant because they still process a disproportionate share of the world’s most sensitive, long-term data, and



“Organisations now want infrastructure that not only processes transactions reliably but also extracts intelligence from them in real time, including fraud detection.”

RAHUL RAO

Distinguished Engineer, IBM India Systems Development Lab



“Mainframes have adapted by integrating hardware-level, NIST-standardised quantum-safe cryptography, positioning them strongly for the post-quantum world.”

KAMAL MATTA

AVP – IT & Security, Sonic Biochem Extractions

our own assessment of quantum-era cybersecurity risks points to this as an area requiring proactive planning.”

Organisations need to prepare now for future threats because long-term-value data is being exposed to future decryption right now, he argues. The security choices made today will shape how resilient digital infrastructure remains for decades. Preparing legacy infrastructure for the quantum era is a shared responsibility that depends on enterprises, IT vendors and policymakers moving together.

THE BUSINESS CASE GOES BEYOND SECURITY

Security, it seems, is not the entire business case for mainframes. Tisnovsky points to two factors that could affect the economics and make the case ROI-positive. “I see two factors that could affect this business case and make it ROI positive. First, massive decline in the cost of processing per unit, and Quantum Computing (QC) is not that. In fact, if you evaluate QC by traditional computing metrics, like cost per raw operation or raw clock speed, QC is more expensive and significantly slower than classical computing.”

Further, in his understanding of Post-Quantum Cryptography (PQC), mainframes are first in line to be PQC-ready. The PQC threat to mainframes is well understood, he says. “The real danger lies in the Talent Premium problem here.”

The business case, however, extends to the workloads these systems support. Gupta contends that in areas such as supply chain management, digital identity verification and the protection of sensitive healthcare data, mainframes provide security, reliability and the ability to handle massive workloads.

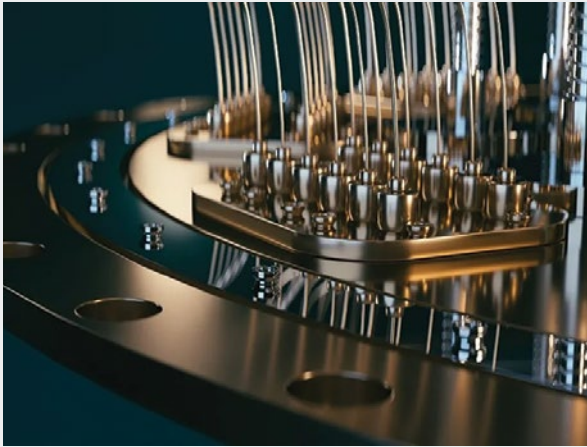
“Also, technology like blockchain and cryptocurrency are about much more than just digital currencies. They provide a secure, transparent way to record and track the transactions. Here, mainframe can continue to play a



THE MAINFRAME ADVANTAGE

- 61% of global infrastructure decision-makers used mainframes in 2024; among them, 54% planned to increase usage over the next two years.
- Mainframe workloads have increased 4x over the past decade, according to IBM, with AI emerging as another potential driver of workload growth.
- Mission-critical applications can be 2–4x less expensive to run on mainframes, according to IBM’s analysis of workloads over the past decade.
- Mainframes support hybrid cloud, microservices and DevOps, while APIs connect core mainframe logic with modern applications and interfaces.
- Even in cloud-first environments, mainframes continue to support workloads demanding high security, availability, compliance and reliability.

Hardware-level cryptographic acceleration and chip-level isolation could give mainframes an important role across regulated, data-intensive IT environments.



THE QUANTUM THREAT

- Q-Day could become a plausible risk by 2030, according to Forrester's 2026 assessment, putting today's public-key cryptography under pressure.
- 58% of organisations have no budget for quantum security, according to QNu Labs, with skills, awareness and funding among the key barriers.
- 67% of enterprises expect quantum computing to increase or alter cybersecurity risks over the next decade, according to ISACA's 2025 research.
- 40% of cyber and IT professionals have not considered implementing post-quantum cryptography, while only 5% strongly understand NIST's new PQC standards.
- NIST has finalised its first PQC standards, while enterprise migration could take five to 15 years or more, adding urgency to preparations today.

significant role by supporting industry-grade blockchain solutions and other mission-critical workloads."

Expectations from these systems are also changing. "Organisations now want infrastructure that not only processes transactions reliably but also extracts intelligence from them in real time," says Rao. "This includes use-cases such as fraud detection, risk analysis, claims processing, customer service automation and operational optimisation."

Data sovereignty adds another dimension. Mainframes provide organisations with greater control over where sensitive data resides, making them well suited for industries such as healthcare, banking, insurance and government, where regulatory compliance and data protection are non-negotiable, Gupta adds.

Rao sees sovereignty as a much broader conversation than simply data location. "Enterprises increasingly need control over how data is governed, processed and secured across hybrid environments. Mainframes continue to play a critical role in this through advanced, chip-level isolation technologies like IBM Hyper Protect Virtual Servers and Secure Execution."

"Instead of becoming obsolete, mainframes will evolve as secure, high-performance transaction engines that work adjacent to cloud, edge and AI ecosystems, and not compete with them," says Gupta.

That may ultimately define the mainframe's place in the next generation of digital infrastructure. Its relevance will depend less on being viewed as a legacy system or an inherently quantum-proof platform, and more on how effectively it can combine transaction processing, security, data control and emerging workloads within increasingly hybrid environments.

As enterprises move towards post-quantum cryptography, mainframes could, therefore, remain an important part of the infrastructure mix, provided their applications and cryptographic architectures evolve with them. 🧠

pratimah@cybermedia.co.in



THE INDIAN NEWSPAPER SOCIETY

VOICE & DATA
Connecting the Digital World

Lies try to
disguise themselves
as the sensational truth.
But we all seek the truth.
That's why every word
we print is corroborated,
verified, and only
then put to paper.
Between these lines,
there is no room
for falsehood.
Here, what's written
and what's true are always
the same thing because

Nothing but the truth.

Ink Doesn't Lie





SAMIR MISHRA

Managing Director, Enterprise,
Cisco India & South Asia

“One of the biggest constraints for AI is the network”

As enterprises move Artificial Intelligence (AI) from experimentation to production, the infrastructure beneath it is becoming increasingly critical. Agentic AI adds another dimension: autonomous agents operate continuously and at machine speed, potentially multiplying network traffic, infrastructure demand and security risks. Networks, compute, data, observability and cybersecurity are consequently becoming integral to enterprise AI strategies.

Samir Mishra, Managing Director, Enterprise, Cisco India and South Asia, believes AI is becoming fundamentally network-bound and could trigger a networking supercycle. In this interaction with **Shubhendu Parth**, he explains why enterprises need to address infrastructure debt, what happens when AI agents go rogue, why Zero Trust must evolve from access to action control, and how networking and security architectures are changing as AI scales. Excerpts:

As enterprises move from AI experimentation to production, is infrastructure becoming the real differentiator? How should Indian enterprises prepare?

This is a pivotal moment. Everybody is talking about AI and how to use it for business, but according to the Cisco AI Readiness Index 2025, only 13% of the organisations surveyed are ready for AI. One of the parameters studied was infrastructure readiness, or AI infrastructure debt. If your digital infrastructure is not ready, that becomes a fundamental challenge.

When we speak to customers, three priorities consistently emerge. The first is infrastructure modernisation. Organisations realise they need to prepare not only for today's digital transformation but also for AI and Agentic AI. The second is cybersecurity, where they need to protect themselves from known risks as well as new threats that AI will introduce as the attack surface expands. The third is data. Much enterprise data remains siloed, and organisations are looking at how AI can unlock greater value from it.

AI workloads are already arriving, and enterprises need to modernise their infrastructure now. There is really no option except to build resilient, modern infrastructure that is ready for the future.

As AI infrastructure expands, how important does the network become compared with compute, memory and power?

When people discuss AI constraints, they usually talk about power, compute and memory. But one of the biggest constraints is the network. If your GPUs are lying idle because data is not reaching them in time, you are losing money. You need the speed and bandwidth to ensure these GPUs receive data when they need it.

We believe AI is fundamentally network-bound. During the chatbot era, infrastructure demand was relatively spiky because interactions were human-led. A user asked a question, received a response and moved on.

“If your GPUs are lying idle because data is not reaching them in time, you are losing money; you need the network speed and bandwidth to keep them working.”

“Agents work 24x7 and operate at machine speed, creating persistent infrastructure demand which is significantly higher than what enterprises have seen before.”

Agentic AI changes that completely. Agents work 24x7, creating persistent demand for infrastructure. They also operate at machine speed, so the volume of infrastructure required will be significantly higher.

This is creating a networking supercycle. It is not limited to data centres; it extends to workplaces where humans and AI agents will increasingly work together. Our research shows that an AI agent performing a task can generate over 450% higher infrastructure demand than a human performing the same task. Many organisations are still underestimating the implications of this shift.

How does Agentic AI change the way enterprises should design their networks and security architecture?

As humans begin working alongside AI agents, we are also entering the era of Physical AI, where robots and sensors become part of everyday enterprise operations. The underlying infrastructure therefore has to be rethought completely.

We need AI-scale data centres because that is where digital co-workers will reside. At the same time, humans and agents will work together across campuses, branches and factories, all of which must remain connected to those data centres. Throughput, speed and resilience become critical.

The arrival of AI agents also changes the security model. Agents need to be treated as identities, much like human users, because they interact with other agents, enterprise applications and external tools through an MCP server.

The biggest difference is that agents have access to tools that allow them to execute tasks on our behalf. As organisations become more comfortable, they will delegate increasingly complex responsibilities to them. That makes trust fundamental.

Those same capabilities create a new attack surface. Agents communicating with other agents or external tools can become points of exploitation if they are not

secured properly. Enterprises therefore need to make their infrastructure ready for AI at scale while securing the emerging agentic workforce.

As organisations hand over more work to AI agents, what happens if an agent goes rogue? Do we need an architectural kill switch?

This is one of the areas where Cisco is innovating. About a year ago, we began focusing on securing AI models, LLMs and applications because safe and secure AI adoption is fundamental. As AI evolves, we now need to extend those capabilities to agents.

There are three aspects to this. The first is protecting the agent from the outside world. If an agent is working on my behalf, it could be exposed to prompt injection or data poisoning attacks that alter its behaviour. We are extending Cisco AI Defense beyond models and applications to agents by introducing guardrails through visibility, validation and runtime enforcement.

The second is protecting the world from the agent. I often compare an agent to a teenager. It is ambitious and capable, but it does not understand consequences. If you give it unrestricted access, it can create problems. The question is how you detect behavioural drift, intervene at the right time and put guardrails around it.

Traditional Zero Trust focuses on users, where the principle is always verify, never trust, and users receive only the minimum access required. Agents are different. They are task-oriented rather than judgement-oriented, so security has to move from access control to action control.

That means discovering the agent, authorising every action and adapting to risk in real time. If its behaviour changes, you must be able to intercept it, apply guardrails and respond immediately. Finally, threats need to be detected and remediated at machine speed. That is where concepts such as the Agentic SOC become important.

Networks were initially monitored using AI; now they must support and manage AI opera-

“Research shows that an AI agent performing a task can generate over 450% higher infrastructure demand than a human, a shift many organisations are still underestimating.”

tions themselves. How is the network operation changing?

Our approach is built on three principles. The first is simplifying operations with AI. Infrastructure management has to become simpler and more unified because customers increasingly want a single management experience rather than multiple disconnected tools.

The second is embedding AI natively across our portfolio. We are moving towards Agentic Ops, where AI agents can help automate operational tasks. If an issue occurs, an agent can initiate diagnostics, create a support ticket, identify where the problem originated and recommend corrective action. That information can then be shared with IT operations, security teams or other AI agents capable of resolving the issue. The objective is to move from reactive operations to a more proactive operating model.

The third is scaling infrastructure for AI. Our own silicon provides the programmability and performance needed for AI-scale networking. As organisations deploy larger GPU clusters, they need to scale within racks, across multiple racks and across geographically distributed data centres.

This is where the Infrastructure Economy becomes relevant. Speed, throughput, resilience and security are becoming strategic differentiators. We are also embedding security directly into the network fabric because protection has to move closer to the workload.

Does embedding security into the infrastructure change how enterprises should handle vulnerabilities?

Yes. The time between a vulnerability being disclosed and being exploited has reduced dramatically, from days to minutes in some cases. Organisations cannot rely solely on periodic patching anymore.

