AI in Telecom Networks: Building Intelligent, Secure and Resilient Digital Infrastructure for India

A COAI White Paper

Table of Contents

1. Executive Summary

Artificial Intelligence is often discussed from the perspective of end-user devices: smartphones, applications, chatbots, cameras, assistants and consumer-facing digital services. While these applications are visible to citizens, a quieter and more consequential transformation is taking place inside the telecom network itself.

AI in telecom networks is fundamentally different from AI on end-user devices. Device-level AI improves individual user experience. Network-level AI strengthens the digital infrastructure on which millions of users, enterprises, public services and critical applications depend simultaneously. It helps networks predict congestion, optimise energy use, detect faults, manage traffic, support quality of service, improve cybersecurity and enable faster restoration during failures.

From COAI's perspective, AI-enabled networks are not merely a technology upgrade. They are a strategic requirement for India's digital future. As India moves towards 5G-Advanced, 6G, Industry 4.0, smart cities, digital governance, telemedicine, connected mobility, fintech, public safety and AI-driven enterprise services, telecom networks will need to become more intelligent, automated and adaptive.

Internationally, standards bodies and industry forums are already moving in this direction. 3GPP has embedded AI/ML-related work across 5G system management, core network analytics and RAN intelligence, including functions such as Network Data Analytics Function (NWDAF) - the standardized artificial intelligence (AI) and machine learning (ML) intelligence layer in 5G Core networks defined by the 3GPP. ETSI is developing frameworks for zero-touch network and service management as well as experiential networked intelligence. ITU's IMT-2030 work recognises Artificial Intelligence and Communication as one of the usage scenarios for future networks. O-RAN Alliance work also highlights AI/ML-driven optimisation through RAN Intelligent Controller (RIC), xApps (microservice-based applications running on the Near-Real-Time RAN Intelligent Controller for fast radio network control) and rApps (modular, cloud-native software applications running on the Non-Real-Time RIC within Open RAN architectures to automate, optimize and manage cellular radio access networks), alongside a parallel emphasis on zero-trust security and protection of AI/ML systems in open network architectures.

India must now develop a coherent national approach for AI in telecom networks. This requires regulatory clarity, secure data governance, standards alignment, trusted testing environments, cybersecurity safeguards, skilled manpower, domestic capability development and a policy environment that encourages innovation without creating avoidable compliance uncertainty.

This white paper outlines the distinction between device AI and network AI, the major use cases, the risks, international best practices and the enabling actions required from Government and industry.

2. Background: Why AI in Networks Matters

Telecom networks have evolved from voice-centric infrastructure into the foundation of the digital economy. Today, they support not only calls and messages, but also digital payments, online education, remote healthcare, e-governance, logistics, entertainment, emergency response, enterprise applications and cloud-based services. As it is, telecom networks have evolved to Information & Communications Technologies, Electronics and Cyber (ICTEC) to form a converged mode for a wide range of services to be offered.

With 5G and future 6G networks, this complexity will increase further. Networks will have to support billions of connected devices, ultra-low latency services, massive machine-type communication, private networks, network slicing, edge computing, satellite-terrestrial integration and mission-critical applications.

Traditional network management methods will not be sufficient for this. Manual monitoring, reactive troubleshooting and static network planning cannot fully meet the requirements of future digital services. AI and automation can help facilitating networks move from reactive management to predictive and eventually, autonomous operations.

The objective is not to remove human oversight. The objective is to augment human capability and enable networks to respond faster, more efficiently and more intelligently.

3. AI on Devices vs AI in Networks

A clear distinction must be made between AI on end-user devices and AI in telecom networks.

AI on End-User Devices
AI on smartphones and consumer devices typically supports functions such as image enhancement, voice recognition, language translation, personal assistants, spam filtering, battery optimisation and app-level personalisation. Its impact is usually limited to the individual user or device.

The primary concerns in device AI include user privacy, consent, app security, device performance, explainability and misuse of personal data.

AI in Telecom Networks
AI in networks operate at a different scale and level of consequence. It is embedded into the systems that manage traffic, radio resources, network faults, cybersecurity, service quality, energy consumption, customer experience and network resilience.

