DISRUPTIVE TELECOMS

Enable. Innovate. Transform

WORLD REPORT January 2026

QUANTUM COUNTDOWN
Securing Telecoms

Nokia Using AI as a Powerful Accelerator for Transforming Networks

Arvind Khurana
Nokia India

How AI is Creating a Proactive Network That Predicts and Protects

Jitendra Singh Chaudhary
HFCL

TCCA –A Year in Review

Tero Pesonen
TCCA

What People Are Actually Doing with ChatGPT?

Dario Betti
Mobile Ecosystem Forum (MEF)

How Satellite Broadband Complements India's Mobile Networks

Konark Trivedi
Frog Innovation Ltd

An Initiative by TelecomDrive.com

TelecomDrive

THE EDUCATION PROJECT

A unique platform by TelecomDrive.com
to put spotlight on innovators – and next generation innovation driven by global universities, technology institutes and industry ecosystem

TelecomDrive.com

From the Editor

Zia Askari
Editor, TelecomDrive.com

10 Predictions for Telecoms in 2026:
Beyond Connectivity, Towards Cognitive Ecosystems

As we are embracing the year 2026, the telecommunications industry is shedding its skin. No longer merely the dutiful pipe for voice and data, it is morphing into the central nervous system of a hyper-digital, AI-soaked world. The trends of today—5G-Advanced, AI, cloudification—will be crystallised into new realities, reshaping not just how we communicate, but how societies and economies function. Here are ten predictions for the telecom landscape for the year 2026, viewed through a lens of strategic necessity and critical perspective.

1. The 'Composable Network' Becomes Strategic Imperative

The rigid, monolithic network architecture will be a relic. In its place: the Composable Network, a cloud-native, AI-driven fabric where functions are assembled dynamically based on real-time demand. Need ultra-low latency for a city's autonomous vehicle grid during rush hour? The network slices itself, allocates edge resources, and scales precisely. This isn't just efficiency; it's the core competitive differentiator. Telcos that fail to achieve this fluidity will be relegated to wholesale bit-haulers, while the innovators will become true platform providers.

2. AI-Native Operations: From Automation to Anticipation

Today's AIOps will evolve into AI-Native Operations. Predictive algorithms won't just flag a failing cell tower; they will simulate traffic impacts, re-route resources pre-emptively, and dispatch engineers before customers notice a blip. The network becomes self-healing and self-optimising. The perspective shift is profound: the primary role of thousands of engineers will transition from maintenance and monitoring to training, overseeing, and ethically governing these AI systems. The OPEX savings are immense, but the cultural and skillset transformation will be the real make-or-break challenge.

3. The Battle for the AI Agent's Soul (It Will Need a SIM Card)

This year our digital lives will be increasingly managed by proactive AI Agents—personal assistants that schedule meetings, book trips, and manage smart homes. My prediction: the most reliable, context-aware, and secure of these agents will be offered by your telecom provider. Why? Because the telco has a unique trifecta: real-time location data, network quality-of-service control, and billing relationships. An agent that can guarantee a seamless video call by prioritising network slices for you is more effective. This is telcos' golden chance to move up the value chain, but they must act before hyperscalers and device makers lock users in.

4. Sustainability as a Service (and a Billable Metric)

Network energy consumption will be untenable without radical innovation. Leading operators will not only run networks on 100% renewable energy but will also offer Sustainability-as-a-Service. Enterprises will buy connectivity with a guaranteed carbon-footprint metric per gigabyte, enabled by AI-driven energy optimisation across core and RAN. The perspective here is commercial, not just ethical: green connectivity will become a premium, enterprise-grade selling point, baked into SLAs.

5. Satellite-Cellular Hybridity: Seamless by Default

The hype around satellite direct-to-device will mature into quiet ubiquity. Apple, SpaceX, and the 3GPP's NTN (Non-Terrestrial Network) standards will ensure that every flagship smartphone will be a satellite hybrid. The "searching for signal" icon will vanish. This isn't about replacing terrestrial networks but creating a seamless, global safety net. For telcos, it means new wholesale partnerships and the erosion of their final monopoly: remote coverage.

6. The Rise of the 'Cyber-Immune' Network

As critical infrastructure, networks will be the number-one target for state-sponsored and criminal cyber-attacks. The response will be the Cyber-Immune Network, leveraging AI not just for defence but for active deception. Networks will deploy millions of AI-generated honeypots and dynamically reconfiguring attack surfaces. The philosophical shift: from building higher walls to creating an ecosystem where the network's very "immune system" identifies and neutralises threats autonomously.

7. API Revenue Surpasses Traditional Wholesale

The telco business model will see a pivotal shift. While consumer ARPU stagnates, revenue from Network APIs exposed to enterprises and developers will skyrocket. It will outstrip traditional wholesale. Developers will pay to inject latency sensitivity into their cloud gaming apps or guarantee uplink speed for their live-streaming service. This is the true monetisation of 5G-Advanced and early 6G R&D, turning network capabilities into a developer-friendly platform.

8. The Digital Twin Divide

Enterprises will run mission-critical operations on real-time digital twins of factories, ports, and supply chains. The fidelity and utility of these twins will be directly determined by the underlying telecoms infrastructure. The "Digital Twin Divide" will emerge: companies with access to high-capacity, ultra-low-latency, and reliably synced networks will have twins that are predictive mirrors. Those without will have laggy, historical models. Telcos become purveyors of reality, not just connectivity.

9. Regulatory Revolt Over Data Dominance

The immense data trove telcos sit on—location, traffic patterns, device behaviour—will become a regulatory battleground. This year, we will see the first major "Telco Data Trust" rulings, forcing operators to anonymise and pool certain data for public good (urban planning, disaster response) while severely restricting its use for commercial hyper-targeting. The perspective is cautionary: telcos must proactively shape this narrative with transparency, or face brutal, innovation-stifling mandates.

10. The Quiet Consolidation: From Competitors to Co-Creators

The capital demands of continuous network evolution will force a final prediction: the era of fierce retail competition between telcos in mature markets will give way to strategic co-creation. We will see deeper, operational sharing of 6G R&D costs, AI training platforms, and even combined edge infrastructure. They will compete on service layers and AI agents, while co-owning the astronomically expensive underlying fabric. It's a pragmatic, necessary retreat from duplicate infrastructure that will redefine market landscapes.

CONTENT

Quantum Countdown

Securing Telecoms Against Tomorrow's Threat

In the high-stakes arena of global telecommunications, a silent, transformative race is underway—one that will redefine the very foundations of trust, privacy, and security in the digital age. The prize?The integrity of every financial transaction, government communication, piece of critical infrastructure data, and private message that flows across global networks.The challenger? The nascent but rapidly advancing quantum computer, capable of rendering today's strongest encryption obsolete. The response?A proactive, strategic embrace of quantum-safe technologies, positioning telecom operators not as passive victims of a future threat, but as the architects of a next-generation, resilient digital ecosystem.

This is the Quantum Countdown, and for forward-thinking telecom leaders, it is the ultimate convergence of risk mitigation and value creation.

Part 1: The Looming Storm – Understanding the Quantum Threat

To appreciate the seismic shift, one must first understand the vulnerability. Modern public-key cryptography—the workhorse securing internet protocols (TLS/SSL), digital signatures, and key exchanges—relies on complex mathematical problems (like integer factorization and discrete logarithms) that are prohibitively difficult for

classical computers to solve. Quantum computers, leveraging the principles of superposition and entanglement, promise to solve these problems exponentially faster.

The threat is not science fiction. While a cryptographically relevant quantum computer (CRQC) is estimated to be 5-15 years away, the risk is present today. Adversaries are already engaging in "harvest now, decrypt later" attacks, where they intercept and store encrypted data flows, waiting for the day quantum capabilities allow them to unlock it. For telecoms, the custodians of this data river, this means the sensitive communications, intellectual property, and state secrets flowing through their networks today could be exposed in the future. The potential fallout is catastrophic: systemic financial fraud, collapse of public trust, national security breaches, and massive regulatory and liability exposure.

The countdown, therefore, is not to the arrival of the quantum computer, but to the moment when quantum-vulnerable encryption must be eradicated from global systems. The timeline for this migration is measured in years, not decades, given the complexity of upgrading legacy hardware, software, and standards across sprawling, multi-vendor networks.

Part 2: From Vulnerability to Value: The Telecom Quantum Imperative

For telecom operators, the quantum threat is not merely a technical IT challenge; it is a fundamental business, strategic, and trust imperative. The response is being framed across three critical dimensions:

1. ***The Trust Imperative:*** A telecom's brand is built on reliability and security. Being quantum-prepared is the next benchmark of customer assurance. Enterprise clients, particularly in finance, healthcare, and government, will increasingly demand quantum-resilient service level agreements (SLAs). Operators who can offer verified quantum-safe channels will secure premium contracts and become the partners of choice for the digital sovereignty strategies of nations.
2. ***The Regulatory and Compliance Imperative:*** Governments and standards bodies are moving swiftly. The U.S. National Institute of Standards and Technology (NIST) has finalized its first set of Post-Quantum Cryptography (PQC) algorithms. The National Security Agency (NSA), European Telecommunications Standards Institute (ETSI), and others have issued migration mandates. Telecoms, as regulated critical infrastructure, must demonstrate proactive roadmaps to compliance or face severe penalties and operational restrictions.
3. ***The Innovation and Revenue Imperative:*** This transition is a catalyst for network modernization and service differentiation. Quantum technology isn't just about defense; it presents two key offensive opportunities:

* ***Quantum Key Distribution (QKD):*** Leveraging quantum mechanics (the principle that observing a quantum state alters it) to generate and distribute encryption keys that are provably secure against any computational attack. This enables the creation of ultra-secure, quantum-safe tunnels for critical data.
* ***Quantum-Secured Networks as a Service (QSNaaS):*** Offering quantum-enhanced security as a billable, managed service to enterprise and government clients. This includes quantum-encrypted dedicated lines, secure access service edge (SASE) with PQC, and cloud security integrations.

The narrative is clear: The operator that masters the quantum transition evolves from a "dumb pipe" to an Intelligent Trust Fabric, an indispensable and value-added guardian of the digital economy.

Part 3: The Quantum Toolkit: PQC, QKD, and Hybrid Architectures

Telecoms are deploying a multi-layered arsenal to win the countdown. The strategy is pragmatic, focusing on coexistence and gradual migration.

Post-Quantum Cryptography (PQC): The Software Foundation

PQC involves replacing current public-key algorithms with NIST-standardized quantum-resistant ones. This is primarily a software and protocol upgrade, affecting network elements, authentication systems, and certificate authorities. The advantage is deployability on existing hardware. Major pilots are underway integrating PQC into 4G/5G core signaling, IoT device authentication, and software-defined networking (SDN) controllers. The challenge lies in computational overhead and the need for comprehensive testing to avoid new vulnerabilities.

Quantum Key Distribution (QKD): The Hardware-Based Shield

QKD uses photons transmitted over fiber-optic networks to generate shared, random secret keys. Any eavesdropping attempt introduces detectable anomalies. This makes it a powerful solution for point-to-point high-security links, like those between data centers, government hubs, or financial trading floors. Deployments are already live in several countries. The limitations are range (without trusted nodes or quantum repeaters)

and the need for dedicated fiber or specialized satellite links for free-space QKD.

The Winning Strategy: Hybrid Solutions

Recognizing that no single solution is a silver bullet, telecoms are pioneering hybrid quantum-safe networks. These systems run PQC and QKD (or classical key distribution) in parallel. For example, a key might be exchanged using both a PQC algorithm and a QKD channel, with the system falling back to the PQC-secured key if the QKD link is interrupted. This creates defense-in-depth, ensures interoperability during the long transition, and future-proofs investments. It is the pragmatic backbone of the migration strategy.

Part 4: Case Studies in Quantum Resilience – The Global Vanguard

The transition is already in progress. Leading operators are providing a blueprint for the industry:

SK Telecom (South Korea): A global leader, SKT has launched a commercial Quantum-Secured Network-as-a-Service (QSNaaS). They provide end-to-end quantum-safe solutions combining PQC and QKD to enterprise clients, securing connections from the device to the data center. They are also integrating quantum randomness into their 5G core for stronger authentication.

British Telecom (BT) & Toshiba (UK): Operating the world's first commercial QKD network-as-a-service, the Quantum Secure Metro Network in London. It provides a quantum-secured backbone for financial institutions and critical national infrastructure, with keys generated by QKD and delivered via APIs to encrypt customer data.

Orange (France): Actively testing PQC across its networks and participating in the French government's national quantum communication strategy. They focus on the integration challenges and performance impact of PQC on live telecom systems.