At the same time, patching complex enterprise infrastructure is not trivial. I recently spoke to an organisation that patches only once a year because the exercise requires nearly 30,000 person-hours. Increasing the frequency requires more resources and downtime, which is not always practical.

That is why we introduced the concept of a vulnerability shield. Cisco Live Protect is deployed within the data centre, initially on Cisco Nexus, and provides a compensating control between patch cycles. It helps shield the infrastructure until the next scheduled patch cycle.

It is important to distinguish this from real-time patching. This is not a replacement for patching; patching still has to happen. The objective is to reduce exposure between patch cycles. It uses technologies such as eBPF, or Extended Berkeley Packet Filter, operating at the kernel level to provide an additional layer of protection.

Looking ahead, what infrastructure constraint are CIOs still underestimating as enterprise AI scales?

Power, compute and memory will all remain important constraints. However, from our perspective, networking will become the defining factor.

As organisations deploy more AI agents, infrastructure demand will increase dramatically. Our research indicates that AI agents can generate around 450% more network traffic than humans. If GPUs are not connected efficiently, they cannot deliver their full potential. Organisations therefore need to modernise their infrastructure before AI adoption accelerates.

The second area is data. Enterprises need to leverage machine data more effectively to generate AI insights and enable capabilities such as Agentic SOC. The third is security. Organisations must secure both AI models and the agentic workforce if they want employees to trust AI and delegate more responsibilities to it.

AI adoption is accelerating rapidly, but organisations that are not prepared from an infrastructure perspective will struggle to realise its full value. Infrastructure modernisation, readiness for Agentic AI and securing the agentic workforce will be the defining priorities over the next few years. 🧠

shubhendup@cybermedia.co.in

Connected data, not smarter AI, will win healthcare's race

Interoperability across systems can turn fragmented records into usable intelligence, improving care decisions, efficiency and digital health outcomes.



BY AYUSH JAIN

Fragmented data has long been one of healthcare's most expensive invisible challenges. It slows operations, limits care decisions and undermines artificial intelligence (AI) before it starts. For CIOs, CTOs, CDOs and other CXOs, addressing this has become a defining mandate.

According to a 2025 study published in the World Journal of Advanced Engineering Technology and Sciences, healthcare data is growing at a rate of 63% annually. Hospitals, laboratories, insurers, pharmacies, device manufacturers and emerging digital health platforms are generating more data than ever, yet much of it remains trapped in silos.

Healthcare systems today are racing to adopt the latest AI models. However, the biggest gains will come from organisations that can successfully connect data across hospitals, laboratories, pharmacies and other systems.

The Ayushman Bharat Digital Mission (ABDM), an initiative of the Government of India, has crossed 100 crore ABHA-linked health records, with the number doubling from 50 crore in February 2025 to more than 100 crore within 15 months, according to the Ministry of Health and Family Welfare. This indicates how electronic health records are becoming an integral part of the healthcare system.

Scale alone, however, does not prove value. The real test is whether this growing digital infrastructure is translating into better outcomes on the ground.

TURNING CONNECTED DATA INTO HEALTHCARE VALUE

The impact of ABDM is further supported by the ministry. In a written reply in the Lok Sabha, Union Minister of State for Health and Family Welfare Prataprao Jadhav stated that a third-party evaluation of ABDM, conducted

A discharge summary, insurance claim, pharmacy record and wearable reading gain more value when every system can interpret them through a common data language.

between June and August 2025, found that the mission had reduced waiting times, enabled cost savings and improved access to services, particularly benefiting women and underserved populations.

With both the scale and impact of connected records becoming evident, the more pressing question for healthcare leaders is what it takes to achieve this.

At present, one of the biggest challenges for healthcare leaders is executing the planned strategy. Cognizant's 10 Major Moves in Healthcare Interoperability in 2025 underscores that the hardest challenge is no longer technology, but cultural and operating-model alignment.

Addressing this means treating interoperability as a change-management effort as much as a technical one: securing executive sponsorship early, involving clinicians in defining what connected data should look like in their workflows, and setting shared metrics, such as reduced duplicate testing or faster authorisation times, for which both IT and clinical teams are accountable.

For long-term progress, healthcare leaders cannot rely solely on technical delivery. Consistent leadership, governance and change management are also required, along with a well-defined roadmap for how information flows within the system.

BUILDING GOVERNANCE AROUND CONNECTED DATA

Organisational structures must adapt accordingly. Collaborative data governance across clinical, IT, operations, compliance and security functions requires clear accountability, with the CDO responsible for data strategy, the CISO for security, and clinical champions for data quality and utilisation.

In the US, such governance is being developed around HIPAA compliance. The HIPAA Journal Annual Survey 2025 of hundreds of US healthcare organisations reveals varying levels of maturity in HIPAA privacy programmes, with many still lacking robust internal structures, privacy



IN BRIEF

- Healthcare data is growing at 63% annually, yet silos across hospitals, laboratories, insurers and pharmacies continue to limit its value.
- ABDM has crossed 100 crore ABHA-linked health records, while an evaluation found lower waiting times, cost savings and better access.
- Interoperability requires organisational change alongside technology, with executive sponsorship, clinician involvement and shared metrics.
- Data governance needs clear accountability across clinical, IT, operations, compliance and security teams as connected ecosystems expand.
- HL7 and FHIR provide a common data language, while APIs, cloud, cybersecurity and identity management form the technology foundation.
- High-value use cases such as duplicate-test reduction, faster authorisation and medication reconciliation can provide a path to scale.

officers with decision-making authority and up-to-date risk assessments.

In India, the governance environment is developing around ABDM, the National Health Claims Exchange

API-first and event-driven architectures can shift healthcare data exchange from periodic transfers towards systems that respond as information changes.

(NHCX) and the Digital Personal Data Protection (DPDP) Act. According to IIM Bangalore's State of DPI in India 2025 report, digital public infrastructure has simplified healthcare delivery and reduced costs, but challenges remain around digital infrastructure, workforce constraints, privacy under the DPDP Act 2023 and interoperability.

CREATING THE TECHNOLOGY FOUNDATION FOR DATA

At the technology level, the priorities are clear. The foundation is an interoperable data platform that brings together information spread across the healthcare ecosystem. Such a platform must rest on established data standards such as Health Level Seven (HL7) and Fast Healthcare Interoperability Resources (FHIR), ensuring consistency of terms.

These standards do more than create consistency on paper. A common data language allows a hospital's discharge summary to be read correctly by an insurer's claims system, a pharmacy's dispensing record to match a laboratory test result, and a wearable device's readings to sit within the same patient record as a clinician's notes.

Without this shared structure, hospitals, laboratories, insurers, pharmacies and device manufacturers can end up maintaining different versions of the truth, making reconciliation a manual and error-prone exercise.

Cloud and hybrid computing enable large volumes of data to be stored and processed with scalability and security, while application programming interfaces (APIs) provide standard interfaces for real-time transactions. Cybersecurity, governance and identity management are core design requirements rather than add-ons.

In practice, an insurer's prior-authorisation system can query a hospital's records in real time instead of waiting for a fax or manual upload, cutting approval times from days to hours.

Security is equally important. According to a 2025 IBM study titled *When Ransomware Kills*, attacks against healthcare organisations have resulted in the diversion of emergency services, missed treatment and even patient

deaths. Such outcomes can be reduced through security by design, network segmentation, regular backups, tested incident response and continuous monitoring.

Identity management plays a similarly practical role. When a patient moves between a hospital, diagnostic laboratory and pharmacy, each system needs to establish that it is looking at the same person. Weak identity matching can duplicate records, delay care and, in the worst cases, merge the histories of two different patients.

SCALING INTEROPERABILITY FROM USE CASES

The challenge for CIOs, CTOs, CDOs and other healthcare leaders is to transform isolated projects into an integrated programme. Organisations do not need to reinvent their entire data infrastructure at once. A few high-value use cases can provide a starting point.

One is eliminating duplicate laboratory tests by giving hospitals visibility into results already available elsewhere. Another is speeding up insurance prior-authorisation by giving insurers real-time access to relevant clinical data. A third is medication reconciliation, ensuring that a patient's prescription history is visible across pharmacies and providers so that potentially dangerous interactions can be identified before a prescription is filled.

Each can be piloted narrowly, demonstrating value before the organisation scales the underlying data flows to other use cases.

Even a narrow starting point requires the right foundation to scale. Healthcare leaders are investing in interoperability infrastructure, data engineers, and security and identity solutions, while collaborating with electronic health record (EHR) companies, laboratories and medical device providers to define standard APIs. The focus is also shifting towards API-first and event-driven architectures.

In India, this approach increasingly means developing an infrastructure layer that connects existing hospital and electronic medical record (EMR) systems with FHIR and ABDM consent management.

Connecting hospital and EMR systems to FHIR and ABDM consent management is emerging as a critical infrastructure layer for healthcare interoperability in India.

The Connected Healthcare Data Stack

Technology foundation for interoperable, secure and patient-centric healthcare



The future of healthcare will be shaped not by technology alone, but by the leadership behind it. Connected data can enable smarter decisions, safer care and more efficient processes, but its value is realised only when it becomes a strategic priority across the organisation. Leaders who treat connected data as a

strategic, organisational and technological programme, and execute it with discipline, will set the pace for the next decade. 🌟

The author is the CEO of Mindbowser.
feedbackvnd@cybermedia.co.in



Cloud discipline becomes the new currency of digital growth

With cloud access commoditised and AI driving costs higher, competitive advantage now depends on linking technology consumption to measurable business value.



BY NAMAN JAIN

For much of the last decade, digital growth was driven by one simple advantage: access. Organisations that embraced cloud technologies early gained the ability to build faster, scale faster, and experiment faster. Infrastructure was no longer a bottleneck. Teams could launch environments in minutes instead of waiting weeks or months for hardware procurement and deployment. The cloud fundamentally changed how businesses approached innovation.

Today, that advantage has largely disappeared. Cloud platforms, developer tools, and AI services are widely accessible. Startups and enterprises often have access to

the same technology foundations. The competitive gap is no longer created by access to technology itself. It is increasingly determined by how effectively organisations manage and extract value from that technology.

This is why cloud discipline is becoming one of the most important business capabilities for the next phase of digital growth.

Global spending on public cloud services continues to rise as organisations invest in AI, analytics, and digital services. At the same time, industry estimates suggest that 25–35% of cloud spending is wasted through idle

Cloud flexibility removed infrastructure bottlenecks, but also weakened natural spending controls as resources became easy to provision, scale and then forget.

AI is turning technology economics into a boardroom issue, forcing leaders to weigh efficient scalability and sustainability alongside capability and ambition.

resources, overprovisioned infrastructure, and inefficient usage patterns.

WHY CLOUD SUCCESS CREATED A NEW CHALLENGE

One of the cloud's greatest strengths is its flexibility. Development teams can provision resources instantly. Business units can launch initiatives without lengthy procurement cycles. New products can move from idea to deployment at unprecedented speed.

However, the same flexibility that accelerates innovation can also make spending harder to govern. Traditional infrastructure environments came with natural controls. Major investments required planning, approvals, and budget discussions. Cloud transformed infrastructure into an on-demand service, making consumption remarkably easy.

The challenge is that accountability did not evolve at the same pace. Most organisations do not struggle because they lack cloud expertise. Many have highly capable engineering teams and mature cloud environments. However, the teams creating cloud consumption are often disconnected from the teams evaluating its business impact.

By the time spending is reviewed, the decisions that created it have already been made.

This became particularly common during periods of rapid growth. If additional cloud spending accelerated product delivery or improved customer experiences, it was often viewed as a reasonable trade-off. Efficiency mattered, but speed mattered more.

The unintended consequence is that many organisations developed a culture where cloud consumption was easy to create but difficult to fully understand. Temporary environments remained active. Infrastructure was sized for peak demand and rarely revisited. New services were adopted faster than governance processes could mature around them.

Individually, these decisions made sense. Collectively, they created inefficiencies that often remained hidden beneath broader growth objectives.



IN BRIEF

- Industry estimates suggest 25–35% of cloud spending is wasted through idle resources, overprovisioning and inefficient usage patterns.
- Cloud flexibility accelerated innovation, but consumption outpaced the governance and accountability needed to keep spending in check.
- AI workloads make cloud costs harder to forecast as compute-heavy training, inference demand and complex data pipelines expand consumption.
- Cloud spending reaches the boardroom as consumption affects profitability, investment priorities and the economics of AI adoption at scale.
- FinOps requires shared ownership, linking engineering choices, financial visibility and leadership priorities to clear business outcomes.
- Disciplined organisations may not spend less, but they can identify where technology creates value and where inefficiencies erode returns.