AI in telecom networks can influence how capacity is allocated across various geographical locations, how faults are predicted, how congestion is managed, how suspicious traffic is detected, how quality of service is maintained and how critical services are prioritised within lawful and regulatory frameworks.

Therefore, AI in networks is not merely a consumer feature. It is an infrastructure capability.

This distinction is important because the safeguards required for network AI are different. Network AI must be dependable, auditable, secure, interoperable, standards-based, privacy-preserving and resilient against adversarial manipulation. A failure in a device-level AI feature may inconvenience one user. A failure in network-level AI can affect service quality, emergency communications, enterprise operations or critical digital services at scale. Thus, AI in networks would need to be backed by another AI, in case of any sort of failure/rogue manipulation of the same takes place.

4. Key Use Cases of AI in Telecom Networks

4.1 Predictive Network Maintenance

AI can analyse alarms, equipment performance, power behaviour, weather conditions, historical outage patterns and field data to predict faults before they affect consumers. This can reduce downtime, improve restoration time and lower operating costs.

4.2 Dynamic Capacity and Traffic Optimisation

Network traffic varies by time, geography, events, mobility and application usage. AI can help optimise radio parameters, manage congestion, balance traffic between network elements and improve throughput.

4.3 Energy Efficiency

AI can optimise energy consumption by identifying traffic patterns, managing sleep modes and supporting more efficient use of the telecom network resources.

4.4 Quality of Service and Quality of Experience

AI can help correlate technical network parameters with actual consumer experience. This can support better complaint resolution, proactive service improvement and more accurate identification of coverage or congestion issues.

4.5 Cybersecurity and Fraud Detection

AI can assist in identifying abnormal network behaviour, suspicious communication patterns, distributed attacks, spam trends and potential misuse of communication resources. This is especially important as fraud and cyber threats become more automated and sophisticated.

4.6 Tackling issues pertaining to Unsolicited Commercial Communications (UCC)

AI/ML-based network level spam alert services using behavioural parameters such as call volume, call diversity, call duration and series calling can be used as part of the UCC detect systems.

4.7 Network Slicing and Enterprise Services

Future networks will serve different use cases with different performance requirements. AI can help manage slices for healthcare, manufacturing, logistics, smart grids, education and public safety by dynamically allocating network resources.

4.8 Disaster Response and Network Resilience

During floods, earthquakes, public emergencies or major events, AI can help predict network stress, identify vulnerable sites, optimise restoration priorities and support continuity of essential communication services.

4.9 Standards and Operations Support

Generative AI and domain-specific AI tools can assist engineers in navigating complex telecom standards, troubleshooting, configuration management and operational decision support. Research has already shown the potential of LLMs for telecom standards understanding and network operations support.

5. Risks and Governance Challenges

AI in networks must be deployed carefully because **telecom networks are critical infrastructure.** The key risks include:

5.1 Model Drift

AI models trained on historical network behaviour may become less accurate as traffic patterns, devices, applications and user behaviours change.

5.2 Adversarial Manipulation

AI systems can be targeted through manipulated inputs, poisoned data or adversarial attacks. Research on ML-based O-RAN xApps has demonstrated that adversarial manipulation can reduce model accuracy and affect network performance.

5.3 Misconfiguration

Automated systems may create unintended consequences if multiple AI-driven applications issue conflicting policies. Studies on O-RAN have highlighted the need to manage misconfiguration risks in AI/ML-enabled network environments.

5.4 Lack of Explainability

Where AI influences network decisions, operators must have sufficient visibility into why a recommendation or action was taken, particularly for critical or high-impact decisions.

5.5 Data Governance

Network AI depends on large volumes of operational telemetry. This data must be handled with strong controls on purpose limitation, access, retention, anonymisation, aggregation and security.

5.6 Vendor Dependence and Interoperability

AI tools embedded into network equipment and platforms must not create avoidable lock-in or interoperability challenges. Standards-based approaches are essential.

5.7 Regulatory Uncertainty

If regulatory expectations are unclear, operators may hesitate to deploy advanced automation, especially where automated decisions could later be questioned without a clear governance framework.

6. International Best Practices and Standards Direction

Global best practices indicate that AI in networks should be developed through open standards, risk management, controlled automation and security-by-design.