Singtel (Singapore): Partnering with government agencies to trial quantum-safe technologies to secure Singapore's status as a digital hub. They are exploring both terrestrial QKD and satellite-based quantum key distribution for broader coverage.

These pioneers demonstrate that the technology is viable, commercial, and driven by clear customer demand from security-conscious sectors.

Part 5: The Deployment Hurdles: Navigating the Quantum Maze

The path is fraught with complexity. Key challenges include:

Interoperability: Ensuring new PQC algorithms and QKD systems from different vendors work seamlessly across multi-vendor, multi-generational networks.

Performance & Scale: PQC algorithms can have larger key sizes and higher processing demands. Scaling QKD beyond metropolitan areas requires quantum repeaters (still in R&D) or trusted node networks, which have their own security considerations.

Legacy System Integration: Millions of existing devices (IoT sensors, older routers) may never support PQC. Telecoms must design

network segmentation and encryption gateways to protect these vulnerable endpoints.

Talent & Expertise: A severe shortage of quantum-aware cryptographers and network architects exists. Building this expertise is a critical strategic investment.

Cost & ROI: The business case must balance upfront capex on QKD hardware and software upgrades against the risk cost of a future breach and the revenue potential of new services.

Part 6: The Strategic Roadmap: A Call to Action for Telecom Leadership

The quantum countdown cannot be managed by the CISO's office alone. It requires C-suite ownership and a cross-functional program. The roadmap must be phased:

Inventory & Assess (Now): Conduct a crypto-agility audit. Catalog all systems using cryptography, prioritize assets based on sensitivity and vulnerability, and assess vendor PQC/QKD roadmaps.

Experiment & Pilot (0-2 Years): Establish lab environments. Run controlled pilots for PQC in non-critical systems and test point-to-point QKD links with key enterprise clients. Engage with standards bodies and industry consortia.

Plan & Design (1-3 Years): Develop a comprehensive migration architecture. Decide on hybrid models, select primary vendors, and create a detailed crypto-agility implementation plan. Begin recruiting and training quantum talent.

Gradual Migration (3-10 Years): Start deploying PQC in new equipment purchases and software updates. Begin rolling out quantum-safe services (QSNaaS) in high-value metropolitan corridors. Work with enterprises on their migration.

Full Integration & Evolution (10+ Years): Achieve full crypto-agility across the network core. Integrate emerging technologies like quantum repeaters and quantum random number generators (QRNG) ubiquitously. Evolve service offerings continuously.

Securing the Future, Today

The Quantum Countdown is not a doomsday clock, but an innovation timer. For the telecommunications industry, it represents a pivotal moment of responsibility and opportunity. The operators who act decisively will not only shield the global digital ecosystem from a generational threat but will also redefine their own value proposition.

They will transform their networks from infrastructure into Certified Quantum-Resilient Platforms. They will move from selling bandwidth to selling verifiable trust. In doing so, they will secure far more than data; they will secure their own relevance, profitability, and leadership in the post-quantum era. The race is on. The time for strategic investment, collaboration, and action is now. The networks we secure today will define the trustworthiness of tomorrow's world.

Driving Critical Communications in the AI Era

From Reactive Response to Intelligent Resilience

The critical communications sector—encompassing public safety, emergency services, disaster response, and essential utility networks—stands at the precipice of its most profound transformation in decades. The driving force is Artificial Intelligence (AI), which is rapidly evolving from a speculative tool to an operational imperative. This is not merely about incremental efficiency gains; it is a fundamental shift from reactive, voice-centric dispatch to proactive, data-driven intelligence ecosystems.

In an era of escalating climate events, complex urban threats, and soaring public expectations, AI is becoming the central nervous system for mission-critical operations, promising to enhance situational awareness, accelerate decision-making, and save lives. This analysis explores the fast-emerging AI landscape within critical communications, supported by global case studies, and examines the strategic calculus for leaders in this high-stakes domain.

The Convergence of Necessity and Innovation

Traditional critical communications, anchored by robust standards like TETRA, P25, and now 3GPP Mission-Critical Services (MCX), have mastered reliability and interoperability. However, the "big data" generated by these networks—voice calls, location data, sensor inputs from first responders, and video from bodycams and drones—has often been a latent asset, under-analyzed in real-time. AI unlocks this data's potential. The convergence is fueled by three pressures:

Operational Complexity: Incidents are more multifaceted, requiring coordination across more agencies and data streams.

Data Overload: Command centers are inundated with information,

creating cognitive burden and risk of oversight.

Societal Demand: Citizens expect the speed and precision of digital services in emergency response.

AI addresses these pressures not by replacing human judgment, but by augmenting it, creating what industry leaders now term "Intelligent Resilience."

Key AI Applications Reshaping the Domain

The integration is happening across the operational value chain:

Intelligent Incident Detection & Triage: AI algorithms are now the first line of analysis for emergency calls. By processing natural language in real-time, AI-powered speech analytics can detect stress, identify keywords, and cross-reference location data to predict incident severity and required resources before the call-taker has fully logged it. This shaves critical seconds off response time and improves dispatch accuracy.

Predictive Policing & Resource Allocation: Moving beyond historical controversy, next-generation predictive analytics use anonymized, aggregated data (like crime reports, weather patterns, event schedules, and social trends) to model risk hotspots. AI does not dictate patrols but provides dynamic resource recommendation engines, enabling commanders to optimally position personnel and assets for preventative presence and faster response.

Real-Time Situational Awareness & Sensor Fusion: This is perhaps the most transformative application. AI acts as a force multiplier for human eyes. It can:

Analyze live video feeds from drones, bodycams, and city CCTV to automatically identify anomalies (e.g., an unattended bag, a person collapsed in a crowd, the spread of a fire).

Perform multimodal sensor fusion, correlating acoustic gunshot detection, thermal imaging, and social media alerts to create a single, verified incident view on a commander's dashboard.

Translate and transcribe radio communications in real-time, creating searchable logs and breaking down language barriers in multi-agency responses.

Logistics & Operational Optimization: AI optimizes routing for emergency vehicles using real-time traffic, weather, and road closure data. It can predict equipment failure in critical infrastructure (like radio towers or utility grids) and automate inventory management for essential supplies during prolonged crises.

Global Case Studies: From Pilot to Production

Case Study 1: London Metropolitan Police (UK) – AI-Driven Violence Prediction

Facing rising knife crime and complex urban challenges, the Met has deployed an AI-powered data analytics platform. The system aggregates and analyzes millions of data points from crime reports, intelligence logs, social indicators, and weather data. It generates daily "Violence Harm Risk Assessment" maps, highlighting micro-locations at highest risk of serious violence.

This is not automated deployment; it provides local policing teams with intelligence-led, granular insights to guide targeted patrols, community engagement, and preventative social services interventions. Early results indicate a measurable impact on resource allocation efficiency and a contribution to reductions in violent crime in pilot areas.

Case Study 2: Copenhagen Fire Department (Denmark) – AI for Emergency Call Processing

Copenhagen's emergency services center has integrated an AI solution from Corti into its 1-1-2 call handling. The AI listens in real-time to cardiac arrest calls. By analyzing speech patterns, background sounds, and the conversation between caller and operator, it can identify signs of cardiac arrest with a speed and accuracy that matches or exceeds human operators.

The system provides real-time prompts to the call-taker, ensuring critical questions are asked and CPR instructions are begun immediately. The result: A documented significant increase in the recognition rate of out-of-hospital cardiac arrests, directly leading to more lives saved through faster dispatching of resuscitation teams.

Case Study 3: Tokyo – AI-Enhanced Disaster Response & Evacuation

In a megacity perpetually at risk of

earthquakes, Tokyo's authorities use AI for large-scale disaster simulation and real-time response. AI models simulate earthquake impacts across different magnitudes and epicenters, predicting building damage, fire spread, and road blockages.

During an actual event, AI rapidly analyzes incoming data from thousands of seismic sensors, social media (for crowd-sourced info), and CCTV to update damage assessments in real-time. This directs emergency units to the worst-hit areas and optimizes the issuance of targeted evacuation advisories to citizens' smartphones, preventing gridlock and streamlining the flow of both people and aid.

Strategic Imperatives and Cautions

The integration of AI into critical communications is not without its strategic challenges and ethical considerations:

The Non-Negotiable Foundation: Network Resilience: AI is only as good as its data feed. Its deployment must be built upon ultra-reliable, secure, and high-bandwidth networks. This reinforces the business case for dedicated critical broadband networks (like FirstNet in the USA or ESN in the UK) and hybrid LTE/TETRA solutions, ensuring AI applications function in congested or compromised environments.

Data Sovereignty & Ethical Governance: The use of AI, particularly in predictive policing and video analytics, raises profound questions about bias, privacy, and accountability. Agencies must implement rigorous AI governance frameworks—ensuring algorithmic transparency, auditing for bias, maintaining human-in-the-loop for critical decisions, and securing public trust through clear communication on data use.

Investment & Skill Shift: The transition requires significant investment in cloud/edge compute infrastructure, data platforms, and vendor partnerships. Equally critical is the upskilling of personnel from radio operators to data-literate controllers and commanders who can interpret AI insights effectively.

Conclusion: The Augmented Commander

The era of AI in critical communications is not on the horizon; it is here. The global case studies demonstrate a clear trajectory from experimental pilots to core, life-saving operational tools. For network operators, technology vendors, and public safety agencies, the mandate is clear: to strategically harness AI as a force multiplier that enhances human expertise and operational resilience.

The future of critical communications lies in the partnership between human experience and machine intelligence—the Augmented Commander. This professional, equipped with real-time, AI-processed intelligence, can make faster, more informed decisions that protect communities and responders alike. Organizations that proactively navigate the ethical, technical, and training challenges of this integration will not only future-proof their operations but will define a new global standard for what it means to be resilient in the 21st century. The business of saving lives is becoming smarter, and AI is its most powerful new tool.

Nokia Using AI as a Powerful Accelerator for Transforming Networks

At a time when AI is fundamentally transforming networks from static, hardware-centric infrastructures into dynamic, self-optimizing systems – global telecoms major Nokia is using AI as a powerful accelerator for transforming networks into intelligent and automated systems. The company's unique approach brings together traditional ML, causal AI, and Multi-Agent Reinforcement Learning (MARL) to enable real-time sensing and decisioning.

Arvind Khurana - Regional VP & Country Head for Cloud and Network Services, Nokia India speaks with Zia Askari from TelecomDrive.com about the fast emergence of AI and how Nokia is helping its customers with AI-driven tools in terms of transforming networks and elevating experience.

What does a truly AI-native network look like in practice, and how close is the industry to achieving autonomous network operations at scale?

A truly AI-native network reflects the industry's shift toward the era of AI-native mobility, where AI-driven network designs, advanced algorithms, and trusted security frameworks are built into the network from the ground up. This approach enables networks to become more adaptive, autonomous, and seamless to the user.

At Nokia, one of our focuses is on autonomous networking, supported by a programmable, cloud-native core, zero-touch automation, and API-led monetization to help telecommunications service providers scale innovation efficiently. From a readiness perspective, many of the foundational elements, such as cloud-native core network functions, orchestration systems, AI models, and observability frameworks, are already production-ready or being trialled at scale.

While progressing toward TM Forum Levels 3 - 4 autonomy remains a journey that depends on richer data, stronger standards, and wider ecosystem adoption, the critical technical building blocks required to achieve autonomous network operations are firmly in place.

How is Nokia using AI and Generative AI to move beyond traditional automation and improve performance, operational efficiency, and customer experience?

At Nokia, we view AI, including Generative AI (GenAI), as a powerful accelerator for transforming networks into intelligent and automated systems. Our approach brings together traditional ML, causal AI, and Multi-Agent Reinforcement Learning (MARL) to enable real-time sensing and decisioning, while GenAI is applied to manage unstructured data, summarise insights, support telco assistants, and accelerate complex, non-real-time automation tasks.

In practical terms, this delivers faster fault detection and resolution, more accurate capacity forecasts, automated service orchestration, and AI-assisted customer and security workflows. Together, these capabilities help reduce mean-time-to-repair, enhance operational efficiency, and improve the overall customer experience.

As 5G deployments mature globally, where do you see the most compelling revenue

opportunities for telecom service providers beyond basic connectivity?

As 5G deployments continue to mature, the most compelling revenue opportunities beyond basic connectivity are emerging around network-exposed platform services, including APIs / Network as Code, that allow developers to directly consume network capabilities. Additional upside comes from enterprise slices tailored to vertical needs, such as industrial automation and logistics, as well as edge-native applications spanning AR/VR and real-time analytics. Cybersecurity services also represent significant monetization potential.