AI IS MAKING CLOUD ECONOMICS IMPOSSIBLE TO IGNORE

If cloud adoption exposed weaknesses in how organisations manage technology consumption, AI is magnifying them. Much of the discussion around AI

Cloud optimisation works best when the goal shifts from cutting costs to spending smarter, with each investment tied more directly to measurable business value.

focuses on opportunity. Organisations are exploring how AI can improve productivity, create new customer experiences, and unlock new revenue streams. Those opportunities are real.

What receives less attention is that AI is changing the economics of technology investment.

AI workloads are different from traditional IT workloads. Training models requires significant computing power. Inference workloads can expand rapidly depending on demand. Data pipelines supporting AI initiatives often consume resources across multiple environments and services. As a result, cloud consumption becomes harder to forecast and more difficult to optimise.

What makes AI particularly significant is that it is forcing business leaders to ask questions that were often overlooked during earlier phases of cloud adoption. It is no longer enough to ask what technology can do. Organisations are increasingly asking whether they can scale that technology efficiently and sustainably.

This represents an important change in how technology investments are evaluated. Five years ago, cloud costs were largely discussed within engineering teams. Today, conversations around cloud consumption increasingly reach the executive level because they influence profitability, investment priorities, and the economics of AI adoption.

It is a sign that cloud and FinOps has become central to business strategy.

FROM COST MANAGEMENT TO BUSINESS ACCOUNTABILITY

One of the most common mistakes organisations make is treating cloud optimisation as a cost-reduction exercise. The objective should be spending better and smarter.

Organisations should continue investing in innovation, experimentation, and growth opportunities. The challenge is ensuring that technology spending remains connected to measurable business outcomes. This requires more than dashboards and reporting tools.

Most enterprises already have access to cloud cost data. What they often lack is shared ownership. When engineering teams understand the financial impact of architectural decisions, priorities begin to change.

When finance teams gain better visibility into operational requirements, conversations become more productive. When leadership teams can connect technology investments directly to business value, decision-making improves across the organisation. The most successful organisations increasingly treat cloud spending as a shared business responsibility rather than a technical afterthought.

Importantly, this approach does not slow innovation. It strengthens it. Teams that understand their consumption patterns can make decisions with greater confidence, justify investments more effectively, and focus on delivering business value rather than explaining unexpected costs.

Ultimately, this is what cloud discipline is about. It is about ensuring that innovation remains sustainable.

Cloud and AI is now foundational to business growth and the gap between disciplined and undisciplined organisations is likely to widen. Access to technology is no longer the differentiator it once was. Most organisations can access the same platforms and capabilities. The differentiator will be how effectively they manage them.

The next phase of digital growth will belong to organisations that understand this distinction. They may not spend less than their competitors, but they will have a clearer understanding of where investments are creating value, where inefficiencies exist, and how technology decisions influence business outcomes. In the years ahead, that clarity may become one of the most important competitive advantages for any organisation leveraging cloud computing. 🍌

The author is the Chief Growth and Marketing Officer of CloudKeeper.

feedbackvnd@cybermedia.co.in



DATAQUEST AUGUST 2026 EDITION: FROM PRESENCE TO POWER WOMEN LEADING THE AI ECONOMY

ALSO READ MORE ON

- From Factory Floors To The AI Economy: Women Reshape Technology Leadership
 - Gen Z Women Are Speaking Up, But Workplaces Still Need To Catch Up
 - Lisa Su's Systems Bet Puts Women At AI Infrastructure's Core
 - Cyber resilience in the age of AI will be decided in the boardroom
 - Jharkhand's Plan for Responsible and Inclusive 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

Can Agentic AI crack quantum computing's use-case puzzle?

While quantum systems remain noisy and difficult to scale, AI agents could help identify where they offer real value and when classical computing remains better.



BY AMITKUMAR SHRIVASTAVA

Quantum computing has spent years between promise and practicality. Its potential is significant in areas such as optimisation, chemistry, materials science, logistics, finance and advanced simulation. But the reality is equally important: today's quantum systems are still noisy, limited and difficult to scale. Quantum computing will not solve every complex business problem and, in many cases, classical computing will remain the better option.

The more useful question is how organisations can prepare for areas where quantum methods may create meaningful value. Agentic Artificial Intelligence or AI could help make that transition more practical.

Agentic AI refers to AI systems that can work towards a goal, create a plan, use tools, learn from results and decide the next step. Instead of simply answering a question, an AI agent can help move a problem through a full workflow: understanding the business objective,

The smartest role for an AI agent may be deciding not to go quantum, after testing whether conventional or quantum-inspired methods can do the job better.

Quantum computing has plenty of promise. The harder task is finding the problems worth sending its way, and AI agents could help businesses make that call.

evaluating possible methods, coordinating systems, comparing results and presenting recommendations that leaders and experts can act on.

For quantum computing, this matters because the technology is still difficult to access and apply. Most business users should not need to understand quantum circuits, hardware noise, and error behaviour or algorithm selection. What they need is a bridge between a real business problem and the right computational approach. Agentic AI can become part of that bridge.

ORCHESTRATING HYBRID COMPUTING SYSTEMS

The future of quantum adoption will likely depend on orchestration. Classical computing, data platforms, graphics processing units (GPUs), quantum processing units (QPUs), simulators, quantum-inspired solvers and AI models will need to work together. A hybrid orchestration layer can manage problem decomposition, backend selection, data movement, error mitigation, classical post-processing, reproducibility and performance monitoring. Agentic AI can support this by helping make decisions in a structured and measurable way.

One practical starting point is optimisation. Organisations make complex decisions every day across supply chains, logistics, production planning, energy usage, inventory and financial modelling. These problems often involve thousands or millions of possible combinations. A logistics company, for example, may need to route vehicles while considering fuel costs, delivery windows, driver availability, traffic and customer priority.

Quantum optimisation is promising, but it is not guaranteed to outperform classical methods in every case. Agentic AI can help by testing classical solvers first, comparing domain-specific heuristics, evaluating quantum-inspired approaches and deciding whether quantum hardware is worth exploring. In this role, the agent is not simply using quantum computing. It is helping decide whether quantum computing should be used at all.

FORMULATING PROBLEMS FOR QUANTUM USE

Problem formulation will be critical. Many commercial problems must be translated into mathematical

representations such as Quadratic Unconstrained Binary Optimisation (QUBO), Ising, Hamiltonian, variational or annealing-based models before quantum or quantum-inspired methods can be tested.

Choices around constraints, penalties, data encoding, circuit depth, noise and measurement overhead can determine whether the approach is meaningful. Agentic AI can help document these choices, test alternatives and compare outcomes against clear business and technical metrics.

Beyond optimisation, agentic AI could support research in drug discovery, batteries, advanced materials and chemistry by screening ideas, running initial simulations and identifying where deeper quantum-level analysis may be worthwhile. It could also help operate quantum systems through workload scheduling, calibration, error mitigation, backend selection and performance monitoring.

BUILDING READINESS WITH CLEAR GUARDRAILS

Governance must be built in from the start. These systems could influence decisions in finance, logistics, manufacturing, energy and healthcare research. Human oversight, explainability, auditability, cybersecurity and clear decision boundaries are essential.

Organisations should not wait passively for perfect quantum computers, but they should also avoid unrealistic expectations. The real opportunity lies in building readiness now: identifying the right problems, running focused pilots, developing talent, strengthening governance and learning how to orchestrate AI, classical systems, quantum-inspired methods and quantum hardware responsibly.

Agentic AI can help translate quantum potential into practical business impact. The organisations that benefit most will be those that apply these technologies with purpose, discipline and imagination. 🧠

The author is the Head of Business Incubation and Global Fujitsu Distinguished Engineer, Fujitsu Research of India.

feedbackvnd@cybermedia.co.in





DAVID HUGHES
SVP – SASE and Security,
HPE Networking

“AI is pushing security deeper into the network”

Artificial intelligence (AI) is changing not only what runs across enterprise networks, but also how those networks need to be secured. AI data centres generate intensive east-west traffic between GPUs, while inference workloads and autonomous agents introduce machine identities and communication patterns that conventional security architectures were not necessarily designed to handle.

David Hughes, SVP – SASE and Security, HPE Networking, believes this is pushing networking and security closer together. In this conversation with **Shubhendu Parth** at HPE Discover 2026 in Las Vegas, he discusses AI data centre security, agentic AI risks, machine identities, Zero Trust and autonomous networking, while explaining how HPE is embedding security and policy enforcement across its networking architecture. Excerpts:

AI clusters are creating east-west traffic patterns fundamentally different from traditional enterprise applications. How does this change network security architecture?

When you talk about an AI data centre and GPU interconnect, it is so different from a normal data centre that it really is its own category. The amount of bandwidth you need, the latency requirements and the uptime required are extremely high.

An AI data centre typically has a backend fabric and a frontend fabric. The backend fabric interconnects all those GPUs, so it is essentially all east-west traffic. There is typically a separate network connecting the cluster to the outside world, which carries what would normally be considered north-south traffic.

In any data centre, there are two main areas where you want security. One is north-south, covering what is going in and out. That is relatively similar for an AI data centre and a traditional data centre. The second is east-west security, where segmentation is commonly used.

In an AI data centre, however, organisations are not typically doing east-west segmentation inside the cluster because the performance requirements are so intense. In a traditional data centre, you would use micro-segmentation so that a workload communicates only with the workloads necessary to do its job. In an AI cluster, potentially every GPU needs to communicate with every other GPU. You are building a specially engineered network to maximise performance, which makes some of the security considerations very different.

As enterprises deploy AI systems and autonomous agents, are we creating a new attack surface that existing security architectures were not designed to protect?

There are a couple of different things here. One is the large AI data centre used for training. Another is AI deployed on-premises for inference, which may be rack or sub-rack scale infrastructure within a larger traditional data centre.

Deploying an inference pod isolated with north-south traffic going in and out does not necessarily create a fundamentally new attack surface. Everything you add creates some attack surface, but that is probably not the main issue.

The biggest new attack surface being created this year is with the deployment of agentic AI, particularly homegrown agentic. That creates a huge new attack surface because people are giving these machines human identities. When prompt injection and other techniques can be used to trick these agents, it opens up a Pandora's Box.

Zero Trust has traditionally focused on users and devices. Does it now need to extend to AI agents and other non-human identities?

Absolutely. Zero Trust Network Access (ZTNA) works

“Agentic AI creates a huge new attack surface because machines are being given human identities, while prompt injection and other techniques can trick these agents.”

very well for people. We look at the identity of a person and ensure that the only resources they can see on the network are those they need to do their job. The rest of the network is invisible.

We believe that is a great principle to apply to non-human identities as well, whether they are the Internet of Things (IoT) devices, workloads or agentic identities.

If you give an AI agent an identity, you can use that identity to drive policy determining what the agent can see. For example, you could configure an agent so that it can access only three specific resources. ZTNA can therefore provide a powerful set of guardrails, or a sandbox, around agent-to-agent and agent-to-service communications.

There is still a lot the industry needs to figure out around agent-to-agent security. ZTNA principles are one tool. Another is using capabilities in firewalls to intercept human-to-agent or agent-to-agent communications and put guardrails around them. For example, you could ensure that files being transferred do not contain private information, effectively applying data loss prevention principles to agentic communications.

We do not necessarily have to reinvent security. Techniques such as ZTNA, firewall inspection and proxy-based inspection can be extended and adapted to this new environment.

As networks, applications and infrastructure become more integrated, how important will full-stack telemetry and observability become to cybersecurity?

Telemetry is incredibly important. One thing sometimes overlooked is that the network is an awesome security sensor. Whether the threat involves data exfiltration, phishing or command-and-control channels, the associated data and packets travel over the network.

The network is therefore a great place to observe those threats and also to intercept and block them. But

cyber defence requires defence in depth. You also want visibility across infrastructure, compute, storage, virtual machines and workloads, collecting as much information about the environment as possible.

The whole point of observability is to drive actions. For many organisations, network, infrastructure and application observability are incredibly important to building a modern Security Operations Centre.

That instrumentation can identify anomalies, such as systems that do not normally communicate suddenly talking to each other or parts of the infrastructure communicating with a country where the organisation does not do business. That is important security information for the SOC.