6.1 Standards-Based Network Intelligence

3GPP has recognised AI/ML capabilities across management and orchestration, 5G Core and RAN intelligence. NWDAF, introduced from Release 15, provides a network analytics function for 5G systems. This demonstrates that AI in networks is becoming part of mainstream telecom architecture, not a peripheral add-on.

6.2 Zero-Touch and Autonomous Network Frameworks

ETSI's Zero-touch network and Service Management work focuses on end-to-end automation for future networks. TM Forum's Autonomous Networks framework provides maturity levels from manual management to fully autonomous networks and offers a structured approach for telcos to assess and progress automation capability.

6.3 Cognitive and Experiential Network Intelligence

ETSI ENI is working on cognitive network management architectures using AI, modelling and policy management to improve operator experience and network intelligence.

6.4 Open RAN AI with Security Controls

O-RAN architecture supports AI/ML-driven optimisation through Non-Real-Time RAN Intelligent Controller, Near-Real Time RAN Intelligent Controller, rApps and xApps. Importantly, O-RAN's security work has focused on zero-trust architecture, security requirements for AI/ML and coordinated vulnerability disclosure. This is a useful model: openness and programmability must be matched by security assurance.

6.5 AI Risk Management Frameworks

The National Institute of Standards and Technology's (NIST) AI Risk Management Framework provides a useful structure around governance, mapping, measurement and management of AI risks. Organisation for Economic Co-operation and Development's (OECD) AI Principles similarly stress trustworthy AI, robustness, safety, accountability and risk management across the AI lifecycle.

6.6 AI as a Future Network Capability

ITU's IMT-2030 framework includes Artificial Intelligence and Communication as a future usage scenario, alongside immersive communication, hyper-reliable low latency communication, massive communication, ubiquitous connectivity and integrated sensing and communication. This indicates that AI will be intrinsic to future network design.

7. COAI’s Suggested Principles for AI in Networks

COAI considers the following principles:

7.1 Human-Governed Automation
AI should support increasing levels of automation, but critical network decisions must remain subject to appropriate human oversight, escalation and audit.

7.2 Security by Design
AI systems used in networks must be protected against data poisoning, adversarial manipulation, unauthorised access, model theft and malicious configuration changes.

7.3 Standards Alignment
India needs to align with 3GPP, ITU, ETSI, O-RAN, TM Forum and relevant global cybersecurity frameworks, while also encouraging domestic standards contributions through TEC and TSDSI.

7.4 Privacy-Preserving Data Use
Network AI should primarily rely on operational telemetry, aggregated data, anonymised insights and privacy-preserving analytics. It should not become a basis for intrusive user-level surveillance.

7.5 Explainability and Auditability
High-impact AI decisions must be logged, explainable to an appropriate technical degree and auditable by authorised internal and regulatory mechanisms.

7.6 Risk-Based Regulation
Regulatory oversight should be proportionate to the risk. Experimental, low-impact and internal optimisation use cases should not be treated the same as high-impact automated network control.

7.7 Shared Responsibility
Telecom operators, vendors, cloud providers, cybersecurity agencies, standards bodies, device ecosystems and the Government must work together. AI-enabled network trust cannot be created by any one stakeholder alone.

8. Steps Required to Fortify AI in Networks

8.1 Create Trusted Testbeds and Sandboxes

India needs to create national AI-in-telecom testbeds involving DoT, TEC, TSDSI, academia, startups, vendors and telecom operators.

8.2 Develop AI Model Assurance Protocols

AI models need to be evaluated for accuracy, robustness, explainability, bias, drift, resilience and cybersecurity. Assurance should be practical and risk-based, not paperwork-heavy.

8.3 Build Telecom Data Governance Norms

A clear framework is required for network telemetry, data sharing, anonymisation, retention, access and audit.

8.4 Protect AI Supply Chains

AI-enabled network tools may depend on software libraries, cloud platforms, chips, APIs and vendor systems. Supply-chain assurance must cover the full AI lifecycle.