The differentiator lies in packaging network capabilities as modular digital services that developers can easily consume. This shift enables telecommunications service providers to move from infrastructure-led models to recurring, higher-value digital services.

The API economy is increasingly seen as a catalyst for telecom innovation. How do network APIs change the role of CSPs in the digital services ecosystem? What role do open, programmable network architectures play in accelerating innovation, and how can operators safely expose network capabilities through APIs?

Network APIs simplify how advanced network functions, such as QoS adjustments, slice creation, location, edge placement, and telemetry, are consumed by abstracting them into straightforward software calls. This allows application developers and system integrators to innovate quickly without requiring deep telco expertise. When programmable network capabilities are exposed through developer portals and marketplaces, networks evolve into platforms where third parties can create, deploy, and monetize digital services, shifting telecommunications service providers from connectivity pipe providers to platform providers within the broader digital services ecosystem.

To support this transition, we have developed a Network as Code approach through a developer portal and platform that presents network capabilities as easily consumable resources. This accelerates developer onboarding, aligns with industry standards such as GSMA Open Gateway / CAMARA, and enables telecommunications service providers to launch APIs and service marketplaces efficiently. Built on a cloud-native architecture, with service meshes and API-enabled automation tools, the platform allows service providers to safely expose network capabilities while maintaining control, security, and assured performance.

With the expansion of AI-driven and cloud-native networks, how are cybersecurity priorities evolving for telecom operators today? How is Nokia embedding AI-driven threat detection and cyber resilience within its network offerings?

As networks become increasingly AI-driven and cloud-native, cybersecurity priorities for telecommunications service providers are expanding beyond traditional perimeter defenses. Today, the emphasis is on end-to-end visibility and telemetry, threat detection tailored to telco protocols, and strong identity and access controls across cloud-native components. These service providers are also focusing on supply-chain and OSS/BSS hardening, along with readiness for more advanced threat scenarios, including AI-assisted attacks. In parallel, resilience planning, segmented architectures, and robust incident response capabilities are critical to maintaining network integrity.

Within our network offerings, we embed AI and XDR capabilities directly into the security portfolio, including solutions such as NetGuard Cybersecurity Dome integrated with telco-centric GenAI assistants. These capabilities help aggregate signals, reduce false positives, and accelerate triage and remediation. By using AI to correlate cross-domain telemetry, prioritize incidents, and recommend or automate containment actions, we significantly enhance both threat detection quality and operational response times, strengthening overall cyber resilience.

Looking ahead, how will the convergence of AI, 5G, and cloud technologies reshape the telecom ecosystem and business models over the next few years?

Over the next few years, as AI extends into autonomous systems, robotics, industrial automation, and augmented reality, networks will continue to evolve toward delivering ubiquitous, trusted, and adaptive connectivity that increasingly becomes invisible to the user. This implies connectivity that is automatically provisioned, optimized in real time, and able to support new workloads with the required bandwidth, latency, and security.

The growing convergence of AI, 5G, and cloud will also reshape the telecom ecosystem by moving it away from connectivity-centric models toward platform and data-centric ecosystems. 5G and distributed cloud will provide highly reliable connectivity and local compute, while AI converts network and application telemetry into actionable insights and automation. Through open APIs, developers, enterprises, and partners will be linked into new value chains, enabling real-time industries such as autonomous logistics, remote healthcare, and advanced AR, and redefining how telecommunications service providers monetize networks.

How AI is Creating a Proactive Network That Predicts and Protects

By Jitendra Singh Chaudhary, Executive President – Communications, HFCL

Enterprise networks are no longer just pipes that move data from one point to another. Today, they function as the digital nervous system of modern business, supporting cloud platforms, digital payments, IoT deployments, remote work, and real-time customer experiences. As organisations adopt cloud-native architectures, 5G, edge computing, and distributed applications, network complexity has increased dramatically.

What has not evolved at the same pace is how many networks are managed. Manual configurations, static automation scripts, and reactive troubleshooting were designed for a far simpler environment. In a world where downtime impacts revenue and user experience defines competitiveness, waiting for something to break before fixing it is no longer sustainable.

This is where AI in networking moves beyond hype and becomes a business necessity. AI introduces predictive intelligence and adaptive learning into network operations, enabling networks to anticipate issues rather than simply respond to them. For IT leaders, the real question today is not whether AI belongs in the network, but how quickly it can be integrated to future-proof infrastructure.

Moving Beyond Traditional Automation

Most enterprises already rely on automation to handle repetitive tasks such as provisioning or configuration updates. That is an important first step, but automation has clear limitations. It follows predefined rules and cannot adapt when conditions change in unexpected ways.

AI represents a more fundamental shift. Instead of executing static instructions, AI-driven networks continuously learn from telemetry data, traffic patterns, system logs, and user behaviour. They identify trends, predict outcomes, and make intelligent decisions in real time.

Put simply, automation reacts when congestion occurs. AI anticipates congestion before users feel the impact and adjusts traffic proactively. Instead of investigating outages after applications fail, AI spots early warning signals and triggers preventive action. The network evolves from a static system into an adaptive platform that constantly optimises itself.

Predictive Intelligence That Scales With the Business

One of the most powerful benefits of AI in networking is operational intelligence at scale. Modern networks generate enormous volumes of data across devices, applications, and environments. Human teams cannot realistically analyse this information in real time.

AI models excel in this space. They analyse millions of data points simultaneously to identify anomalies, performance degradation, and hidden dependencies. This significantly reduces Mean Time to Identify and Mean Time to Repair, often turning hours of troubleshooting into minutes.

Predictive maintenance is a practical example. By analysing trends in latency, packet loss, hardware telemetry, and power usage, AI can forecast failures before they occur. This allows IT teams to plan

maintenance proactively rather than responding to outages under pressure. The result is higher uptime, lower operational costs, and a more stable digital environment.

Smarter Traffic Management for Modern Applications

As applications become more latency-sensitive, static traffic engineering is no longer effective. Video collaboration, real-time analytics, and digital transactions all require consistent performance.

AI-powered traffic management dynamically optimises routing based on real-time network conditions. Using advanced analytics and learning models, the network continuously evaluates traffic flows and application performance. When congestion is predicted, traffic is rerouted automatically to maintain service quality.

This capability is particularly valuable in hybrid and multi-cloud environments, where traffic patterns change constantly. Instead of over-provisioning capacity just in case, organisations can use existing resources more efficiently while still delivering a superior user experience.

Security That Learns and Adapts

Network security is another area where AI brings a meaningful shift. Traditional security tools rely heavily on known signatures and predefined rules. While effective against familiar threats, they struggle with zero-day attacks and subtle lateral movement within the network.

AI-driven security systems take a behavioural approach. By learning what "normal" looks like for users, devices, and applications, AI can detect deviations that may indicate a threat. These anomalies are flagged in real time, enabling faster investigation and response.

In many cases, AI can automatically isolate compromised devices or reroute sensitive traffic, reducing response times from hours to seconds and limiting potential damage.

From Configuration to Intent-Based Networking

One of the most transformative changes enabled by AI is intent-based networking. Instead of configuring devices individually, IT teams define high-level business intent, such as prioritising customer-facing applications or enforcing consistent security policies across locations.

AI translates this intent into network configurations, continuously verifies compliance, and adjusts settings as conditions change. Closed-loop automation allows the network to detect issues, decide on corrective actions, and implement changes without human intervention.

This approach reduces configuration errors, accelerates service deployment, and ensures consistency across increasingly complex, multi-vendor environments.

Addressing the Reality of Adoption

Despite its promise, adopting AI in networking comes with challenges. Data quality remains critical, as AI models depend on accurate and consistent telemetry. Integration with legacy infrastructure and organisational readiness can also slow progress.

A phased approach is often the most effective path forward. Organisations can start with high-impact use cases such as predictive maintenance or anomaly detection, invest in skills development, and establish governance frameworks that balance autonomy with oversight. Explainable AI and human-in-the-loop controls are essential for building trust and accountability.

The Path to Autonomous Networks

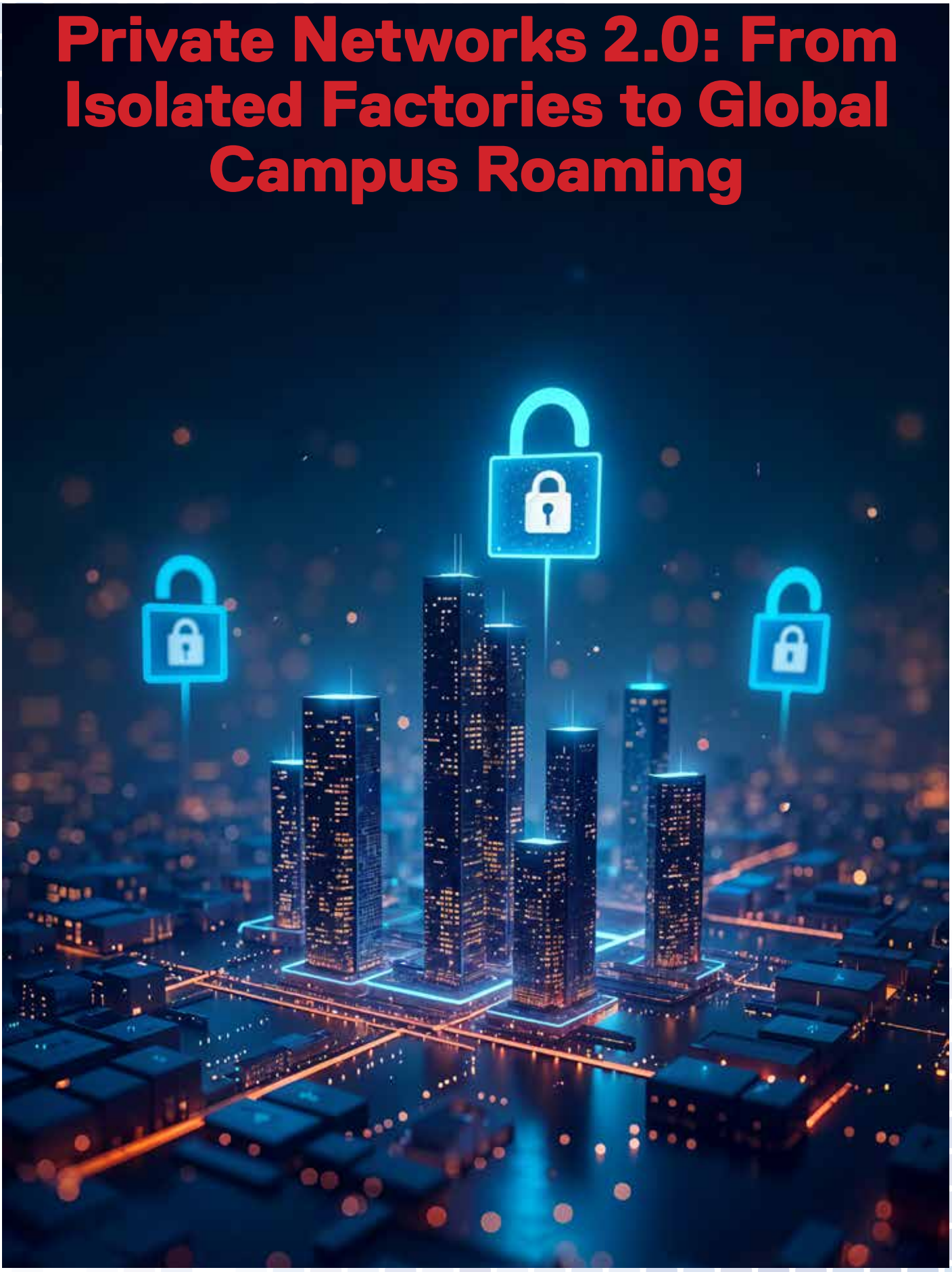
The future of networking is autonomous. Networks will increasingly predict failures, optimise themselves, and heal without manual intervention. Generative AI will simplify operations by enabling natural language-based configuration and policy management. Network digital twins will allow teams to simulate changes and predict outcomes before deploying them in live environments.

The question for enterprises is no longer whether AI will reshape networking, but how prepared they are to embrace that shift. Organisations that move early will gain networks that do more than connect systems. They will build intelligent, adaptive foundations that drive agility, resilience, and long-term competitive advantage.