AI fabrics place a lot of emphasis on performance and latency. Where should security enforcement sit when even microseconds matter?

It needs to be everywhere because security is about defence in depth. You need to look at it from all angles: the endpoint, firewall egress points, WAN gateways and SD-WAN gateways.

We also believe there is a lot of advantage in embedding security capabilities into access points and switches. One of the core premises of HPE's Universal ZTNA architecture is universal enforcement. When we need to block something, we want to block as close to the source as possible.

Ideally, if something malicious is happening and we want to quarantine or block a device, we should do that in the access point or the switch. Our approach is to distribute enforcement as far out as possible.

There are certain functions beyond simply blocking traffic. You may want to allow something through but inspect it, and that may not be suitable to run on an access point or switch. In those cases, inspection might happen at a gateway or firewall. For a remote worker at home, it may be performed in the cloud.

“With Marvis Actions, customers can choose whether they want a recommendation with a human in the loop or whether they want the action fully automated.”

HPE is moving towards increasingly autonomous networking through AIOps and self-driving capabilities. How do you ensure automated remediation can be trusted?

One of the things we believe is really important when building a self-driving network is making sure the efficacy is very good. Essentially, when AI is doing something, you need to ensure it is not making mistakes.

With our Mist-based self-driving capabilities, we have what we call Marvis Actions. They are curated using years' worth of data from customer trouble tickets and by looking at how those problems were remediated.

We then run the same model against historical data to determine whether an action is going to be trustworthy before introducing it. The user also has a choice. They can decide whether they want a recommendation with a human in the loop or whether they want the action automated.

Generally, for the actions we make available, we believe the accuracy is high enough for customers to automate them. But customers still need to build trust in the system. Organisations can begin with recommendations, retain human oversight and then increase the level of automation as confidence develops.

Will security eventually become an embedded property of the network rather than a separate stack? How is HPE approaching this?

We believe the network and security should be very closely tied together. If you have a security system that does not include the network, you are missing the threat-sensing capabilities of the network and its policy-enforcement characteristics. A modern network should not be built separately from security. A modern network needs security built in.

My business is the SASE and security business inside HPE Networking, and one of the core frameworks we see bringing security and networking together is Universal Zero Trust Network Access. Whether it is universal policy,

universal identities or universal enforcement, these are aspects we are building into our network infrastructure.

At the architectural level, there are several dimensions. The first is secure design, ensuring that we get the fundamentals right in our development processes. The second is ensuring that hardware has not been tampered with in transit, so when somebody receives a switch, they know it has not been compromised.

Another aspect is maintaining a secure software supply chain. That is not easy. There have been numerous compromises involving open-source repositories, with organisations pulling software from those repositories and becoming infected themselves. Software supply-chain security is therefore extremely important.

There is also an opportunity to use frontier AI to find vulnerabilities more effectively, address existing vulnerability backlogs and ensure that software continues to be checked as it is developed.

Another element involves technologies for ensuring privacy and trust, including IPsec, MACsec and TLS, and, going forward, quantum-safe versions of those technologies.

Then there is minimising the blast radius so that when a breach occurs, it can be contained automatically. Technologies such as VLANs, firewall zones and micro-segmentation contribute to that. Universal Zero Trust helps prevent lateral movement, while advanced threat-protection capabilities within our SASE and security offerings can detect threats in files and monitor and intercept active threats on the network based on behaviour.

Ultimately, networking teams and security teams should not operate as separate worlds. When the network itself can sense threats, apply identity-based policies and enforce security controls close to the source, networking and security can become force multipliers for each other. 🧠

shubhendup@cybermedia.co.in

Outside-in testing exposes digital infrastructure blind spots

Real-world benchmarking tracks how infrastructure performs in different places, networks, and devices, adding useful insight beyond standard monitoring.



BY CHANDRASEKAR RAMAMOORTHY

Digital infrastructure is conventionally measured through internal dashboards, network availability, server uptime, link utilisation, latency metrics, cloud health indicators and capacity reports. These remain indispensable for daily operations and investment planning. Yet they do not always show how infrastructure performs from the perspective of the person actually using it.

As digital ecosystems become more distributed and interconnected, this measurement gap becomes increasingly significant. A network can appear healthy, servers can be fully operational, and cloud resources can remain comfortably within their thresholds while

users in a particular city, on a particular access network or using a particular device still face delays, inconsistent connectivity, packet loss or sluggish responsiveness. Individual components can be working as designed even when the experience they collectively deliver falls short.

Real-world performance benchmarking provides an additional measurement layer by examining digital infrastructure under the conditions in which services are actually consumed.

MEASURING INFRASTRUCTURE FROM THE OUTSIDE

Where traditional monitoring offers an inside-out view of infrastructure health, field-based benchmarking takes

A network can look healthy, servers can remain operational and cloud capacity can be ample, yet the experience at the other end can still fall short.

an outside-in perspective, measuring performance across geographies, access technologies, network routes and device types. Instead of relying only on what infrastructure reports about itself, it tests how that infrastructure behaves when users on different networks and devices are at the other end.

This becomes relevant because of the complexity of a single digital interaction. One transaction might pass through mobile or fixed broadband, Domain Name System (DNS) resolution, internet routing and peering, a cloud region, a content delivery network (CDN) node, Wi-Fi and, finally, a device. Each layer may perform adequately on its own, with problems surfacing only through the way these layers interact.

Conventional monitoring tools, built largely to observe individual infrastructure layers, can miss these cross-layer effects. An organisation can therefore meet the targets on its operational dashboards while still experiencing performance issues that affect users.

MEASURING PERFORMANCE ACROSS NETWORKS

A field-based benchmarking framework looks across several dimensions simultaneously. Geography is one of the major variables, as performance can differ between metropolitan centres, smaller cities, rural regions, enterprise campuses and high-density urban areas.

Access technology is another variable. Users may connect through 4G, 5G, fibre, fixed wireless, enterprise networks or public Wi-Fi. Device diversity adds another layer, particularly in markets where the installed base spans a wide mix of smartphones, operating systems and networking hardware.

The objective is not simply to establish whether infrastructure is available. It is to measure whether it delivers a consistent, reliable and responsive experience across these different conditions, rather than only those under which individual components have been tested.

HOW BENCHMARKING REVEALS NETWORK GAPS

This approach provides another way of assessing infrastructure performance for telecom operators, internet ser-



IN BRIEF

- Traditional uptime, capacity and latency metrics remain essential, but cannot always show how infrastructure performs for actual users.
- Outside-in benchmarking adds a real-world layer, testing performance across geographies, access technologies, routes and device types.
- Cross-layer problems can emerge between networks, DNS, cloud, CDN, Wi-Fi and devices even when each component appears to work normally.
- Granular measurements can uncover regional and network-level disparities that national averages and aggregated infrastructure data may conceal.
- Real-world evidence can help identify bottlenecks, prioritise investment and determine whether infrastructure upgrades improve actual performance.
- Combining operational monitoring with field benchmarking provides a fuller end-to-end view of increasingly distributed digital infrastructure.

vice providers, cloud and CDN providers, enterprises, regulators and policymakers. Payments, healthcare, education, logistics and government platforms all depend on the underlying digital infrastructure performing consistently.

The weakest point in a digital interaction may not sit within one network or platform, but emerge where broadband, routing, cloud and devices intersect.

Is Your Network Performing Well?

A practical outside-in checklist for network and infrastructure teams.

01 CHECK GEOGRAPHY

Compare performance across metros, smaller cities, rural regions, campuses and high-density areas.

02 TEST ACCESS NETWORKS

Validate performance across 4G, 5G, fibre, fixed wireless, enterprise networks and public Wi-Fi.

03 FOLLOW THE ROUTE

Examine DNS resolution, routing, peering, handoffs and CDN paths for latency, jitter or packet loss.

04 INCLUDE DEVICES

Test across representative devices, operating systems and network hardware in real-world conditions.

05 LOOK END TO END

Assess the complete service journey. Healthy components do not always mean a healthy user experience.

06 VERIFY THE INVESTMENT

Measure before and after upgrades to confirm that investments deliver real-world improvements.

OUTSIDE-IN TESTING

Measures digital services from the user's perspective across locations, networks, routes and devices.

WHAT TO MEASURE

LATENCY

Time taken for data to travel across the complete journey.

JITTER

Variability in latency that affects real-time applications.

PACKET LOSS

Lost packets that impact reliability and performance.

THROUGHPUT

Actual data rates achieved by users across different conditions.

AVAILABILITY

Ability of the service to be consistently reachable and usable.

USER EXPERIENCE

Responsiveness and consistency as experienced by real users.

Granular measurements can reveal differences that aggregated infrastructure metrics may obscure. A national average, for example, can appear healthy while specific regions experience persistent degradation. Similarly, broadband can deliver its advertised speed while users encounter latency, jitter or DNS issues that broader metrics may not reveal.

These measurements can also inform infrastructure investment. Network and infrastructure upgrades involve significant capital expenditure and long planning cycles. Identifying where bottlenecks occur can help organisations prioritise capacity expansion, optimise routing and peering, and assess whether previous investments have resulted in measurable improvements in performance.

The same measurement approach can assist with accountability across interconnected infrastructure. A single user experience is typically shaped by multiple stakeholders, with each responsible for only one part of the delivery chain. When a performance problem occurs, individual dashboards may show that each component is operating normally, making root-cause analysis more difficult.

A shared, evidence-based performance reference can help identify where degradation originates and support coordination between stakeholders. For policymakers, similar measurements can complement coverage and installed-capacity statistics as governments expand broadband, 5G and digital public services across regions with significant variations in geography, connectivity and devices.

MEASURING DIGITAL INFRASTRUCTURE END TO END

As digital infrastructure expands, coverage, capacity and uptime remain important measures of performance. Real-world benchmarking adds another dimension by showing how that infrastructure behaves across different networks, locations, routes and devices.

Combining the inside-out view provided by operational monitoring with an outside-in view of real-world performance can provide a more complete picture of infrastructure behaviour. It connects the performance of individual components with the experience produced by the wider infrastructure chain.

For increasingly distributed digital ecosystems, this end-to-end measurement can help identify cross-layer performance issues that remain difficult to detect through conventional monitoring alone. It provides a way to assess whether infrastructure capacity and availability translate into consistent performance under the conditions in which digital services are actually used. 🧩

The author is the Chief Product Officer of Mozark.

feedbackvnd@cybermedia.co.in



AIoT convergence moves intelligence closer to the action

Connected assets are becoming contextual systems that anticipate events, make decisions and respond in real time within clearly defined, governed boundaries.



BY SUNIL DAVID

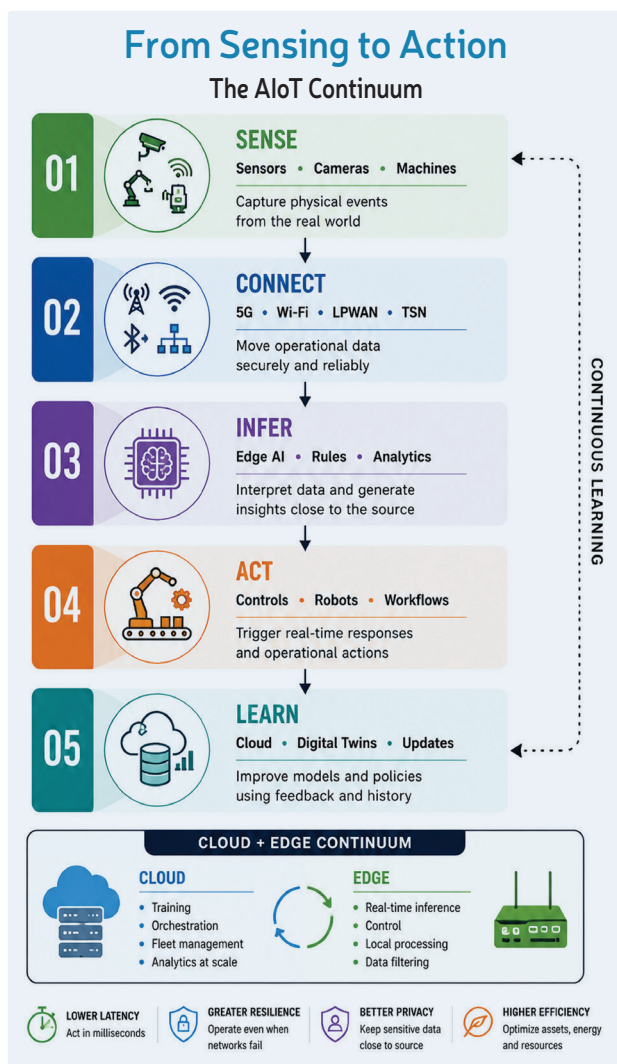
Enterprises have spent much of the past decade connecting machines, products, buildings and infrastructure. Yet connectivity by itself does not create transformation. The real breakthrough occurs when connected assets can understand context, anticipate outcomes and trigger the right response at the right time. This is why the convergence of AI, the IoT, and edge computing, often described as the Artificial Intelligence of Things (AIoT), has become so important.