8.5 Strengthen Incident Reporting

India should distinguish between ordinary network faults, cybersecurity breaches and AI-specific operational incidents such as model failure, harmful automated action or severe model drift. A graded reporting framework can help improve resilience without creating punitive disincentives.

8.6 Develop Skills and Certification

India needs specialised training in AI for radio networks, core networks, cybersecurity, cloud-native telecom, data engineering, automation and network operations.

9. Policy Assurances Required from Government

For AI in networks to succeed, the Government may consider assuring the following:

9.1 Regulatory Clarity
Telecom Operators need clarity on permissible AI use cases, accountability norms, testing expectations and reporting requirements.

9.2 Innovation-Friendly Compliance
AI deployment should not be discouraged by premature or overly prescriptive regulation. A sandbox-based and risk-based approach is preferable.

9.3 Protection of Sensitive Network Data
Any regulatory data requirement must be proportionate, purpose-specific and secure. Network telemetry, configuration data and operational intelligence are highly sensitive and should not be subject to broad or open-ended duplication.

9.4 Standards-Led Approach
Government should encourage alignment with global standards while enabling Indian participation in standards development. TEC and TSDSI can play a stronger role in India-specific profiles.

9.5 Funding for Testbeds and R&D
IndiaAI Mission already aims to support compute access, datasets, application development, future skills and safe and trusted AI.

9.6 Cybersecurity Coordination
DoT, MeitY, CERT-In, NCIIPC, TEC and sectoral regulators should develop coordinated protocols for AI-related telecom network incidents.

9.7 Support for Infrastructure Investment
AI-enabled networks require investment in fiber, data centres, cloud infrastructure, edge computing, secure software platforms, test labs and skilled manpower. A financially healthy telecom sector is essential for such investment.

9.8 Trusted Procurement and Supply Chain Policies
Government should support trusted, secure and interoperable telecom AI solutions while avoiding rules that unintentionally restrict innovation or create excessive dependence on a limited set of suppliers.

9.9 Public-Private Collaboration
AI in networks should be treated as a national digital infrastructure priority. Structured collaboration among the Government, operators, vendors, academia and startups should be institutionalised.

10. Recommended India Roadmap

Phase 1: Foundation

- Define AI taxonomy and risk categories.
- Map use cases across RAN, core, transport, OSS/BSS, cybersecurity and customer experience.
- Establish common terminology for AI in networks.
- Create voluntary baseline guidelines for AI governance.

Phase 2: Test and Validate

- Build national telecom AI testbeds.
- Develop model validation and assurance frameworks.
- Enable controlled trials through regulatory sandboxes.
- Promote indigenous solutions for network optimisation and cyber analytics.

Phase 3: Scale Deployment

- Encourage AI-led predictive maintenance, energy optimisation and QoS enhancement.
- Support interoperable and standards-based AI tools.
- Create incident-sharing mechanisms for AI-related network risks.
- Promote workforce certification.

Phase 4: Autonomous and AI-Native Networks

- Prepare for 5G-Advanced and 6G AI-native architectures.
- Strengthen India’s role in ITU, 3GPP, ETSI, O-RAN and TM Forum workstreams.
- Develop India-specific AI network use cases for rural coverage, disaster management, smart agriculture, healthcare, logistics and public safety.

11. Conclusion

AI in telecom networks is far more than a back-end operational tool. It is an essential capability for the next phase of India's digital growth. Unlike AI on end-user devices, AI in networks operate at infrastructure scale. It can improve service quality, reduce outages, optimise energy, strengthen cybersecurity, enable enterprise use cases and make networks more resilient.

However, the same characteristics that make network AI powerful also require careful governance. It must be secure, auditable, explainable, standards-aligned, privacy-preserving and resilient. India should avoid both extremes: unregulated deployment without safeguards and over-regulation that prevents innovation.

The right approach is balanced and forward-looking: enable innovation, manage risk, protect consumers, secure critical infrastructure and build domestic capability.

From COAI's perspective, AI-enabled networks should be viewed as a national digital infrastructure priority. If India gets this right, it can build networks that do not merely connect people, but intelligently support the economy, governance, enterprises and citizens.

The future of telecom will not be defined only by coverage and speed. It will be defined by networks that can sense, learn, adapt, protect and recover. AI will be central to that future.