Jitendra Singh Chaudhary

Mr. Chaudhary is responsible for the Communications Business Unit spanning multiple verticals of the company - Public, Defence, and Railway Communications. He led a successful launch of a new product brand IO with a range of Access solutions. A PGDM holder from IIM, Calcutta and B.Tech from MMM Engineering College, Gorakhpur, Mr. Chaudhary has rich experience in managing and leading businesses, including the responsibility for P&L of respective Business Units, Sales, Marketing, Business Development, and Product Management across multiple geographies, majorly in the Asia Pacific Region. Prior to joining HFCL, he was working with DragonWave HFCL India Private Limited as CEO. In the past, he was associated with organizations such as SIAE Microelectronics, Aviat Networks, Harris Stratex Networks and Siemens.

Private Networks 2.0: From Isolated Factories to Global Campus Roaming



The first wave of private cellular networks (4G/5G) delivered a revolution in reliability, security, and control for enterprise environments—transforming factories, ports, and campuses into islands of ultra-optimized connectivity. Yet, this very strength—their isolation—has become a limiting factor in an interconnected global economy.

Enter Private Networks 2.0, the next evolutionary leap. This paradigm shifts from standalone, siloed deployments to a federated, globally interconnected ecosystem of private networks. It enables what was once unthinkable: a certified autonomous vehicle in Stuttgart can roll off the production line, maintain its secure, low-latency connection across a logistics hub in Rotterdam, and operate seamlessly inside a partner's assembly facility in Nagoya—all under a unified digital identity and security policy.

This is not merely a technical upgrade; it is a foundational shift enabling the fluid, secure movement of data, devices, and intelligence across organizational and geographic boundaries.

The Limitation of Isolation: The 1.0 Ceiling

Private Networks 1.0 solved critical pain points: replacing unreliable Wi-Fi for mission-critical automation, ensuring data sovereignty within the factory walls, and enabling precise network slicing for differentiated applications (e.g., separating AGV control from AR maintenance guides). However, they created "walled gardens." This fragmentation poses severe business constraints:

Broken Processes: Global supply chains and distributed manufacturing require continuous data and control. A device crossing from a private network to public cellular or a partner's network experiences a hard break—a session drop, policy change, and security re-authentication.

Operational Inefficiency: Managing thousands of discrete private networks globally is a scalability nightmare for multinationals, with inconsistent security postures and manual, site-by-site provisioning.

Inhibited Innovation: Collaborative robotics, global telepresence for experts, and distributed digital twins are stifled when connectivity and security models cannot extend beyond a single site.

The Architecture of Interconnection: Building the Federation

Private Networks 2.0 solves this through a layered architectural evolution, built on emerging standards and strategic partnerships:

The Foundation: Standardized, Cloud-Native Core Networks: The shift begins with the adoption of 3GPP-standardized, cloud-native 5G Standalone (SA) cores for private deployments. This provides the essential DNA for interoperability. Each private network becomes a peer in a potential global system, speaking the same language.

The Enabling Fabric: Multi-Domain Network Slicing: This is the core technical breakthrough. A global end-to-end network slice is created, stitching together slices from multiple private networks and, where necessary, secure segments of public mobile operator networks. This slice acts as a dedicated, virtualized "express lane" across the federated environment. The device's session and policy context travel within this lane.

The Orchestration Brain: Cross-Domain Slice Orchestrators: Orchestration moves from a single-site tool to a federated, hierarchical system. A global orchestrator (managed by the enterprise, a systems integrator, or a consortium) negotiates with local orchestrators at each private network site. It provisions the global slice, ensuring resource availability and policy alignment from end-to-end. Key players here include hyperscalers (AWS Private 5G, Microsoft Azure Private MEC) and telecom vendors evolving their orchestration platforms.

The Trust and Policy Layer: Unified Identity & Security: A device or user has a single, cryptographically strong identity (e.g., based on SIM or certificate), authenticated via a global home network core or a trusted neutral host. Security policies—defining what data the device can access, what commands it can receive—are centrally defined and dynamically enforced at each network edge via SEAL (Secure Edge Access Layer) or similar frameworks. This ensures "follow-me" security that is consistent, regardless of physical location.

The Business Enabler: Federation Agreements & Neutral Hosts: The model requires commercial and legal frameworks—Federation Agreements—that define service level expectations, liability, and billing between enterprises or between an enterprise and multiple telcos. Emerging specialized neutral hosts are positioning themselves as global intermediaries, operating the federation platform and simplifying the commercial complexity.

Global Case Studies in Action

Siemens & Bosch: The Federated Smart Factory: Competing as vendors but collaborating as users, these manufacturing giants are

piloting a federation for their own global operations and ecosystem partners. A Bosch assembly robot's digital twin, hosted in Stuttgart, can receive real-time sensor data from an identical robot operating in a Siemens factory in Munich, over a dedicated, low-latency slice spanning both private networks, enabling predictive maintenance benchmarking without exposing core IP.

BMW Group: Global Logistics & Assembly Roaming: BMW is pioneering the "follow-the-product" network. As a vehicle chassis moves from a manufacturing plant (private network) onto a carrier ship equipped with a private cellular network, and then to a finishing factory abroad, its embedded connectivity module maintains a persistent, secure connection. This allows continuous tracking, diagnostics, and even remote software updates, all under the policy of the BMW global core network.

Port of Rotterdam & Singapore PSA: Maritime Logistics Chain: These ports, equipped with massive private networks for crane and AGV automation, are federating to create a "green lane" for connected shipping containers. Sensor data on location, temperature, and integrity flows seamlessly from the origin port's network to the destination's network, streamlining customs and reducing spoilage.

Strategic Implications and the Road Ahead

The rise of Private Networks 2.0 redefines competitive landscapes:

For Enterprises (The Users): It transforms connectivity from a cost center into a strategic platform for global operational excellence, enabling truly elastic supply chains and collaborative ecosystems. The ROI case shifts from single-site efficiency to global velocity and innovation.

For Network Vendors & Integrators: The battle moves from selling hardware to providing federation platforms, global orchestration software, and lifecycle management services. Ecosystem partnership strategies become paramount.

For Telecommunications Operators: They face both competition and opportunity. They can compete as neutral host federation providers or offer "hybrid federation" services, seamlessly bridging private campus networks with their public network slices for true ubiquitous coverage.

The Borderless Enterprise Reality

Private Networks 2.0 marks the end of the connectivity silo. It promises a future where the secure, high-performance digital environment of an enterprise is no longer anchored to a physical location but is a portable, global asset. This evolution is essential for realizing the full vision of Industry 4.0, autonomous systems, and the distributed enterprise.

The foundational work—in standards, technology, and partnerships—is underway today. Forward-leading organizations are not just deploying private networks; they are actively designing their federation strategy, positioning themselves to operate in a world where their campus, quite literally, has no borders. The era of the globally roaming machine has begun.

Network Transformation | The NaaS Battlefield

The enterprise networking landscape is undergoing its most radical transformation since the dawn of the internet. The rigid, capex-heavy model of buying, deploying, and managing proprietary hardware is being decisively supplanted by a cloud-inspired paradigm: Network-as-a-Service (NaaS). This promises on-demand, consumption-based access to networking, security, and connectivity functions, delivered with cloud-like agility.

However, this market is not emerging as a unified front; it is a fiercely contested battlefield where three distinct archetypes—Traditional Vendors, Hyperscalers, and New Disruptors—are clashing with divergent strategies, assets, and visions. The prize is nothing less than ownership of the enterprise's digital nervous system. This analysis dissects each contender's model and assesses who holds the winning hand for delivering the future of flexible enterprise connectivity.

The Contours of the Battlefield: What Enterprise Demands?

True NaaS is more than a financing shift (leasing hardware). It is an operational model defined by:

Consumption-Based OpEx: Pay-per-use or subscription models.

Self-Service & Automation: Zero-touch provisioning and policy changes via API or portal.

Integrated Stack: Convergence of networking (LAN/WAN), security (SASE/SSE), and multicloud connectivity.

Assured Outcomes: SLAs for performance, uptime, and security, not just device availability.

This holistic demand set renders traditional vendor lock-in unsustainable and opens the door for new challengers.

Contender 1: The Traditional Titans (Cisco, HPE/Aruba, Juniper) – The Pivot from Products to Platforms

Strategy: Their approach is an evolution, not a revolution. They aim to wrap their vast installed base of hardware (switches, routers,

APs) in a software-defined, cloud-managed layer, transitioning clients to subscription licenses.

Their core thesis is that performance and reliability at the network edge require specialized hardware, which they control. Their NaaS offerings (e.g., Cisco Catalyst Center as a Service, HPE GreenLake for Aruba) are often hybrid, combining cloud management with on-premises appliances.

Strengths:

Deep Installed Base & Trust: Unparalleled relationships with global enterprise IT and deep domain expertise in complex networking.

Performance & Feature Depth: Hard to match in terms of raw throughput, low latency, and nuanced control for demanding environments.

Hybrid Reality: Acknowledges that not all workloads can move to the cloud, offering a bridge for the hybrid enterprise.

Weaknesses:

Inherent Conflict: The "product to platform" pivot risks cannibalizing lucrative hardware margins. Their NaaS can feel like a repackaging of old products rather than a ground-up cloud service.

Software & Experience Lag: Their cloud-native software and developer-centric UX often trail hyperscalers and disruptors.

Vendor Lock-in 2.0: The goal remains to keep customers within their proprietary ecosystem, albeit via subscription.

Case Study: Cisco+ SASE

Cisco bundles its Meraki SD-WAN, Umbrella SSE, and Thousand Eyes observability into a unified SASE subscription. A global retailer uses it to connect thousands of stores. The strength is single-vendor accountability and integration with their existing Cisco campus gear. The weakness is that it remains a distinctly Cisco cloud, lacking the native hyperscale application integration that a Microsoft-centric shop might desire.

Contender 2: The Hyperscalers (AWS, Microsoft Azure, Google Cloud) – The Cloud-Extension Play

Strategy: For hyperscalers, NaaS is a natural extension of their cloud dominion. Their goal is to make the wide area network (WAN) an indistinguishable, seamless extension of their cloud regions. Services like AWS Cloud WAN, Azure Virtual WAN, and Google Network Connectivity Center are designed to simplify connecting branches, data centers, and remote users directly and securely into their cloud backbones. Their core thesis: the network's primary purpose is to connect everything to their cloud.

Strengths:

Native Cloud Integration: Unbeatable for workloads already residing in their ecosystem. Security (Zero Trust), identity (Entra ID), and application policies are inherently unified.

Global Backbone: They operate the world's most sophisticated networks, offering high performance and redundancy.

Developer-Centric & API-First: Designed from the ground up for automation and infrastructure-as-code.

Weaknesses:

Cloud-Centric Myopia: Their models can struggle with traditional on-premises data centers, legacy applications, or true multicloud neutrality. Performance for intra-branch traffic or non-cloud apps can be suboptimal.

Limited Physical Edge: They lack deep expertise in campus/LAN environments (Wi-Fi, IoT switching). Partnerships (e.g., Azure with Aruba) reveal this gap.

Strategic Lock-in: The goal is to capture more cloud spend, creating a powerful new form of ecosystem lock-in.

Case Study: Microsoft Azure Virtual WAN with SASE

A company undergoing a "Microsoft-first" transformation uses Azure Virtual WAN as its network hub. It connects branches via SD-WAN vendors integrated into the platform and routes all traffic through Microsoft's global Secure Web Gateway (SWG) and Firewall. Employees enjoy seamless Zero Trust Network Access (ZTNA) to applications using their Entra ID. The model is supremely efficient for a Microsoft 365 and Azure-centric enterprise but adds complexity if major workloads reside on AWS or in a private data center.

Contender 3: The New Disruptors (Versa Networks, Aruba ESP (HPE), VMware, Palo Alto Networks) – The Best-of-Suite Aggregators

Strategy: This group, often born in software or security, is building cloud-native, vendor-agnostic control planes. They aggregate multiple network and security functions—SD-WAN, Firewall-as-a-Service, ZTNA, SWG—into a unified Secure Access Service Edge (SASE) or SSE offering delivered from the cloud. Their core thesis is that the future belongs to cloud-native software that can abstract and control a diverse mix of underlying transport and edge CPE (uCPE).

Strengths:

Cloud-Native & Agile: Built as multitenant cloud services from day one, enabling rapid feature rollout.

Best-of-Suite Integration: They offer a cohesive, pre-integrated stack of critical functions, reducing complexity vs. multi-vendor "best-of-breed."

Vendor Flexibility: Some (like

Versa) can run on a variety of white-box uCPE hardware, avoiding proprietary lock-in.

Weaknesses:

Limited Physical Reach: They rely on partners for last-mile connectivity and hardware logistics.

The "Jack of All Trades" Risk: While integrated, individual functions (e.g., a disruptor's firewall) may not match the depth of a dedicated security pure-play like Palo Alto.

Scale & Stability: While growing fast, they may lack the absolute global scale and financial longevity of a hyperscaler or Cisco.