IoT creates visibility into the physical world, AI converts data into intelligence, and edge computing brings that intelligence closer to where events occur. Together,

they move organisations from connected operations towards contextual, predictive and increasingly autonomous systems.

The shift is already visible across industries. Billions of connected devices are producing continuous streams of operational data, while AI and edge computing are emerging as key accelerators of the next phase. Value is no longer derived simply from connecting assets. It comes from combining operational data, domain knowledge and AI so that systems can anticipate, decide and act across factories, fleets, buildings, hospitals and public infrastructure.

AIoT follows a sense-connect-infer-act-learn loop, linking sensors and networks with edge intelligence, physical action and continuous cloud-based learning.



and fleet management, while the edge supports real-time inference and control. Physical and agentic AI take this further by enabling machines, robots and software agents not merely to generate insights, but also to coordinate actions.

HOW THE AIoT ARCHITECTURE WORKS IN PRACTICE

A useful way to understand this architecture is through five stages: sense, connect, infer, act and learn. Sensors, cameras and machines first capture what is happening. Technologies such as 5G, Wi-Fi, low-power wide-area networks (LPWAN) and time-sensitive networking transport the data. Edge AI, rules engines and stream analytics interpret it.

The system responds through alerts, controls, robotics or workflows, while cloud platforms, digital twins and fleet updates create a continuous learning loop. Models and policies improve as real-world outcomes are observed.

This explains why the cloud alone is not sufficient. Many operational decisions cannot wait for data to travel to a distant data centre and back. Milliseconds matter in safety, motion control, quality inspection and autonomous response. Edge processing also improves resilience when connectivity is weak and reduces bandwidth costs by filtering high-volume sensor and video streams.

It can also support privacy and data sovereignty and provide the predictable performance required by industrial control. The winning architecture is therefore hybrid: each workload should be placed where it creates the most value.

WHERE AIoT CONVERGENCE CREATES VALUE

The business outcomes are compelling. The convergence can improve uptime by predicting failures and optimising maintenance, raise quality through defect detection at line speed, strengthen safety by identifying hazards, and reduce energy use by optimising equipment and facilities. It can also improve agility and create new revenue models, such as remote services and outcome-based offerings.

Several technology trends are accelerating this evolution. TinyML and more efficient models are enabling inference on microcontrollers, cameras, gateways and industrial PCs. Multimodal sensing combines vision, audio, vibration, location and process data to provide richer situational awareness. Private 5G networks support mobile assets, robotics and distributed operations that require reliable, low-latency connectivity.

The cloud and edge are also becoming part of a single continuum. The cloud handles training, orchestration

Edge processing can filter high-volume sensor and video streams locally, reducing bandwidth demands while supporting privacy and data sovereignty.

The strongest business cases usually combine multiple outcomes. These may include quality with speed, or uptime with energy efficiency, rather than pursuing a single isolated benefit.

HOW AIoT IS BEING DEPLOYED IN PRACTICE

Real-world deployments illustrate the potential. Siemens Energy connected legacy and modern assets across 18 factories and scaled more than 30 use cases. Its connected-factory programme reportedly reduced data-collection time by 50%, lowered maintenance costs by 25% and improved machine availability by 15%.

P&G adopted a cloud-managed edge architecture to standardise AI deployment across a large manufacturing estate and reported reductions of up to 90% in model-deployment time. This demonstrates that scaling AIoT is as much an operating-model and lifecycle-management challenge as it is a model-development challenge.

At Bengaluru International Airport, more than 500 live camera feeds support edge-based vision AI use cases. Processing video closer to the source enables faster situational awareness, more efficient terminal operations and better passenger experiences without transmitting every raw frame to a central cloud.

The opportunity extends far beyond manufacturing. In energy and utilities, AIoT can support grid intelligence, asset inspection and fault detection. In healthcare, wearables and bedside devices can enable privacy-preserving inference. Retailers can use smart shelves, automated checkout and store analytics.

Mobility and logistics companies can improve routing, cargo safety and driver performance, while agriculture can benefit from precision irrigation, crop vision and equipment monitoring. Across these sectors, the common principle is to bring intelligence closer to physical operations while retaining the cloud for broader coordination, learning and management.

WHAT HOLDS BACK ENTERPRISES TODAY

Enterprises must overcome significant barriers before AIoT can move from promising deployments to scalable operational systems. Fragmented operational technology

(OT), information technology (IT) and engineering data often lack common context. Many initiatives remain trapped in “pilot purgatory”, proving technical feasibility without establishing repeatable economics. Legacy assets and proprietary protocols also limit interoperability.

Model drift, version control and remote updates become harder across thousands of edge nodes. Cyber-physical risk is especially serious because a compromised device or model can affect real-world operations. Skills and ownership are also fragmented across AI, cloud, OT and business teams, making coordination essential as deployments move from pilots to production.

BUILDING A PRACTICAL ENTERPRISE PLAYBOOK

It begins with a clear key performance indicator (KPI) and a costly, recurring operational problem. Edge and cloud should be designed together. Data must be enriched with asset, process, event and business context. Security must be embedded through identity, signed software, segmentation, zero-trust principles and continuous monitoring.

Organisations must also industrialise machine learning operations (MLOps) for fleet deployment, observability, rollback and governance. Most importantly, they must scale a reusable platform rather than a collection of disconnected pilots. This creates a consistent foundation for managing models, devices, policies and updates across distributed environments.

The destination is not “lights-out everything”. It is governed autonomy: machines and agents acting within clearly defined boundaries, with security, transparency and human accountability. Connectivity is not the destination; the edge is the decision frontier, and autonomy must always be governed.

AI, IoT and edge computing are not merely converging technologies. Together, they form the architecture of a more responsive, resilient and intelligent enterprise. 🌟

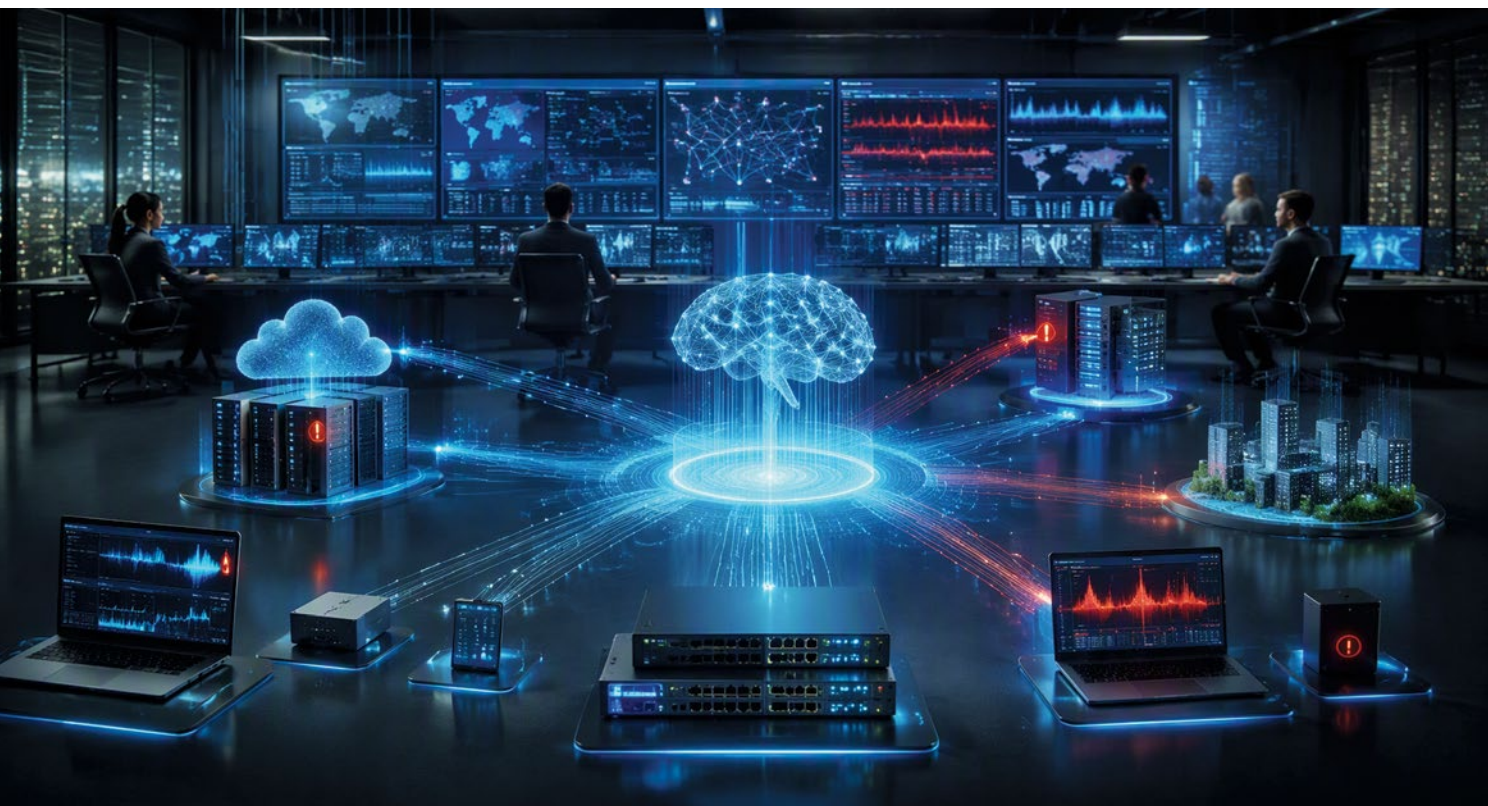
The author, a former Regional Director for IoT (India & ASEAN) at AT&T, is a Digital Tech Consultant.

feedbackvnd@cybermedia.co.in



Distributed infrastructure puts observability to a new test

AI-driven telemetry is connecting IT operations and security, giving technology teams a broader view of performance, threats and system behaviour.



BY ROHIT SHUKLA

Hybrid work has rapidly evolved from a temporary adjustment into a long-term model for enterprises across industries in India. Driven largely by the growth of India's digital economy and its sizeable workforce with advanced technology skills, organisations are increasingly embedding hybrid work into their business and talent strategies.

India's digital economy is anticipated to account for almost 20% of the country's GDP by 2029, reflecting the growth of technology-enabled business models. For enterprises managing teams across multiple cities and global delivery centres, hybrid work has progressed from a short-term adjustment to a core business strategy.

Workforce expectations are reinforcing this shift. According to Great Place to Work India's report, Voice of India on Return to Office, 63% of Indian employees currently work fully on-site, while hybrid work remains the preferred model for 39% of the workforce.

This shift is also changing enterprise technology environments. Employees access corporate resources using multiple tools across different locations and networks, while cloud applications and remote access tools add operational complexity. Traditional monitoring tools can prove inadequate in such distributed environments, increasing the need for greater visibility across applications, networks, devices and infrastructure.

The real observability challenge is no longer collecting more telemetry, but connecting signals fast enough to reveal what is happening across distributed systems.

HOW OBSERVABILITY EXTENDS IT VISIBILITY

Observability refers to an organisation's ability to gain deep, real-time visibility into the health and performance of its IT environment through telemetry data such as logs, metrics, traces and events. Unlike traditional monitoring, observability enables teams to understand not only what went wrong, but also why it happened and how it affects the broader digital ecosystem.

In hybrid work environments, observability provides end-to-end visibility across applications, networks, devices, cloud infrastructure and user interactions. This allows IT teams to identify performance bottlenecks proactively, monitor network health, troubleshoot issues faster and maintain seamless digital experiences regardless of employee location.

For enterprises managing thousands of remote endpoints and cloud-based workflows, real-time visibility is particularly important. Even minor disruptions, such as degraded cloud application responsiveness, can directly affect productivity and employee experience.