Case Study: Palo Alto Networks Prisma SASE

A financial services firm with stringent security requirements adopts Prisma SASE. It deploys lightweight SD-WAN devices at branches that connect directly to Palo Alto's cloud security stack (CASB, FWaaS, SWG). The winning proposition is a uniformly enforced, world-class security policy from a single provider across all users and locations. It demonstrates the power of a security-led NaaS/SASE disruption, though it may depend on telco partners for underlying transport SLAs.

Analysis: Who Holds the Winning Model?

There is no single winner, but a clear stratification based on enterprise context is emerging:

For the "Cloud-First" Enterprise: The Hyperscalers are winning. If an organization's strategic direction is tightly aligned with AWS, Azure, or GCP, their native NaaS offers the path of least resistance, deepest integration, and likely the best performance for cloud workloads.

For the Complex, Hybrid Enterprise: The Traditional Vendors (evolving successfully) and Security-Led Disruptors are in a tight race. Large, global organizations with legacy data centers, complex campus environments, and a multi-cloud reality need a unifying layer that spans all domains. Traditional vendors with a genuine hybrid platform (e.g., HPE Aruba ESP with Central as-a-Service) have an edge if they execute the software transition flawlessly. Security-centric disruptors like Palo Alto win where security is the paramount, non-negotiable driver.

For Agile, Greenfield, or Specialized Needs: The Cloud-Native Disruptors win. New business initiatives, digital branches, or companies born in the cloud favor the agility, simplicity, and subscription purity of a Versa or similar player.

The Future: The Federated Mesh

The ultimate "winning model" may not belong to any single archetype but will emerge from federation. We will see partnerships where hyperscalers provide the global backbone and cloud integration, traditional vendors or specialists manage the physical/campus edge, and disruptors provide the overarching SASE control plane software.

The enterprise that can strategically assemble and orchestrate these pieces—perhaps with the help of a next-gen systems integrator or managed service provider—will achieve the true promise of NaaS: flexible, outcome-driven connectivity as a seamless utility. The battlefield is set, and the war will be won by those who best master both technology and partnership ecosystems.

TCCA –A Year in Review

By Tero Pesonen, chair of TCCA's Critical Communications Broadband Group, and TCCA Board vice-chair

It is difficult to condense into one article the achievements of TCCA members over the last year – the vast majority of work carried out as unpaid voluntary contributions in addition to the hugely demanding 'day jobs' of our Working Group members. For it is TCCA's Working Groups that comprise the heart of the association, coming together for the common good of all, to advance global critical communications for a safer, more connected world.

Massive Mission Critical Video

2025 began with the launch of the first of our authoritative white papers of the year, *'Guidance for the successful usage of Massive Mission Critical Video'*, produced by members of our Broadband Industry Group (BIG) and our Critical Communications Broadband Group (CCBG)

Video is one of the most promising and versatile technologies for improving operational efficiency and effectiveness for first responders, and the white paper explores what public safety agencies and operators need to consider to successfully deploy video services supporting mission-critical

operations, especially where the scale of its usage is considered 'massive'. The overall objective is to ensure that first responders and public safety agencies (and by implication other critical communication sectors) can use video effectively and for operational benefit.

The importance of physical infrastructure security

Our Legal and Regulatory Working Group (LRWG) followed this with the publication of the paper *'Legal and Regulatory aspects relating to the physical security of the telecommunications infrastructure used for critical communication services',* aiming to focus the attention of critical communications providers to the importance of physical infrastructure security. The goal is to catalyse the creation of a global standard for the physical security of infrastructure supporting critical communications.

Why is this important now? Because most of the current critical communication networks using technologies as TETRA, Tetrapol and P25, are owned and operated by the state, and their physical security is assured by the state to the extent deemed necessary. However, the emerging use of commercial mobile operator (MNO) networks to support broadband critical communications, particularly as Radio Access Networks, is changing the operating model.The physical security of these network elements is of paramount importance, but it is debatable whether the measures that MNOs are currently adopting in this regard are sufficiently robust and fit for purpose – hence the need for legal and regulatory measures.

Safeguarding TETRA Interoperability

Managed by our Technical Forum, TCCA's world-leading TETRA Interoperability (IOP) testing and certification process underpins the ongoing success of the TETRA standard, the most widely used mission critical communications system in the world. The independence of the IOP process ensures the ongoing strength of the market and its support by multiple vendors. In June 2025 TCCA announced the appointment of DEKRA, the world's largest independent, non-listed expert organisation in the field of standards-based testing, inspection and certification, as the new TETRA Certification Body that will oversee the IOP testing process and issue the certificates.Several DEKRA offices around the world are involved in supporting the TETRA IOP process, including those in Germany, Chile, China and Spain.

Quality of Service, Priority and Pre-emption (QPP)

TCCA's *QPP Implementation Guide,* written by a task force comprising members from our CCBG and BIG, was launched just prior to Critical Communications World. The Guide deliversa common industry recommendation for the implementation of QPP capability when using 3GPP mechanisms. The Guide represents the collective insights and best practice from leading government authorities, commercial operators, infrastructure providers, control room specialists, device manufacturers, and app vendors with experience in QPP implementations.

Critical Communications World 2025

Our world-leading Critical Communications World (CCW) 2025 event was hosted in Belgium by national critical network operator and TCCA member ASTRID. With record attendance, including from government operators from around the globe, the show sets the agenda for the future of the critical communications sector. India's announcement of their proof-of-concept for critical broadband adoption with local operators highlighted the government ambitions to enhance their public safety systems with broadband capabilities following the example of South Korea, Finland, France and USA critical broadband efforts. Join us in London for CCW 2026!

Critical training courses

For anyone connected with critical communications, there is now for the first time, a range of training courses to meet all requirements. From new entrants to the sector using narrowband to those adopting 4G/5G critical broadband networks and those on the periphery, TCCA and Wray Castle launched *The Critical Communications Institute,* featuring a suite of specialist training solutions to help professionals understand, design, build and optimise the critical communications networks of today and tomorrow.

The focused, practical and highly relevant courses cover the latest critical telecoms technologies including mission critical narrowband TETRA, mission critical broadband, LTE and 5G technologies, tailored to the precise needs of critical industry sector users such as those in public safety, utilities, transport, energy and mining.

The Interworking Function (IWF)

The increasing development of critical broadband networks means the key issue for network operators is how to ensure mission critical services delivered over broadband interwork with the existing narrowband land mobile radio (LMR) networks such as TETRA.

Our newest Working Group, the IWF Working Group, delivered a detailed white paper *'Interworking*

Function (IWF) Interworking of LMR networks with 3GPP Mission Critical Services' that explores the opportunities and challenges of interworking LMR networks with 4G/5G-based 3GPP Mission Critical Services (MCX) solutions by leveraging the standard-defined Interworking Function and achieve seamless interoperability for a gradual and successful adoption of broadband technologies.

First Critical Communications India event

August 2025 saw *Safeguard The Future: India's First Mission-CriticalCommunications Conference,* take place in New Delhi, jointly presented by TCCA and the Broadband India Forum (BIF), the independent policy forum and think tank that works towards the development and enhancement of the entire broadband and broadcasting ecosystem in a holistic, technology and service neutral manner.

Theconference focused on trusted, reliable, secure, and interoperable communications in public safety, disaster response, utilities, transport, healthcare, and smart cities, and united key stakeholders from government, emergency response and critical infrastructure organisations, global standards bodies, Regulators, Spectrum Managers, Industries to showcase innovations in critical communications. The 2026 event will take place in September.

Broadband Callout Specifications

Towards the end of the year, the extensive work of a task force within TCCA's CCBG led to the creation of new mission critical broadband callout specifications compatible with 3GPP MCX standards, using MCData SDS and MCPTT. The two new critical documents are the *Mission Critical Broadband Callout Service Overview* with requirements and use cases, and the *Mission Critical Broadband Callout Service Definition* with the detailed specifications.

Callout is a two-way paging service that enables a control room dispatcher to select the first responders that should respond to an incident and send them callout alerts with a description of the incident situation. The TETRA callout specifications were developed by TCCA in 2009 and is a vital service in TETRA networks but has, until now, not been available for 3GPP 4G and 5G broadband mission critical networks.

Success in cooperation

TCCA works closely with likeminded organisations such as EUTC, 450 MHz Alliance and UIC, and is a key supporter of the ETSI MCX and FRMCS Plugtests. TCCA is the 3GPP Market Representation Partner for the critical communications sector, driving the sector's views and needs. During the year TCCA has actively pushed for trust to be the key design principle in 3GPP standardisation and this is being recognised in the 6G studies. This mainly translates to reliability, resilience and availability since the connection is in this sector the lifeline. This work needs to continue. Previous and this year's contributions to address services like device-to-device multi-hop are now ready for implementation as 3GPP 5G Advanced Release 19 is completed.

The 3GPP standards form the foundation for common global mission critical broadband services for PPDR (Public Protection and Disaster Relief). TCCA and GCF (Global Certification Forum) jointly developed 3GPP conformance and later interoperability certification to truly enable multivendor market evolution, interoperability with better quality products, wider supply and innovation for less cost due to larger market and wider competition. To help agencies to procure compliant products, TCCA's LRWG has already published a procurement guide.

This is just a snapshot of TCCA's year. There is much work under way, and much to be done. If you want to be involved – join us! Further information on all of the above, and how to join, can be found at **www.tcca.info.**

Tero Pesonen

Tero Pesonen, TCCA Board Vice-Chair and Chair of TCCA's Critical Communications Broadband Group (CCBG)
With a career spanning more than 25 years in critical communications, Tero has been involved in various global management and leadership roles, facilitating strong customer relations, strategic business orientation and wide-ranging solution development. He has been involved with professional mobile radio communications since 1997, beginning his career promoting and organising TETRA interoperability activities and developing a deep understanding of public safety application models.
Today, Tero is deeply involved in ground-breaking work related to new opportunities in mission critical broadband. He works closely with major public safety and critical infrastructure operators and users, creating advanced solutions to meet mission critical requirements.
Since September 2014 he has been chair of TCCA's Critical Communications Broadband Group (CCBG), bringing different stakeholders together to create a common critical broadband future. He is also the vice chair of TCCA's Board, representing the Finnish governmental public safety operator Erillisverkot. Tero holds Master of Science degrees in electrical engineering and economics.

Gen AI Assistant | Your New Customer Service Agent and Network Engineer

The narrative around artificial intelligence in telecommunications is undergoing a fundamental rewrite. We are moving beyond deterministic, rules-based automation and scripted chatbots into a new era of cognitive, generative partnership.

Fueled by the seismic leap of large language models (LLMs) and foundation models, Generative AI (GenAI) is not merely a tool for efficiency; it is emerging as a transformative co-pilot capable of assuming multifaceted roles across the telecom value chain. This technology is beginning to act as an intuitive customer service agent, a hyper-personalized product seller, and—most disruptively—a reasoning network engineer.

This evolution marks the shift from AI that automates tasks to AI that understands context, generates solutions, and collaborates with humans to solve unprecedented challenges.

Part 1: From Frustrating Chatbots to Empathetic, Generative Concierges

The legacy chatbot, trapped in its decision-tree prison, has been a persistent source of customer frustration. GenAI shatters that model. Today's advanced Generative AI Customer Assistant is built on a fine-tuned LLM that ingests a carrier's entire knowledge base—terms of service, network outage data, troubleshooting guides, and individual customer history.

The Generative Difference:

When a customer messages, "My internet is slow during video calls," the legacy bot might offer a generic reboot script. The GenAI assistant, however, performs real-time analysis. It checks the customer's line quality, correlates the issue with localized network performance metrics, reviews the customer's service plan, and understands the intent behind "slow during video calls." It can then respond in natural language: *"I see you're on our 100Mb plan, and your line is currently experiencing intermittent latency spikes between 7-9 PM, which would affect video calls. This aligns with a minor capacity upgrade underway in your area, scheduled for completion this Friday. In the interim, I can prioritize your work-from-home traffic during those hours. Would you like me to implement that temporary optimization?"* This moves the interaction from transactional to consultative, building trust and reducing escalations by an estimated 40-50%.

Part 2: The Hyper-Personalized Seller: From Bundles to Bespoke Life Solutions

GenAI redefines the commercial engine. Instead of pushing pre-packaged bundles, it acts as a Personalized Service Architect. By analyzing a customer's aggregated, anonymized usage patterns (data consumption, roaming history, app usage, device types) and correlating it with lifecycle events (a move, a new device purchase), the AI can generate and propose uniquely tailored service plans.