HOW AI IS CHANGING IT OBSERVABILITY

Predictive and automated issue resolution powered by artificial intelligence (AI) is also changing how observability supports enterprise operations. Observability platforms can ingest high volumes of telemetry streams and perform real-time anomaly detection, pattern recognition and root-cause analysis to identify issues before they manifest as outages.

This can shift IT workflows from reactive firefighting towards proactive operations, helping reduce downtime, improve efficiency and increase service reliability. As hybrid work adds complexity to enterprise technology environments, observability is consequently evolving from an IT operations-focused tool into a broader strategic capability.

OBSERVABILITY AS A SECURITY CAPABILITY

The expansion of hybrid work has also significantly widened the enterprise attack surface. Nearly 77% of Indian organisations experienced at least one identity-related

security breach in the past year, highlighting growing risks associated with distributed work environments and cloud adoption.

Modern observability systems enable IT and security teams to monitor system behaviour continuously and analyse suspicious activity across complex distributed environments. This can include unusual login attempts, abnormal network traffic, unauthorised attempts to access systems and sudden changes in application behaviour.

Observability systems can provide contextual information that helps security teams detect and respond to such activity more quickly. As cyberattacks become more sophisticated and distributed work environments continue to expand, this visibility is becoming increasingly relevant to enterprise cybersecurity strategies.

CONNECTING PERFORMANCE AND CYBER RESILIENCE

As hybrid work environments continue to evolve, maintaining seamless digital experiences, operational continuity and strong cybersecurity requires greater real-time visibility across applications, networks, cloud environments and endpoints.

Observability brings together operational visibility, AI-driven insights and security intelligence across these distributed environments. For Indian organisations, this can support proactive performance management, faster troubleshooting and incident response, and stronger cyber resilience.

As enterprise technology environments become more decentralised, the role of observability is therefore expanding alongside the infrastructure it monitors. Its ability to connect telemetry across different parts of the IT environment gives technology teams a broader view of performance and security across increasingly distributed operations. 🌟

The author is APJC Leader at SolarWinds.

feedbackvnd@cybermedia.co.in



Beyond GPS, real-time visibility becomes the new standard

Connected platforms turn live operational data into actionable intelligence, helping logistics firms anticipate disruptions and improve efficiency at scale.



BY NITIN O MAHIPAL

For the past few decades, GPS tracking has served as the gold standard for visibility in logistics. Knowing the location of a vehicle at any given moment has transformed fleet management, improved route planning and provided customers with greater confidence in delivery timelines. Today, as supply chains become increasingly complex and customer expectations continue to evolve, the industry is realising that tracking location alone is no longer enough.

Logistics companies are entering an era where real-time visibility goes far beyond dots moving on a map. Businesses now demand live information on shipments, operational bottlenecks, delivery exceptions, driver behaviour, inventory movement and customer interactions. Visibility is no longer simply a

value-added feature; it is becoming a foundation for efficient logistics operations.

The rise of e-commerce, quick commerce and just-in-time supply chains has significantly increased expectations around speed and predictability. Customers no longer want to know only that their shipment has left the warehouse or entered a city. They expect accurate estimated arrival times, proactive updates in case of delays and transparency throughout the journey. Similarly, enterprises managing large supply chains need actionable intelligence that allows them to make decisions before disruptions affect operations.

HOW LOGISTICS VISIBILITY IS EVOLVING

This shift has changed the role of technology in logistics. Traditional GPS systems answered the question, “Where

is the truck?" Modern visibility platforms address more critical questions, such as "Will the shipment arrive on time?", "What risks could delay delivery?" and "What corrective action can be taken immediately?"

Real-time visibility brings together data from multiple sources, including telematics systems, route optimisation tools, warehouse management systems, Internet of Things (IoT) sensors, customer interfaces and driver applications. When these systems communicate with one another, logistics companies gain a dynamic view of operations rather than a series of isolated snapshots.

For example, when traffic congestion causes a delay on a key route, an intelligent visibility platform can immediately update the estimated time of arrival, notify customers, recommend an alternative route and alert operations teams to adjust downstream activities. This level of responsiveness improves efficiency while strengthening customer trust.

The advantages become particularly important in industries where time sensitivity is critical. Healthcare logistics, automotive manufacturing, retail distribution and industrial supply chains rely heavily on predictability. A delayed shipment in these sectors can lead to production stoppages, stock shortages or service disruptions, with substantial financial consequences. Real-time visibility helps organisations anticipate issues rather than react after the disruption has occurred.

TURNING LOGISTICS DATA INTO INTELLIGENCE

Operational optimisation is another important benefit. Logistics companies generate large volumes of data every day, but data without context offers limited value. Visibility platforms can transform raw information into actionable insights by identifying recurring delays, underutilised assets, inefficient routes and operational bottlenecks. These insights can help businesses improve fleet utilisation, reduce idle time and optimise resource allocation.

Driver management is another area undergoing significant change. Modern visibility tools can assess route adherence, driving patterns, fuel efficiency and stoppage durations in real time. Rather than functioning solely as surveillance mechanisms, these systems can support safer driving practices, improve productivity and contribute to more sustainable operations.

Sustainability has also become a significant driver of investment in visibility technology. As organisations seek to reduce emissions and improve environmental

performance, access to real-time operational data becomes increasingly important. Better route planning, reduced fuel consumption, fewer empty return trips and improved vehicle utilisation can contribute to lower carbon footprints while improving profitability.

WHY VISIBILITY MATTERS MORE IN INDIA

In India, the need for enhanced visibility is particularly significant given the scale and diversity of the logistics ecosystem. Long-distance transportation, varying infrastructure conditions and multimodal supply chains create operational complexities that require faster decision-making and greater coordination. Real-time visibility can help logistics providers maintain consistent service despite these challenges.

Globally, this evolution is reshaping the logistics sector, with technology shifting from a support function to a core part of operations. Integrated digital platforms and tracking systems can connect information across fleets, warehouses, drivers and customers, creating greater accountability and enabling faster operational decisions.

The future of logistics will not be defined only by how many vehicles a company operates or how extensive its network becomes. Competitive advantage will increasingly depend on how efficiently organisations capture, analyse and act on real-time information. Artificial intelligence and predictive analytics will further enhance this capability by identifying potential disruptions before they occur and recommending preventive action.

BUILDING CONNECTED LOGISTICS OPERATIONS

The logistics industry has always played a key role in moving goods from one location to another. Increasingly, however, it is also about moving information with the same speed and precision. Companies that embrace this transformation will be better positioned to deliver reliability, agility and customer satisfaction in an increasingly demanding market.

GPS may have started the visibility revolution, but it is only the beginning of the journey. The future lies in logistics ecosystems that are connected, intelligent and capable of making decisions in real time. In that future, visibility will not simply be a differentiator; it will be the minimum standard expected by customers and businesses. 🌟

The author is the Managing Director of Mega Freight Movers.

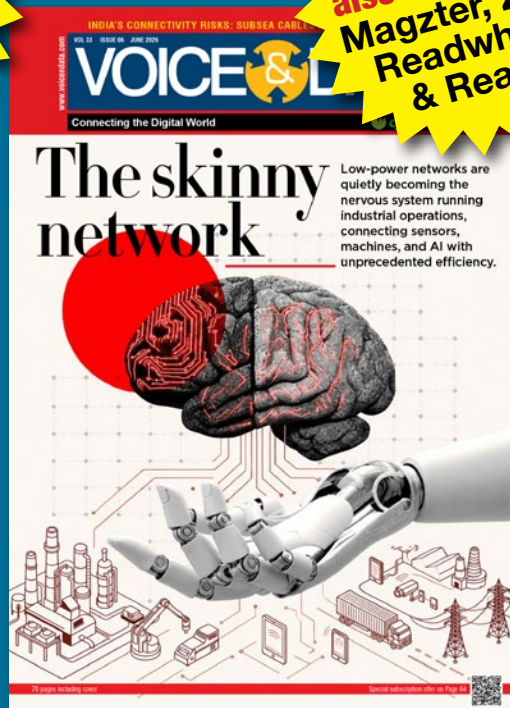
feedbackvnd@cybermedia.co.in



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

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

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



Book Digital Subscription Now!

Web: subscriptions.cybermedia.co.in/voicendata.aspx, For Digital subscription Contact: Alok Saxena

Email: aloksa@cybermedia.co.in, Call: 99531 50474

Yes! I want to subscribe to Voice&Data



Scan QR Code
& Subscribe now...

Subscribe to Digital Edition @ ₹735/-

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

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

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

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

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

Name [•]: Mr/ Ms _____ Date of Birth:

Organisation: _____ Designation: _____

Delivery Address: _____

City: _____ State: _____ Postal Code:

Mob [•]: Tel: Email [•]: _____

GST No. [•]: PAN No. [•]:

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

Payable at (specify bank and city) _____

OR

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

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

[•] Essential fields

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

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

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

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

For Subscription queries:

9289870545

Terms & Conditions: _____

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

India's defence drone push moves deeper into the tech stack

From sensors and propulsion to secure communications and resilient navigation, strategic autonomy now depends on controlling the technologies inside the UAV.



BY PRATIMA HARIGUNANI

In a memorable scene from the movie Uri: The Surgical Strike, national security strategist Govind Bhardwaj, played by Paresh Rawal, is looking for something that can help soldiers watch and read the enemy before executing a surgical strike. His attention falls on an intern working on what appears to be a side project.

The project is an Unmanned Aerial Vehicle (UAV), named Garuda. During a demonstration, the intern explains its camera, range, hovering capability and battery life. Bhardwaj immediately sees its potential and asks him to build more.

India has come a long way from the days when such projects were on the fringes and UAVs were a novelty in military operations. More recently, Operation Sindoor offered a glimpse of the significance of these systems.

From surveillance and attacks to real-time strategic manoeuvres, drones have become increasingly important in the defence landscape.

That is precisely why it matters for these systems to be designed, engineered, assembled and equipped within the country. Indigenisation carries a very different connotation for this category of technology. It is about more than self-reliance; it has implications for defence readiness, resilience and strategic autonomy.

BUILDING INDIA'S INDIGENOUS DRONE STACK

India's defence drone ecosystem has evolved rapidly over the past few years, says Agenda Kumar, Managing Director, Esri India, a player in geographic information systems (GIS), mapping and spatial data analytics technology.



“We are seeing serious investment beyond airframes in autonomous navigation, AI-driven decisions, secure communications, edge computing and resilient software.”

RADHA KRISHNAN

Founder & President, Detroit Engineered Products

“The emphasis has shifted towards building complete indigenous capabilities encompassing drones, sensors, command-and-control systems, AI-driven analytics, geospatial intelligence, and mission-critical software. Drones are becoming intelligent sensing platforms that continuously collect vast volumes of imagery and real-time data.”

Indigenisation has also matured, says Radha Krishnan, Founder and President, Detroit Engineered Products (DEP), a product engineering company. “Earlier, it often meant assembling products locally. Now the focus is steadily moving towards developing critical technologies within India, from flight control systems and mission software to sensors, electronics, and propulsion. There is still work to be done in some areas, but the direction is clear, and the ecosystem is becoming deeper with every passing year.”

There is also reason to be upbeat about how UAVs are changing the defence ecosystem, says Joseph Sudheer, Global CEO and Managing Director, Magellanic Cloud, a digital engineering player with a presence in drone technology.

“The biggest change I have observed is that drones are no longer viewed as support assets. They are increasingly becoming central to military planning, operational execution, and force multiplication strategies. Three or four years ago, most discussions focused on surveillance, reconnaissance, and intelligence gathering. Today, conversations have expanded significantly. Global conflicts have demonstrated the effectiveness of loitering munitions, swarm technologies, autonomous targeting systems, and precision-strike capabilities. These developments are influencing defence priorities worldwide, including in India.”

India's defence ecosystem, he explains, is moving towards integrated unmanned capabilities where surveillance, targeting, communication relays, electronic



IN BRIEF

- India's defence drone story is moving beyond assembly as indigenous capabilities expand across flight systems, sensors, AI and mission software.
- Drones are moving to the heart of warfare, combining surveillance, targeting, communications and precision engagement in integrated operations.
- Simulation, GeoAI and extreme-condition testing are accelerating how indigenous UAVs are designed, validated and prepared for missions.
- India's toughest localisation battle now lies inside the drone, from advanced sensors and propulsion to semiconductors and secure communications.
- Contested operations raise the stakes as spoofing, jamming and interception make survivability and resilient navigation mission-critical.
- The ultimate test of self-reliance is technology control: who owns what allows a drone to sense, navigate, communicate, survive and strike.