Case in Action:

For a family constantly exceeding data limits, with teenagers showing high gaming data usage and parents frequently on international Zoom calls, the GenAI system doesn't just offer a bigger data bucket. It generates a custom proposition: *"Based on your household's usage, I've designed a 'Home & Hub' plan. It includes: 1) Unlimited priority data for your work laptop during business hours, 2) A 200GB high-speed gaming data pool for the Xbox, 3) A monthly 5-hour international roaming data pass for your trips, and 4) A 20% discount on a mesh Wi-Fi extender for your upstairs office. This is 15% less than your current à la carte spending."* This dynamic, contextual offer creation transforms the sales funnel from a blunt instrument into a precision advisory service, lifting average revenue per user (ARPU) and reducing churn.

Part 3: The Most Disruptive Role: The Generative Network Engineer

This is where GenAI transitions from a front-office marvel to a core strategic asset. The complexity of modern, software-defined networks (SDN, NFV, 5G cores) is exceeding human scale. GenAI is becoming an indispensable member of the Network Operations Center (NOC) and development teams.

1. Natural Language Network Troubleshooting:

Engineers no longer need to write complex SQL queries or master vendor-specific CLI syntax. They can converse with a Network Co-Pilot trained on network topology, real-time telemetry, historical incident logs, and network protocol documentation.

An engineer can ask: "Why are users in the downtown sector experiencing dropped calls between Cell Sites A and B?" The GenAI model, in seconds, cross-references thousands of data points and responds: "Analysis shows a 30% increase in handover failures correlated with a recent software patch on the Mobility Management Entity (MME). The failure logs point to a timer incompatibility. I've generated a recommended configuration rollback script and identified the 5% of users most affected. Would you like to review and execute the mitigation?" This cuts mean-time-to-repair (MTTR) from hours to minutes.

2. Autonomous Code Generation for Network Functions:

In the era of cloud-native network functions (CNFs), code is infrastructure. GenAI models like GitHub Copilot, specialized on

telecom codebases, are now assisting developers in writing and testing code for network automation, policy enforcement, and even 5G core functions. A developer can prompt: "Write a Python function for our orchestrator that scales up the user plane function (UPF) instances in Azure when throughput exceeds 80% for 5 minutes, ensuring session continuity." The AI generates the initial, syntactically correct code, complete with API calls and error handling logic, which the engineer then reviews and refines. This accelerates development cycles by over 30% and allows human engineers to focus on architecture and innovation, not boilerplate code.

3. Proactive Network Synthesis and Security:

GenAI moves beyond reactive fixes to predictive synthesis. It can analyze traffic patterns and generate new security policies or network slices on-the-fly. For example, ahead of a major streaming sports event, the AI could recommend and draft the configuration for a temporary, high-capacity network slice dedicated to streaming traffic in the stadium area, ensuring quality of experience (QoE). Furthermore, by learning normal network behavior, it can generate hypothetical attack scenarios, test defenses, and propose refined security rule sets, creating a self-fortifying network.

The Strategic Imperative and Cautions

Integrating this level of GenAI is not an IT project; it is a core business strategy requiring:

High-Quality, Unified Data: The AI's reasoning is only as good as its ingested data. Breaking down data silos between customer, network, and IT systems is a prerequisite.

Human-in-the-Loop (HITL) Governance: Critical decisions, especially in network operations and code deployment, require human oversight. The model is a co-pilot, not an autopilot. Establishing clear HITL protocols for approval is essential for safety and trust.

Specialized Fine-Tuning & Ecosystem Partnerships: Off-the-shelf LLMs lack telecom domain knowledge. Success lies in fine-tuning foundational models with proprietary network data and partnering with specialized AI vendors (e.g., NVIDIA's RAN-specific AI frameworks, or startups like Arista's cognitive network suites).

The Era of Cognitive Partnership

Generative AI is not replacing the telecom workforce; it is fundamentally augmenting and elevating it. The customer service representative is now a relationship manager overseeing an AI concierge. The salesperson becomes a strategic advisor leveraging AI-driven insights. The network engineer evolves into a platform architect, directing AI agents to manage complexity at machine speed.

The carriers who will thrive are those that stop viewing GenAI as a cost-cutting chatbot and start embracing it as a Cognitive Partner—a new category of intelligent asset capable of generating unprecedented levels of customer loyalty, operational resilience, and service innovation. The future of telecom belongs not to those with the biggest pipes, but to those with the most intelligent, generative partnership between human and machine. The new hire in your customer service, sales, and network engineering departments isn't on the payroll; it's in the cloud, ready to collaborate.

The Open RAN's Tipping Point | Success Stories and Stumbling Blocks in 2025

In the high-stakes theatre of global telecom infrastructure, Open RAN (Open Radio Access Network) has graduated from a compelling PowerPoint vision to a tangible, if complex, reality on the ground. Promising to disaggregate hardware from software, break vendor lock-in, and inject innovation through a multi-supplier ecosystem, it has reached a pivotal year. 2025 is not the year Open RAN conquers all; it is the year of its most candid, public stress test.

Early deployments, from dense urban cores to remote rural outposts, are delivering hard data on the paradigm's true potential and its persistent, formidable challenges. This analysis provides an on-the-ground assessment of where Open RAN is demonstrably succeeding, where the rubber meets the road—and where it's causing operators to question the immediate ROI.

Part 1: The Success Stories – Where the Promise is Materializing

In specific, strategic scenarios,

Open RAN is not just viable but is becoming the architecture of choice, delivering on its core tenets.

1. Success in Greenfield & Neutral Host Deployments:

The most unambiguous wins are in new builds. Japan's Rakuten Mobile, the oft-cited pioneer, has scaled its fully virtualized, cloud-native Open RAN to cover the majority of its population. The success metric here is operational transformation. By building a "telco cloud" with a CI/CD pipeline, Rakuten reports a 40% reduction in deployment costs versus traditional RAN and a 30% reduction in energy consumption per bit—a crucial figure in 2025's energy-conscious climate. The value is not just in cheaper radios, but in the automation of network lifecycle management.

Similarly, in the United States, DISH Wireless has built its 5G network from the ground up with Open RAN. While facing its own scaling challenges, DISH's success story is vendor diversity. Its ecosystem includes Mavenir, Fujitsu, and VMware, demonstrating the technical feasibility of a multi-vendor RAN stack. For DISH, the promise was speed to market and avoiding the traditional duopoly, a goal it has tangibly achieved.

2. Success in Rural & Underserved Coverage:

Perhaps the most socially and politically potent success is in cost-effective rural expansion. In the UK, Vodafone and Virgin Media O2's Shared Rural Network (SRN) initiative is using Open RAN to eliminate "not-spots."

By deploying compact, software-defined radios from specialists like Mavenir or Parallel Wireless on existing mast sites, they can cover challenging, low-population areas at a lower total cost of ownership (TCO). The modularity allows for mixing and matching: a best-of-breed remote radio unit (RRU) from one vendor with a cloud-based Central Unit (CU) from another, optimized for specific terrain.

Case Study Spotlight: India's BhartiAirtel

Airtel's massive Open RAN deployment, targeting tens of thousands of sites, is a masterclass in tactical, cost-driven adoption. Rather than a full "rip and replace," Airtel is using Open RAN for network expansion and modernization in specific circles. The result?Airtel reports a 20-30% lower capex per site compared to a traditional vendor bid. This is the pure, unvarnished economic driver in action: using competitive pressure from new suppliers like NEC, Radisys, and Tata to secure better pricing and flexibility, even if the full software automation promise is phased.

Part 2: The Stumbling Blocks – Where Complexity Bites Back

For every greenfield success, there is a brownfield operator encountering what industry insiders now call "the integration tax."

1. The Systems Integration Quagmire:

In traditional RAN, Nokia, Ericsson, or Huawei provided a single, accountable throat to choke. In Open RAN, the operator becomes the master systems integrator, or hires one. This has spawned a new layer of complexity and cost. Deployments by Vodafone in the UK and Telefónica in Germany have revealed that the cost and effort of integrating radios, servers, and software from 3-5 different vendors can erode the hardware savings.

The new roles of RAN System Integrators (SIs) like Tech Mahindra or IBM are essential but add a new line item to the budget. The promised "best-of-breed" assembly can quickly become a "blame-of-breed" troubleshooting nightmare when a latency spike or handover failure occurs.

2. Performance & Energy Efficiency Gaps:

In dense, high-capacity urban environments—the most lucrative and demanding sites—Open RAN has faced headwinds. Early performance benchmarks in Deutsche Telekom's lab tests and Verizon's field trials showed that some Open RAN configurations, particularly those using general-purpose processors (GPP) for Layer 1 processing, could not match the radio performance and energy efficiency of traditional vendors' optimized, silicon-based systems. The "cloud-native" ideal ran into the physics of radio signal processing. While specialized Layer 1 chips from the likes of Marvell and Qualcomm are now entering the market, they add cost and complicate the vendor landscape further. For a tier-1 operator, the risk of a performance regression in their flagship cities is unacceptable.

3. The Immaturity of the Ecosystem & Security Scrutiny:

While vendor diversity is increasing, true multi-vendor interoperability remains a work in progress. Plugfests and O-RAN ALLIANCE certifications have improved matters, but field deployments still encounter proprietary "extensions" or subtle implementation differences that break seamless operation. Furthermore, the highly software-defined, virtualized nature of Open RAN has expanded the threat surface area. The U.S. government's continued scrutiny and the requirement for stringent component sourcing (e.g., via the FCC's "Covered List") have added a layer of geopolitical and compliance complexity that some operators find daunting. The cost of securing a disaggregated, multi-vendor system

can be higher than securing a monolithic one.

Part 3: The 2025 Verdict: A Strategic Tool, Not a Panacea

The on-the-ground reality in 2025 reveals that Open RAN is not a binary switch to flip across a network. It is a strategic tool with specific, high-ROI use cases.

It is a Winner for: Greenfield operators (building a cloud-native cost base), rural coverage (cost-effective expansion), and as a negotiating lever for brownfield operators to secure better terms from incumbents. Its power to foster innovation in the RAN Intelligent Controller (RIC) for traffic optimization and energy savings is beginning to bear fruit.

It Remains a Challenge for: Dense urban macro deployments where peak performance and efficiency are non-negotiable, and for operators lacking the in-house software and integration expertise to manage the new complexity.

The Path Forward: Hybrid Architectures and Managed Services

The emerging consensus among pragmatic operators is a hybrid, phased approach. They are deploying Open RAN at the network edge (for coverage) and in specific new market segments, while relying on optimized, traditional RAN in capacity-heavy urban cores. Furthermore, a new Managed Open RAN as-a-Service model is gaining traction, where a systems integrator or even a traditional vendor offers to take on the integration and operational burden for a fee. This preserves some diversity while outsourcing the headache.

Beyond the Tipping Point

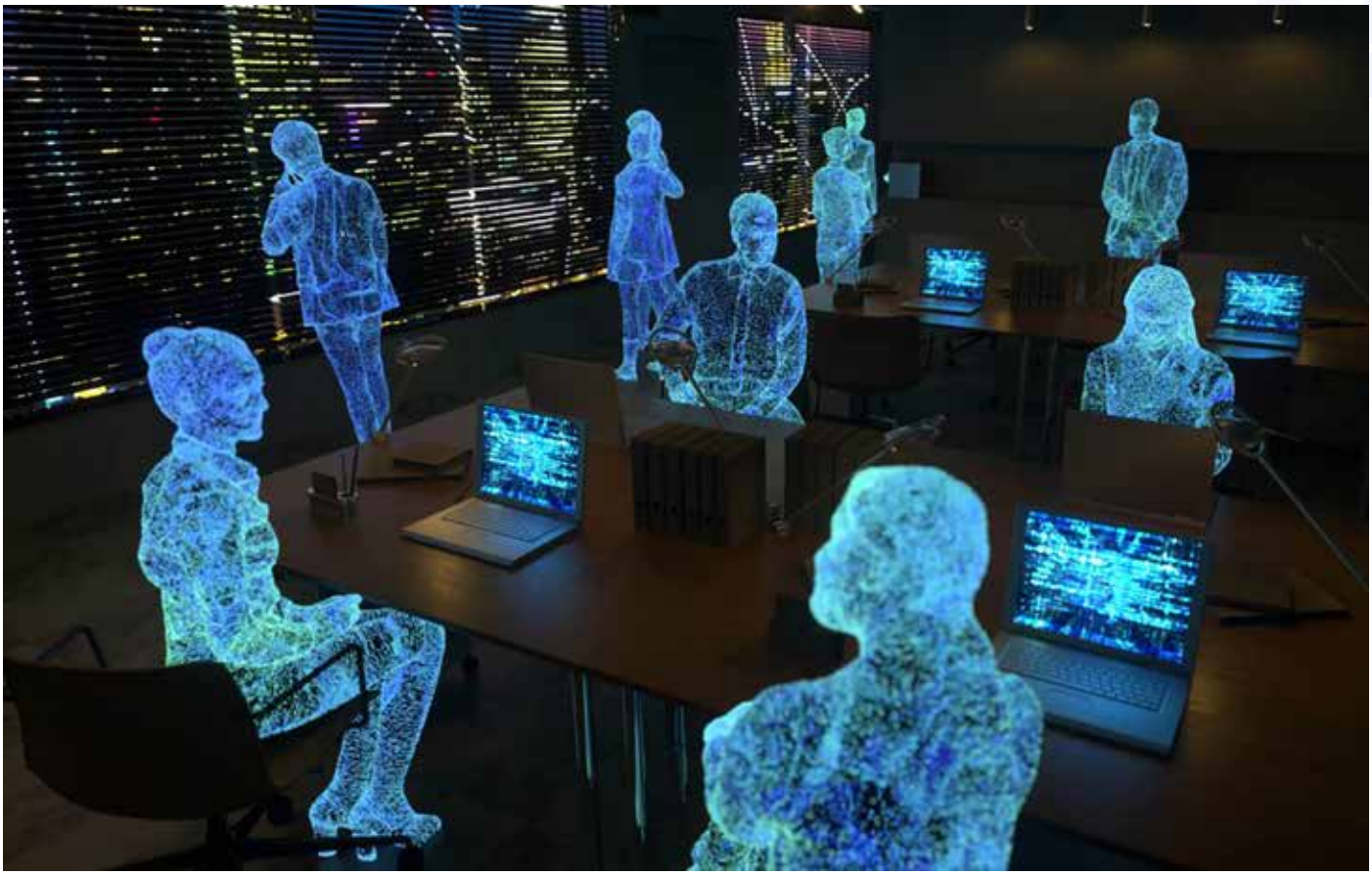
Open RAN has decisively tipped from theory into practice. Its success stories in Japan, India, and rural Europe prove its economic and operational value is real.

However, 2025 has also dispelled the notion of an easy, universal victory. The stumbling blocks of integration, performance parity, and ecosystem maturity are significant and costly. The conclusion is one of strategic nuance: Open RAN is a powerful new weapon in the operator's arsenal—ideal for specific missions—but it is not yet, and may never be, the single weapon for every battle.

The operators winning in 2025 are those not chasing ideology, but soberly deploying Open RAN where its economics and agility make irrefutable sense, and managing its complexity with eyes wide open. The revolution is here; it's just more evolutionary than anyone predicted.

What People Are Actually Doing with ChatGPT?

By Dario Betti, CEO, Mobile Ecosystem Forum (MEF)



For years, asking Alexa has been a familiar part of daily life. Yet, until the long-awaited Alexa+ arrives in all territories, Amazon's voice assistant feels a little like a silent film star at the dawn of the "talkies": a pioneer overshadowed by a new, more expressive generation. The headline act of this new era is ChatGPT — the most visible and widely used of today's generative AI systems. Until recently, however, little was known about what people actually do with it. OpenAI's new study, How People Use ChatGPT, offers the first detailed look at how the tool is being woven into professional, educational, and personal routines.

A report with caveats

The research draws on anonymised data from ChatGPT's consumer users across its Free, Plus, and Pro tiers, analysed through a privacy-preserving system that examines short text snippets rather than full conversations or identifiable information. This method safeguards privacy but limits interpretive depth: researchers can see patterns of use but not full context or motivation. The dataset also leans toward English-speaking, higher-income regions — effectively a snapshot of early adopters rather than a globally representative picture.

Even so, the report offers the clearest evidence yet of how generative AI is embedding itself in modern life and how its role is evolving from curiosity to essential utility.

From experimentation to integration

In its early days, ChatGPT use was marked by playfulness and exploration. People tested boundaries,

asked creative or whimsical questions, and probed the system's quirks. That exploratory phase has now matured into a more purposeful one. Across many professions, ChatGPT is increasingly deployed as an amplifier of human effort rather than a substitute for it. Users seldom automate entire tasks; instead, they use the model to accelerate drafting, summarising, reformatting, or debugging — the "tedious" groundwork.

This could signal a shift in how productivity is viewed. As AI takes on the routine and the mundane, it can expand the capacity of a human workforce, redefining what counts as efficient work. Output expectations are likely to rise because people can achieve more in the same span of time.

Patterns of professional use

The report identifies two main clusters of ChatGPT use. One sees technical users (programmers, analysts, engineers) employ the model to troubleshoot, write code, or explain complex concepts. The other has creative professionals and educators using it for ideation, drafting, or refining communication. However, increasingly these boundaries blur. Creative users employ AI for structured analysis, while technical professionals explore its capacity for conceptual or narrative tasks. The technology's flexibility can encourage a cross-pollination of skills, dissolving old divides between the technical and the creative.

Education as a testing ground

Nowhere is this hybridisation more visible than in education. Students turn to ChatGPT to summarise reading materials, clarify difficult topics, and produce first draft essays; teachers use it to design lessons and generate exam questions. Despite lingering concerns about academic integrity, the prevailing attitude is pragmatic. Both educators and learners treat ChatGPT as a collaborator, not a shortcut, and routinely factcheck and/or adapt AI output. In this context, AI functions as a partner filling multiple roles – a tutor, editor, and research aide rolled into one. Education may, in fact, become the proving ground for a wider cultural shift: a world in which AI is expected to assist rather than simply automate.

Healthcare's cautious experimentation

The report shows that healthcare remains a modest user of ChatGPT, but clinicians and researchers are exploring applications such as summarising patient notes, generating plain-language explanations for patients, and easing administrative burdens. These uses remain early-stage and cautious, but they highlight how generative AI can first establish trust through low-risk, supportive roles before advancing into more complex medical or diagnostic territory.

Generational and sectoral divides

Adoption also varies by age and industry. Professionals in technology, science, and business are leading adopters, while service and manual sectors have been slower to integrate AI into daily work. Younger users—in particular students and early-career professionals—treat ChatGPT as a natural extension of their workflow, while older users approach it more selectively as a productivity aid. These generational differences suggest that as digital natives advance through the workforce, AI fluency will increasingly be assumed rather than learned.

A cautious but significant milestone

The authors of How People Use ChatGPT are careful to acknowledge the study's boundaries. It provides a large-scale, anonymised snapshot rather than a definitive map of the future. Yet even within those limits, the findings are striking. They show that generative AI has moved away from novelty towards necessity. Whether in the classroom, the clinic, or the office, ChatGPT is changing not just the speed of human work but its texture — the way ideas are formed, refined, and shared.

The report is perhaps a cultural turning point. The silent-movie era of AI (defined by scripted, command-based assistants) is giving way to something more conversational, responsive, and creative.

Dario Betti

Dario Betti is CEO of MEF (Mobile Ecosystem Forum) a global trade body established in 2000 and headquartered in the UK with members across the world. As the voice of the mobile ecosystem, it focuses on cross-industry best practices, anti-fraud and monetisation. The Forum, which celebrates its 25th anniversary in 2025, provides its members with global and cross-sector platforms for networking, collaboration and advancing industry solutions.

The 6G Horizon: Beyond Speed, the Dawn of the Sensory Internet

While global enterprise is still grappling with the transformative potential of 5G—with its promise of enhanced mobile broadband, IoT, and low-latency applications—the strategic vanguard of the telecommunications and technology sectors has already pivoted to the next paradigm. The narrative for 6G, targeted for commercial deployment around 2030, is being written today, and it transcends the familiar metric of speed.

6G represents a fundamental shift from a network that connects devices to one that fuses the physical, digital, and human worlds. It heralds the dawn of the "Sensory Internet," an intelligent, pervasive fabric capable of capturing, transmitting, and processing the full spectrum of sensory and contextual data.

For business leaders, understanding this trajectory is not premature; it is critical for long-term R&D investment, ecosystem positioning, and envisioning the future of industry, commerce, and society.

From Connectivity to Cognitive Integration: The 6G Value Proposition

The proposed technical pillars of 6G are not merely incremental improvements but enablers of entirely new service classes:

Terahertz (THz) Frequencies & Extreme Capacity: Utilizing sub-millimeter and terahertz waves

(100 GHz to 3 THz) will unlock unprecedented bandwidth, enabling data rates potentially 100 times faster than 5G. This is not for downloading movies quicker, but for supporting massive, real-time data streams from millions of sensors, ultra-high-fidelity holographic communications, and precise digital twins.

Native AI & Machine Learning: 6G architectures are being designed with AI at their core—not as an overlay, but as an embedded, distributed intelligence. The network itself will autonomously manage resources, predict congestion, and optimize performance for trillions of diverse endpoints, becoming a self-optimizing, cognitive entity.

Integrated Sensing and Communication (ISAC): This is the cornerstone of the Sensory Internet. 6G radio signals will do double duty: they will communicate and sense the environment. By analyzing how signals reflect off objects, the network can map surroundings, detect motion, measure vibrations, and even infer material properties—all without dedicated cameras or LiDAR. This turns the network infrastructure into a ubiquitous, distributed sensor.

Three-Dimensional Connectivity: 6G will seamlessly integrate non-terrestrial networks (NTN)—satellite constellations, high-altitude platform stations (HAPS), and drones—with terrestrial cells. This provides truly global coverage, from deep indoors to remote oceans and skies, enabling persistent service for autonomous systems and global IoT.

Trust, Security, and Sustainability by Design: Given its pervasive nature, 6G standards are prioritizing end-to-end quantum-resistant security, explainable AI operations, and radical energy efficiency through zero-energy device designs and smart energy harvesting.

The Business Imperative: Unlocking New Economic Verticals

The convergence of these capabilities will disrupt and create industries:

The Immersive Metaverse, Realized: 6G will move us beyond screen-based VR to multi-sensory, holographic telepresence. Business meetings, remote expertise, and collaborative design will involve life-like, volumetric avatars interacting in real-time with zero perceptible lag, dissolving geographical barriers for knowledge work.

Precision Digital Twins of Everything: Cities, factories, supply chains, and even human physiology will have ultra-high-resolution, real-

time digital replicas. Fed by continuous data from ISAC and IoT, these twins will enable predictive simulation, optimization, and remote control at a fidelity impossible today. Imagine stress-testing a city's traffic flow during a major event or simulating a full production cycle before a single physical asset is moved.

Autonomous Everything, Everywhere: The reliability, latency, and sensing capabilities of 6G will be the final enabling layer for fully autonomous vehicles, drones, and robotics in unstructured environments. A warehouse robot won't just follow a pre-set path; it will dynamically navigate a live map created and shared by the network itself.

Ubiquitous Sensing-as-a-Service: Enterprises will subscribe to environmental intelligence from their network provider: real-time data on facility occupancy, equipment health, supply chain logistics tracking, and environmental monitoring—all derived from the communication signals themselves.

Global Case Studies: Prototyping the Future

While 6G is in its foundational R&D phase, global consortia are building testbeds to validate its core tenets:

The Hexa-X &Hexa-X-II Projects (Europe): Led by Nokia and involving key academic and industry partners, this flagship EU 6G research program is building a complete end-to-end 6G system blueprint. Their testbeds are exploring critical use cases: "Telepresence in Hazardous Work," where a remote expert uses haptic feedback and ultra-high-definition sensing to guide a on-site robot, and "Sustainability through Network-Driven Efficiency," where the AI-native network dynamically minimizes energy consumption across a smart city's infrastructure.

The 6G Research and Development Pilot (South Korea): Under the "K-Network 2030" strategy, South Korea aims for a 2026 pre-6G trial and 2028 commercial prototype. A key case study led by SK Telecom and Samsung involves "In-Cabin Experience for Autonomous Air Vehicles." Here, 6G's high-capacity, low-latency links provide passengers with immersive augmented reality windows (showing real-time flight data or transformed vistas) and seamless high-fidelity entertainment, while simultaneously ensuring critical vehicle control and sensing data is prioritized.

The IMT-2030 Promotion Group & FuTURE Forum (China): China has mobilized its major carriers and vendors (Huawei, ZTE) in a coordinated national 6G effort. Publicly shared research includes advanced demonstrations of "Integrated Sensing and Communication for Smart Transportation." Test vehicles use 6G prototype base stations not just for connectivity, but to generate high-resolution imaging of the road ahead, detecting obstacles and pedestrians even in poor visibility—showcasing how ISAC could become a primary sensor for vehicle autonomy.