“Beyond manufacturing, India must strengthen testing, certification and export competitiveness to build globally competitive drone technologies entirely at home.”

JOSEPH SUDHEER

Global CEO & Managing Director, Magellanic Cloud

How Deep Does Drone Indegenisation Go?

Mapping India's strengths, gaps and the technologies that will define the next phase.



STRONGER DOMESTIC CAPABILITY

Areas where Indian industry has built depth and delivered.



Airframes



Software and firmware



Guidance and navigation



Mission software



System integration



AI-enabled analytics



Payload integration



LOCALISATION GAPS REMAIN

Critical components and technologies still dependent on external sources.



Ruggedised flight controllers



EO/IR and specialised sensors



Advanced propulsion systems



EW-resilient communication modules



Semiconductors



Advanced batteries



Testing infrastructure



THE NEXT TECHNOLOGY TEST

As UAVs operate in contested environments, localisation must extend into:



Secure communications
Encrypted, tamper-proof and resilient links



Anti-jamming capability
Robust links and spectrum agility to stay connected



Resilient navigation
GNSS-independent systems for GPS-denied ops



Autonomous fail-safe systems
Smart decision-making with built-in safety protocols



Electronic warfare
Detect, withstand and respond to EW threats



Survivability
Low observability, hardening and mission resilience

warfare and precision engagement work together within a single operational framework.

“Defence production and exports have both witnessed strong growth in recent years, reflecting increased confidence in indigenous technologies. From my perspective, we are not moving away from surveillance; we are building upon it. Surveillance remains the starting point, but the future battlefield increasingly demands systems that can sense, analyse, decide, and act with greater speed and precision than ever before.”

India's manufacturing sector has also advanced self-reliance in defence, aerospace and electronics, with local capabilities in drone platforms, including airframes, software and components, as well as aircraft electronics, mission systems and electronic warfare, says Alvin Anthony, Co-Founder and Chief Executive Officer, NextLeap Aeronautics.

Kumar illustrates how technologies surrounding drones are also becoming important. “Indo ArcGIS enables the integration of data from drones, satellites, sensors, and field assets into a common operational picture, providing commanders with real-time situational awareness and AI-driven decision support.”



“Indigenous development gives greater control over critical technologies, enables mission-specific customisation and reduces lifecycle dependence on external vendors.”

ALVIN ANTHONY

Co-Founder & Chief Executive Officer, NextLeap Aeronautics

He adds that Esri India works with organisations such as the Defence Research and Development Organisation (DRDO) and Bharat Electronics Limited (BEL) on geospatial technologies. Such capabilities can support operational coordination, situational awareness and faster decision-making for the armed forces.

DEEPENING THE INDIGENOUS TECHNOLOGY STACK

Krishnan points to engineering and simulation as another area supporting the development of next-generation defence drones. “Instead of waiting days or weeks for simulation results, engineers can predict aerodynamic, structural and thermal performance in minutes, explore multiple design options, and optimise them early in the development cycle. That means faster prototyping, quicker validation, and more time spent improving mission capability rather than running repetitive simulations.”

From an indigenisation standpoint, he says these capabilities enable Indian defence organisations to build AI models using their own engineering data and domain knowledge. This can reduce reliance on external datasets and long development cycles while helping create sovereign engineering intellectual property.

“With capabilities such as AI-driven geometry optimisation and autonomous engineering workflows, it can support the rapid development of future-ready drone platforms designed, validated and evolved entirely within India’s defence ecosystem.”

Sudheer reinforces the change taking place across the ecosystem. “Over the last five years, I have witnessed a remarkable transformation in India’s UAV ecosystem. When we started discussing drone indigenisation seriously, most manufacturers were assembling imported components. Today, India has developed strong capabilities across airframes, flight controllers, mission software, AI-enabled analytics, and specialised payload

integration. Government initiatives such as the Drone Rules 2021 and the Production Linked Incentive (PLI) scheme have accelerated this transition.”

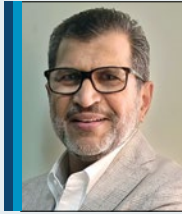
This shift, however, goes deeper than a ‘Made in India’ tag. Indigenisation draws its significance from the ecosystem of capabilities that can be built into and around these aerial platforms.

Krishnan echoes this direction. “Over the last few years, the conversation has shifted from simply buying drones to building a complete drone ecosystem. That is a far more meaningful change. Today, we are seeing serious investment not just in airframes, but in the technologies that make drones reliable in contested environments: autonomous navigation, AI-driven decision-making, secure communications, edge computing, swarming, and resilient mission software.”

Anthony points to developments at the core of these systems as well. “We see investments happening in semiconductor development, which is one of the key requirements for all the electronic components required for the aerospace and defence sector. India has made strong progress in system-level design integration and manufacturing for defence, aerospace, and electronics.”

Kumar adds that the real value lies in converting the data generated by drones into actionable intelligence. “This is where GIS and GeoAI play a critical role. These technologies enable commanders to integrate data from multiple sources, visualise the operational environment in real time, assess threats, plan missions, and make faster, more informed decisions.”

Drone imagery can also be rapidly processed into high-quality 2D and 3D mapping products. “These outputs can be quite consequential to support mission planning, terrain analysis, border surveillance, infrastructure monitoring, damage assessment, and enhanced situational awareness. By transforming raw



“By transforming raw drone imagery into actionable geospatial intelligence, defence teams can make faster, more informed and mission-critical decisions.”

AGENDRA KUMAR
MD, Esri India

drone imagery into actionable geospatial intelligence, defence personnel can make faster, more informed operational decisions.”

Testing is as important as manufacturing because the consequences of real-world use are considerably greater than in most commercial applications. Sudheer cites work undertaken in challenging regions such as Leh.

“Establishing UAV development, testing, and maintenance capabilities at high altitudes is an achievement in itself. These environments allow us to validate aircraft performance under low air density, extreme temperatures, and demanding operational conditions that many drone systems struggle to handle. The insights gained from such testing directly improve the reliability and robustness of our platforms.”

CLOSING THE CRITICAL LOCALISATION GAPS

What has been achieved so far represents only part of what will be required as the role of UAVs in military surveillance and operations becomes deeper and more sophisticated. That translates into a need for greater self-sufficiency across multiple layers of the technology stack.

Advanced propulsion systems, high-end electro-optical sensors, semiconductor dependencies and specialised battery technologies still require deeper localisation, Sudheer says. “Beyond manufacturing, India must also strengthen testing infrastructure, certification pathways, and export competitiveness. I believe the next phase will be about creating globally competitive drone technologies that are designed, engineered, and continuously evolved in India.”

Anthony says India has achieved strong localisation in airframes, precision-machined parts, software and firmware, guidance and navigation systems, and system integration, supported by domestic engineering capabilities.

But challenges persist at the component level. These include “high-performance ruggedised flight

controllers, specialised sensors (e.g., EO/IR payloads), advanced propulsion systems (motors, ESCs), secure EW-resilient communication modules, and advanced batteries”, which remain partially import-dependent because of the developing semiconductor ecosystem and testing infrastructure.

For Sudheer, true self-reliance extends far beyond manufacturing components domestically. “It means developing the engineering expertise, testing environments, supply chains, and operational capabilities required to build reliable systems for India’s unique conditions.”

He adds: “Beyond manufacturing, we have invested heavily in indigenous flight systems, autonomous technologies, AI-powered analytics, and mission-specific payload integration. This enables us to tailor solutions for defence, surveillance, industrial inspection, and critical infrastructure sectors. For me, localisation is ultimately about building confidence in Indian technology.”

There are several areas that will need to be strengthened as the industry expands. While significant advances have been made in vertical take-off and landing (VTOL) architectures, payload flexibility, mission software, AI integration, endurance and platform customisation, Sudheer believes the next phase of competitiveness will be defined by survivability and mission effectiveness.

Collaboration is another important shift, Krishnan points out. “Large defence companies, startups, MSMEs, academia, and government organisations are working much more closely than before. That creates a stronger innovation pipeline because different players bring different strengths to the table. No single company can build the future of autonomous defence systems alone.”

PREPARING DRONES FOR CONTESTED OPERATIONS

Limitations in current devices and systems are also

A drone may carry a Made in India tag, but true autonomy lies in who controls its flight controller, sensors, data links, propulsion and core mission software.

emerging in soft-kill counter-drone capabilities, particularly against autonomous drones, pre-programmed routes, frequency-hopping links and one-way attack UAVs, according to Fortune Business Insights.

This is driving the development of hard-kill interceptors, high-power lasers, radio-frequency effectors and integrated command-and-control systems capable of detecting and classifying threats, assigning an effector and neutralising the threat. The direction is towards integrated counter-UAS systems combining radar, radio-frequency detection, electro-optical and infrared tracking, command and control, electronic warfare, and kinetic or non-kinetic interceptors for fixed-site and mobile deployments.

Modern drone operations also increasingly face threats such as GPS spoofing, jamming, signal interception and communication disruption, Sudheer observes.

“Indian manufacturers are investing heavily in secure communications, encrypted data links, anti-jamming technologies, autonomous fail-safe capabilities, AI-enabled mission planning, and resilient navigation systems. The goal is not simply to assemble drones in India, but to design, test, manufacture, and continuously improve systems that can perform reliably in some of the world’s most demanding environments.”

Kumar also points to the importance of capability building. “We are doing it through training on our Indo ArcGIS platform, helping develop a skilled geospatial workforce that supports India’s vision of ‘Atmanirbhar Bharat’ and future-ready defence preparedness.”

Indigenisation holds particular significance in defence because it directly affects strategic autonomy, operational readiness and long-term national security, Anthony argues.

“Dependence on imports can create vulnerabilities in times of geopolitical uncertainty, supply-chain disruptions, or urgent operational requirements. Indigenous development ensures greater control over critical technologies, enables mission-specific

customisation, and reduces lifecycle and maintenance dependencies on external vendors.”

That is ultimately where the significance of India’s evolving defence drone ecosystem lies. The challenge is no longer simply to assemble or manufacture UAV platforms domestically, but to deepen indigenous capability across the technologies that determine how those platforms perform: flight controls, sensors, propulsion, communications, navigation, AI, geospatial intelligence, mission software and electronic warfare.

The challenge for indigenisation, however, lies deeper in the technology stack. India has built capabilities across airframes, software, guidance and navigation, system integration and mission technologies, but dependencies remain in areas such as high-performance flight controllers, specialised sensors, advanced propulsion systems, secure communication modules, semiconductors and batteries.

And this is where the stakes rise. As UAVs move from surveillance towards autonomous and contested operations, it is not enough for these machines to fly; they must remain dependable when the operating environment turns hostile. GPS spoofing, jamming, signal interception and communication disruption put secure communications, resilient navigation, anti-jamming technologies, autonomous fail-safe capabilities, testing infrastructure and dependable supply chains to the test.

How far India’s defence drones can ultimately fly will depend on how deep indigenisation can go. The real measure will be less about where a UAV is manufactured and more about who controls the technologies that allow it to sense, communicate, navigate, survive and complete its mission. That is where localisation stops being a manufacturing achievement and becomes a strategic capability.

Perhaps that also gives a different weight to Bhardwaj’s words to Garuda’s young creator in the movie: “You might have just won us the war, son!” 🙏

pratimah@cybermedia.co.in

AT&T's trillion-token play rewrites network intelligence

OTel 2.0 goes beyond industry-trained language model, signalling a new phase where operators seek control over models, infrastructure, data and inference costs.



BY THOMAS GEORGE

For the past two years, the telecom industry has discussed how artificial intelligence may transform networks. At AMD Advancing AI 2026 in San Francisco, this discussion shifted from ambition to operational reality.

AT&T announced that it has processed more than one trillion AI tokens using Azure-hosted models on AMD

Instinct GPUs. This experience, along with the data and economic insights obtained, helped develop OTel 2.0, the latest open-source telecommunications model from the Open Telco AI initiative.

The announcement matters because it brings together four elements operators have struggled to integrate: domain-specific intelligence, production-

At billions of tokens a day, choosing the right AI model is no longer a technical preference. It becomes a financial and operational discipline for telcos.

If operators can exploit network data only through one vendor's AI stack, they risk replacing traditional network lock-in with a new generation of AI lock-in.

scale infrastructure, open technology and disciplined inference economics. OTel 2.0 was trained on about 400 billion tokens selected from AT&T's AI corpus, along with telecommunications datasets and benchmarks contributed through the GSMA-led initiative.

It follows OTel 1.0, which reportedly crossed 18 million downloads, indicating demand for models that understand the language, standards and functional relationships of communications networks. However, the key development is not the model's size, but the emergence of a telco AI control plane.

For operators, the strategic question is no longer only whether to use generative AI. It is whether they can determine which model handles each task, where it operates, what infrastructure underpins it, how operational data is protected and how token costs are managed. Telecom needs its own intelligence layer.

WHY TELECOM NEEDS DOMAIN-TRAINED AI

Telecommunications presents a notably difficult environment for general-purpose AI. A network combines radio access, transport, core, cloud, customer platforms, billing, service assurance, cybersecurity, standards documentation and millions of interdependent operational events. A network alarm rarely explains itself. Its significance may depend on topology, traffic patterns, software versions, customer impact and events occurring across several layers.

General-purpose models can explain telecom concepts, yet are less reliable when interpreting live operational data, correlating alarms, recommending remedial actions or distinguishing between comparable incidents with different outcomes. Domain-trained models can be evaluated on tasks operators perform, such as comprehending technical standards, interpreting network data, supporting troubleshooting, automating workflows and enhancing resilience.

However, operators must use them carefully. A telecom-specific model is not a formal industry certification. It still requires validation, governance, security controls and human supervision before it can make consequential



IN BRIEF

- OTel 2.0 combines AT&T's AI corpus with telecom datasets and benchmarks to build intelligence tailored to communications network tasks.
- AT&T processes about 45 billion tokens daily, with more than 100 generative AI models reportedly deployed across production workloads.
- A cache-aware AI gateway routes requests to the best-suited model, helping AT&T claim reductions of up to 80 per cent in AI costs.
- Model selection is becoming a financial discipline as operators balance accuracy, latency, energy consumption and cost across AI workloads.
- Open-source models and mixed computing give operators more control while reducing dependence on a single cloud, model or accelerator.
- Indian operators will need to evaluate, route and govern models across languages, network functions, cloud infrastructure and the edge.

Data sovereignty is evolving into infrastructure sovereignty as operators seek greater control over the clouds, models and chipsets powering their AI workloads.

decisions within a live network. OTel 2.0 should therefore be seen not as an autonomous network brain, but as a key building block towards that goal.

AT&T's deployment offers strong evidence that enterprise AI in telecom has progressed beyond the experimental stage. The operator processes about 45 billion tokens daily, with monthly usage exceeding one trillion tokens and growing at a double-digit rate. More than 100 generative AI models are reportedly in production for customer care, fraud detection, network planning and internal enterprise functions.

Voice is one of its largest workloads. AT&T handles more than 300,000 customer calls every day, creating a continuous requirement for transcription, interpretation, routing and downstream action. This distinction between pilots and industrial AI is critical.

A proof of concept demonstrates that a model works. Production deployment must address latency, accuracy, integration, data protection, availability, observability and cost at enormous scale. AT&T is also moving from standalone copilots towards what it calls the "agentification" of complete workflows, including employee onboarding and cash forecasting.

This is where enterprise value will ultimately be created. Accelerating one stage may produce little benefit if the rest of the workflow stays manual, fragmented or approval-heavy. The larger opportunity lies in redesigning the process around machine-assisted execution.

THE 80% NUMBER THAT MATTERS

The headline milestone is one trillion tokens. The more consequential number may be AT&T's claimed reduction of up to 80% in AI costs. The operator uses a cache-aware AI gateway to route each request to the model best suited to the task. It can direct intricate reasoning to a high-capability model.

Jeremy Legg, Chief Technology Officer of AT&T, described the approach as "moneyballing" across models, chipsets and deployment options. That phrase captures an important shift. Telecom AI will not be economically

sustainable if every request is sent to the largest model running on the most expensive infrastructure. At billions of tokens a day, model selection becomes a financial discipline.

Operators will increasingly require an intelligent routing layer that evaluates accuracy, latency, energy consumption and cost. The winner will not necessarily be the model with the highest benchmark score. It will be the architecture that delivers the required business or network outcome at the lowest sustainable cost.

AT&T also says it achieved performance and accuracy similar to more expensive alternatives while post-training on AMD hardware. For AMD, this is a substantial production reference for its Instinct GPUs and ROCm software platform. For AT&T, it supports a wider objective: avoiding dependence on a single accelerator architecture.

SOVEREIGNTY NOW EXTENDS TO THE AI STACK

Legg's most important observation may have concerned sovereignty. "Your data is your fuel," he said, underlining the central role of proprietary information in building useful enterprise AI. But sovereignty now goes beyond where data is stored. It includes avoiding excessive dependence on one cloud provider, model family, chipset or development environment.

This is particularly relevant to telecom operators. Network telemetry, customer engagements, location patterns, fault histories and planning data are strategic assets. If operators can exploit those assets only through one vendor's model or infrastructure, they may replace traditional network lock-in with AI lock-in.

Open-source models do not eliminate dependencies, but they provide greater control over fine-tuning, deployment and evaluation. Mixed computing adds flexibility. Intelligent gateways allow workloads to move between open and proprietary models based on cost, risk and performance requirements. Data sovereignty is therefore becoming infrastructure sovereignty.

For Indian telecom operators, the argument carries special weight. India combines immense network

The model may not be the lasting advantage. The ability to select, route and govern multiple models dynamically could become the more durable capability.

scale, intense pricing pressure, multilingual customer engagements and a rising emphasis on trusted, indigenous and open digital infrastructure. A model trained for telecommunications, adapted to local operating conditions and deployable across cloud, private infrastructure and edge locations could become strategically important.

But the strongest lesson from AT&T is not simply to adopt OTel 2.0. It is to build the capability to evaluate, route and govern multiple models. Operators will need to know which model best suits a network-planning request, which can handle customer communications in different Indian languages, which should run at the edge and which workloads require a larger proprietary system.

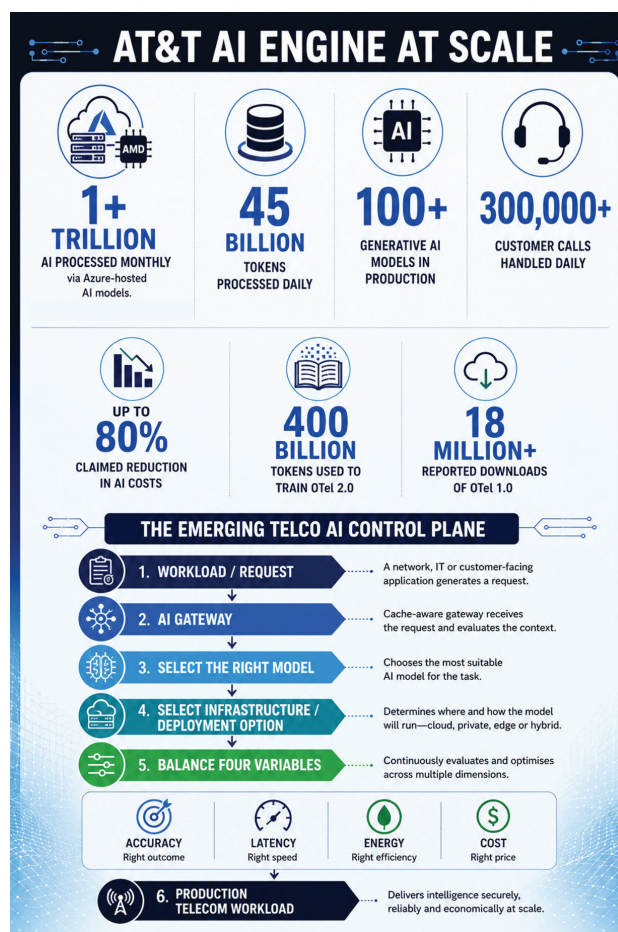
The model itself is only one part of the architecture. The ability to select and manage models dynamically may become the more durable competitive capability.

FROM ECOSYSTEM VISION TO OPERATING MODEL

Open Telco AI was launched at Mobile World Congress 2026 as an industry collaboration involving AMD, AT&T, the GSMA and other participants. Its ambition was to create shared models, datasets, benchmarks and development tools so that telecom AI would not be shaped entirely outside the industry.

OTel 2.0 is the clearest evidence to date that this idea is becoming deployable infrastructure. Its long-term value will depend on use across operators, languages, network contexts and regulatory regimes, and the model must show reliability beyond controlled benchmarks. At the same time, the ecosystem will need common approaches to evaluation, safety, protection and operational governance.

There is also a distinction between an open model and an open operating environment. Operators should assess whether these models can be transferred between different clouds and accelerators, integrated with existing network systems and upgraded without major redevelopment.



Nevertheless, the direction is significant. The telecom AI race will not be won by the operator that consumes the most tokens or deploys the largest model. It will be won by those that combine proprietary data, domain-trained intelligence, heterogeneous infrastructure and workflow redesign, while retaining control over costs.

AT&T's trillion-token milestone should be seen not as AI excess, but as evidence that inference has become an industrial-scale telecom workload. OTel 2.0 represents the next step: ensuring that the intelligence layer governing the network is not only powerful, but also open, adaptable and economically accountable. 🧠

thomasg@cybermedia.co.in

Hanwha, TTA plan AI tactical network

The partners will combine terrestrial 5G and satellite links to build an AI-enabled military communications network.

South Korea's Hanwha Systems has partnered with the Telecommunications Technology Association (TTA) to develop an artificial intelligence-enabled tactical communications system integrating terrestrial 5G networks with satellite connectivity, the company said.

The partners will develop military communications technology that uses AI to manage connections between terrestrial networks (TN) and non-terrestrial networks (NTN), allowing military units to maintain voice and data links as network availability and operational conditions change.

Commercial 5G technology will be adapted for military communications, while the system will be designed to

meet international standards for potential deployment in South Korea and overseas markets.

Hanwha Systems and TTA plan to incorporate commercial 5G and 6G technologies based on standards developed by the 3rd Generation Partnership Project (3GPP), along with NATO communications requirements, from the planning and design stages.

The companies will also conduct interoperability testing aimed at ensuring compatibility with allied communications networks, including those used by NATO members and European countries. The effort is intended to support overseas deployment of South Korean defence systems.

The partnership also covers joint development of Multi-Orbit Satellite System (MOSS) technology for military vehicles and other platforms.

MOSS will integrate mobile tactical 5G base stations and transmission equipment, satellite communications terminals, and command, control, communications, computers, and intelligence (C4I) mission equipment on a single platform.

The development is aimed at creating a multilayer tactical communications architecture capable of switching between terrestrial and satellite links and supporting connected military operations across different network environments.



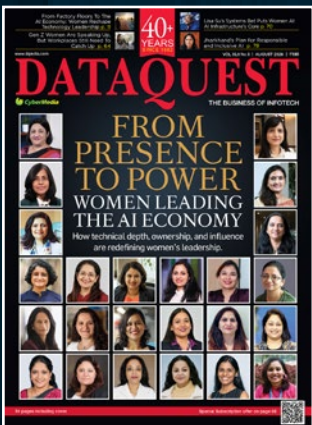
Find more smiles at NormanAndOzi.com



Find more smiles at NormanAndOzi.com

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

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



DATAQUEST
Enterprise &
Tech Leadership



PCQUEST
CIOs, Tech
Influencers & SMBs



VOICE&DATA
Telco & Digital
Infra Leaders



DQCHANNELS
ICT Partners &
Channel Decision Makers

OUR BESPOKE B2B MARKETING PROGRAMMES BUILD, ENGAGE AND SCALE COMMUNITIES

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

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

DELIVER INFLUENCE AND OUTCOMES WITH CYBERMEDIA

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

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

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

Partnerships & Advertising Enquiries

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



APEEJAY SCHOOL

Sector 15, Faridabad | Affiliated to CBSE | Estd. in 1972



Foundation For Lifelong Learning Starts Here



KEY HIGHLIGHTS



Value-based holistic education



State-of-the-art infrastructure



Safe & secure campus



Curriculum aligned with NEP 2020



Focus on experiential and competency-based learning



Spectacular competitive exam results with students placement in National and international Universities

AWARD & RECOGNITION

Ranked No.1 in 'Faridabad Leaders' category by Times School Survey 2025



For admission enquiry, please contact:

Apeejay School, Sector 15, Faridabad, Haryana

Admission Helpline Number:

+91-8826 074 074, +91 9599 105 614

Email: skool.ms.fbd@apj.edu

CONNECT WITH US



FACEBOOK



INSTAGRAM