The Next G Alliance (North America): Organized by the Alliance for Telecommunications Industry Solutions (ATIS), this industry-led group is defining a holistic vision for North American leadership. Their working groups are developing roadmaps for 6G applications in "Distributed Edge AI." A highlighted scenario involves distributed manufacturing, where complex AI models for quality control are split and processed across the network edge, with 6G providing the deterministic latency and synchronization needed for real-time robotic adjustments on a production line.

Strategic Considerations for the C-Suite

The journey to 2030 demands action now:

Ecosystem Strategy: 6G will blur industry lines. Telcos, cloud providers, sensor manufacturers, and vertical industry leaders must form deeper, earlier partnerships to co-create standards and applications.

Spectrum Advocacy: The race for terahertz and mid-band spectrum is a geopolitical and commercial imperative. Businesses must engage in policy dialogues to ensure harmonized, sufficient spectrum is available.

Talent & R&D Investment: The focus must shift from pure connectivity engineers to experts in AI/ML, sensing technologies, holography, and ethical AI governance. Early investment in applied research is crucial.

The Sustainability Lens: The promise of enabling global efficiency must be weighed against the energy footprint of vastly denser networks. Sustainability is not a feature but a design constraint for 6G.

Conclusion: Preparing for a Contextual World

The 6G horizon is not just about a faster network; it is about a more intelligent, perceptive, and integrated one. It moves us from an Internet of Things to an Internet of Senses and Context, where network intelligence understands not just data, but the environment and intent behind it.

For forward-looking enterprises, the message is clear: The foundational work for the 2030 digital economy is happening in labs today. The business models, operational paradigms, and consumer experiences that 6G will unlock are now being imagined. Engaging with this developmental phase—through partnerships, research, and strategic foresight—is how organizations will transition from being adopters of technology to becoming architects of the Sensory Internet era. The dawn is approaching; strategic vision must rise to meet it.

How Satellite Broadband Complements India's Mobile Networks, Not Competes With Them

By Konark Trivedi, Founder and Managing Director, Frog Innovation Ltd

As part of its digital transformation, India is moving fast, which has resulted in the debate about satellite broadband and its role in the country's connectivity landscape getting really heated. There is a widespread misunderstanding that the satellite systems, for example, Starlink, are competing with the existing mobile networks. In fact, these two technologies meet different needs and are, in a way, highly complementary as they are designed to be that way.

Urban India's Network Strength Is Unmatched by Satellite Systems

The Indian telecom operators have set up some of the most advanced and densely distributed mobile broadband networks in the world. In the case of metro cities and big towns, fiber backhaul, 4G, and now 5G infrastructure are providing a high-quality, high-capacity connectivity that is beyond the reach of satellite systems in terms of deployment size.

The area covered by satellite beams is wide and supports a small number of users per beam. In contrast, mobile networks flourish in urban India due to:

- The distance between cell sites can be only a few kilometers
- Spectrum reuse is much more effective
- Capacity can be quickly increased by using small cells,

massive MIMO, and fiberized networks

This situation makes satellite broadband absolutely not suited as the primary connectivity layer for the dense cities in India, where the existing mobile and fiber networks needed for coverage and capacity are already excellent.

India's telecom achievements have been outstanding but still, one area of concern is rural connectivity. It is often not economically viable to lay fiber over rough terrain, serve sparse population clusters, and install high-capacity towers in low-ARPU areas. Here, actually, satellite broadband can change the game. Satellites can overcome most of the hindrances faced by remote areas because, among others, they have the following advantages:

- They do not require last-mile terrestrial infrastructure
- They can provide broadband to areas where fiber rollout is slow or impossible
- They bypass terrain constraints such as mountains, forests, and deserts
- They can connect the "last 1%" or "least served" regions with speed and reliability

For a country with the geographic and demographic diversity of India, satellite is not an alternative to mobile networks; it is an extension of them.

India's Growth Demands a Hybrid Connectivity Architecture

The future of India's digital ecosystem will be built on a hybrid connectivity model:

- Fiber as the backbone
- 4G/5G/6G as the primary urban and suburban access layer
- Satellite broadband as the high-impact rural and remote access layer

This combination ensures nationwide coverage without the necessity for extra infrastructure or a drop in service quality. Furthermore, it is consistent with the country's larger digital aspirations, including Digital India, BharatNet, and the upcoming liberalization of the satellite communication sector.

A Strong Partnership Opportunity for Indian Operators

Instead of rivalry, satellite and telecom operators can join forces in a number of ways that will create a substantial impact:

- Backhaul connectivity for mobile sites that are very remote
- Communication for emergencies and disaster recovery
- Enterprise connectivity for the sectors of mining, maritime, railways, defense, and oil & gas
- Rural broadband access that will be in addition to BharatNet and state-led digital initiatives

These kinds of partnerships will not only create new sources of income for the telecom companies but also speed up India's effort to eliminate the digital divide completely.

The Road Ahead: Inclusive, Ubiquitous Connectivity

India is about to experience a revolution in connectivity; however, the country will not be fully able to tap its potential unless all the tech available is used. Mobile networks will still be the primary means of communication in urban and semi-urban areas, while satellite broadband will make digital access available in the furthest and most difficult places of the country. The goal is not to select one option over the other. Rather, the goal is to merge the two to form the best of both worlds, thus ensuring a digital nation that is truly inclusive.

This is precisely where satellite broadband can come in as a game-changer. Satellite systems will not be able to resolve many of the difficulties that are usually found in remote areas that terrestrial mobile networks simply cannot reach, such as rugged terrains, dense forests, or island communities, but they will bridge those gaps by delivering high-speed internet where fiber and cell towers fall short. By complementing 5G rollouts with low-Earth orbit (LEO) constellations like Starlink or OneWeb, India can ensure last-mile connectivity for over 100 million underserved citizens, powering telemedicine in rural clinics, e-learning in tribal hamlets, and digital payments for small farmers.

Konark Trivedi

DKonark Trivedi is the Founder and Managing Director of Frog Innovations Limited (formerly Frog Cellsat Limited), a leading provider of RF equipment and mobile network coverage solutions. With over two decades in telecommunications, he specializes in GSM, wireless technologies, and in-building systems (IBS) for clients like Airtel, Vodafone, Nokia, and Ericsson. He holds a B.Tech in Electronics from Aligarh Muslim University and a Postgraduate degree in Mobile and Satellite Communications from the University of Westminster.

The End of the Smartphone? Form Factor of the Post-Mobile Era

The smartphone has reigned supreme for nearly two decades, a gleaming rectangle of glass and silicon that has become the central nervous system of modern life. It is our portal, our remote control, our bank, our newspaper, and our primary tether to the digital universe. Yet technological evolution is never static.

A convergence of advancements in artificial intelligence, wearable technology, and ubiquitous connectivity (5G and the nascent 6G) is quietly assembling the components for a successor. We stand at the precipice of a post-mobile era, where the smartphone may not disappear, but will likely be supplanted as our primary interface by ambient, context-aware systems woven into the very fabric of our perception and environment.

The Tyranny of the Rectangle

To understand why a shift is inevitable, we must first acknowledge the smartphone's inherent limitations. For all its power, it is a device that demands our attention. We must stop, look down, and plunge our consciousness into a 6-inch portal, divorcing ourselves from the physical world. This creates what technologist Linda Stone called "continuous partial attention"—a state of perpetual distraction. The form factor itself is a bottleneck: a screen-based, app-centric model that requires conscious interaction, whether tapping, typing, or swiping.

The next paradigm promises something fundamentally different: ambient computing. The goal is not to create a more captivating screen, but to make the interface disappear, moving from "pull" (where we seek information) to "push" (where relevant information finds us, seamlessly). This shift is being powered by three synergistic technologies:

Advanced Wearables (The New Form Factor): AI-powered smart glasses, neural wristbands, and even smart rings or earables are evolving from novelties into sophisticated conduits for information. These devices distribute the smartphone's functions across the body in a more intuitive, always-accessible manner.

Ubiquitous Connectivity (The Invisible Grid): 5G's low latency and high bandwidth, evolving toward 6G's potential for sub-millisecond delays and global coverage, provide the always-on, high-fidelity data pipeline necessary for ambient computing. Information can stream to and from wearables instantly, without the need for a phone as a relay.

Context-Aware AI (The Invisible Butler): This is the true brains of the operation. Next-generation AI assistants will not just respond to voice commands but will understand context—where you are, who you're with, your schedule, your biometrics, and even your intent—to proactively offer information and control.

A Day in the Post-Mobile Life

Imagine a day mediated not by a

phone, but by your glasses and a suite of subtle wearables.

You wake up, and the gentle glow of data is projected in the periphery of your vision: the day's weather, your first meeting, and a reminder from your smart ring that your sleep recovery was optimal. As you make coffee, a glance at the pantry highlights the expiring milk. Your AI, aware of your schedule and preferences, has already summoned a rideshare for your optimal departure time—the confirmation subtly displayed in the corner of your lens.

On your commute, directions are laid as a faint, glowing path on the actual street. A notification about a delayed colleague pulses gently; you respond with a glance-activated voice memo. You pass a restaurant, and a small critic's review hovers near its sign, triggered by your gaze. You pay for your transit with a micro-gesture of your finger, authenticated by your ring.

In a meeting, real-time transcripts and translated subtitles appear below the speaker for non-native colleagues. You pull up a 3D data model with a pinch of your fingers in empty space, collaborating with remote participants whose holographic avatars sit around the table. Your phone remains in your bag, a dormant backup battery and processor for more complex tasks.

This is not science fiction. Prototypes of every described element exist in labs at Apple, Meta, Google, and countless startups. The challenge is integration, miniaturization, and social acceptance.

The Form Factors of Disappearance

The post-mobile era will be defined by a constellation of devices, each with a specialized role:

AI Glasses: The likely heir apparent to the visual interface. Advances in waveguide optics, laser-based retinal projection, and microLED displays are solving the classic problems of bulkiness and poor battery life. They will offer layered reality—from simple notifications and captions to full immersive AR—allowing digital information to coexist with, rather than replace, the physical world.

Neural Interfaces & Smart Audio: Wristbands and earpieces will evolve to read subtle electromyography (EMG) signals—the electrical pulses sent to your muscles when you intend to move a finger. You might control your glasses by barely twitching your thumb. Advanced earbuds will conduct bone-conduction audio and monitor vital signs, becoming a health guardian and an invisible audio channel.

The Environment as Interface: With connectivity everywhere, everyday objects become interactive. Your car's windshield, your office window, your kitchen countertop—all can become contextual displays. Your phone's "screen" is dematerialized and redistributed into the world around you, summoned only when needed.

The Challenges: More Than Just Technology

This transition faces monumental hurdles beyond engineering. Privacy becomes paramount. An always-on, always-sensing device that sees what you see and hears what you hear is a privacy nightmare. This will require a revolutionary approach to data, likely emphasizing on-device processing and user-controlled data vaults. Social acceptance of people wearing cameras and displays on their faces is a cultural battle that Google Glass famously lost in its first iteration. The design must become fashion, and the functionality must provide undeniable, non-intrusive value.

Furthermore, we must guard against the dystopian potential. The "attention economy" could become an "experience economy," where our very perception of reality is mediated, filtered, and potentially monetized by corporations. Digital divides could widen into perception divides. The constant stream of information could lead to cognitive overload more insidious than today's screen addiction.

The Smartphone's Enduring Niche

This does not mean the smartphone will vanish overnight, or perhaps ever. Like the desktop computer after the laptop's rise, it will likely recede into a specific, powerful niche. It may become a personal server—a pocketable powerhouse for complex processing, a secure biometric authenticator, or a high-resolution display for tasks that still benefit from focused, rectangular attention: editing long documents, immersive gaming, or watching a movie. The "phone" becomes less a front-end interface and more a back-end hub for our constellation of wearables.

Conclusion: From Device to Ecosystem

The post-mobile era is not about a single device killing the smartphone. It is about the dissolution of the device into an intelligent ecosystem worn on our bodies and embedded in our surroundings. The form factor shifts from a single, monolithic slab to a distributed, ambient experience. The goal is to enhance human capability and intuition, rather than interrupt it with a demanding screen.

The transition will be gradual, messy, and fraught with debate about the very nature of attention, reality, and human connection. But the trajectory is clear. The age of staring down at a glowing rectangle is reaching its twilight. The next age will be about looking up, and seeing a world intelligently augmented, with information and assistance flowing as effortlessly as thought itself. The smartphone's end is not a disappearance, but a quiet fading into the background—a triumph of technology becoming so useful, it finally begins to disappear.

DISRUPTIVE TELECOMS

Enable. Innovate. Transform

Unique Platform for Showcasing Global Innovations and Disruptions in Telecoms

An initiative by TelecomDrive.com