Bharat6G Alliance

Bharat 6G Alliance Whitepaper

CAPTIVE NON-PUBLIC NETWORK (CNPN)

Strategic Enterprise Connectivity for the 5G-Advanced and 6G Era



October 2026 | Version 1.0

Bharat 6G Alliance Whitepaper

A Perspective on IMT Spectrum Readiness towards 2030 and Beyond

October 2026

Table of Contents

Executive Summary 5
1. What is a CNPN / Private Mobile Network? 7
2. Why India Needs Private Networks 8
3. CNPN Architecture and Building Blocks 10
4. Deployment and Commercial Models 15
5. Spectrum Requirements and Options 24
6. International Experience and Lessons 26
7. Coexistence, Interference and Spectrum Engineering 30
8. High-Value Indian Use Cases 33
9. Standards, Interoperability and Migration 35
10. Security, Sovereignty, Governance and Compliance 36
11. CNPN as India's 5G-Advanced and 6G Testbed 37
12. Recommended Indian CNPN Framework 39
13. Design in India for Global Leadership 40
14. B6GA Solution Portfolio and Priority 6G Capabilities 41
15. Conclusion 53
Terminology and Short Forms 55
References 60

Executive Summary

A Captive Non-Public Network (CNPN) is emerging as a distinct form of digital infrastructure for enterprises, public agencies and critical sectors. In 3GPP terminology, the broader term is Non-Public Network (NPN). Public mobile networks are optimised for mass-market mobility and national coverage, whereas CNPNs are designed for a defined geography, authorised users and devices, and deterministic service priorities. Depending on the architecture, they can also offer local control of data and the user plane, operational integration and local survivability, where redundant power, transport, core/edge and operating procedures are engineered for it.

For India, the opportunity is unusually broad. Railways, metros, mines, oilfields, ports, airports, utilities, defence locations, disaster zones, tunnels, factories, healthcare facilities and rural clusters often require more than broadband and basic communication. They need mission-critical voice and video, group communications, location services, sensors, public-address systems, SCADA/OT integration, local compute, legacy interworking through standards-based or purpose-built gateways, resilient backhaul and, increasingly, AI-assisted sensing and decision support.

India need not choose between telecom operators and private-network specialists. Multiple deployment architectures can coexist, selected according to the needs of each customer and operational context. Operators bring licensed spectrum, national mobility, managed operations, backhaul, roaming and public-network integration. Enterprises and specialised system integrators bring sector expertise, local ownership, speed and legacy integration, while working with operators where their capabilities and operating models are complementary.

Multiple CNPN deployment models should therefore coexist in India, and the spectrum debate should be framed as a design question: for a given operational requirement, geography, power level and security profile, which access model can produce an investable, accountable and interference-safe network? The model should support diverse operational needs while enabling the optimised use of spectrum as a national resource. Mid-band local spectrum can provide high-capacity geographic reuse, while low-band access can be important where coverage and penetration are the dominant considerations. Operator spectrum, leasing, MORAN/MOCN, APNs, slices and direct/local models can each contribute, depending on the context.

In countries where national authorities are considering dedicated spectrum or comparable arrangements for local industrial networks, the implementation model should be determined by national policy objectives, market conditions, spectrum availability, ecosystem readiness and coexistence requirements. In such circumstances, the real-estate principle — linking priority access to the ownership or tenancy of the relevant premises — could be the preferred approach.

A second strategic proposition is that CNPN can become India's practical testbed for 5G-Advanced and 6G. Bounded enterprise environments make it possible to validate AI-native orchestration, Integrated Sensing and Communication (ISAC), terrestrial/non-terrestrial integration, digital twins, precise positioning, edge intelligence, energy-aware operation and sovereign, auditable AI against measurable operational KPIs.

Priority	Baseline direction
1. Multiple models	Enable TSP-managed, leased, local/private, shared and hybrid routes rather than forcing one architecture.
2. Predictable spectrum	Define candidate bands, coexistence envelopes, application process and pricing sufficiently clearly for investment.
3. Interoperability	Build on 3GPP / MCX / IMS with certified legacy integration, APIs, security and multi-vendor operation.
4. Proof before scale	Use lighthouse deployments to measure operational KPIs, coexistence, TCO and security before hardening rules.
5. 6G-ready by design	Require open APIs, edge/AI hooks and testability so private 5G becomes a platform for sensing, NTN, twins and auditable AI.

1. What is a CNPN / Private Mobile Network?

1.1 Definition and purpose

Private networks are known by different names outside 3GPP. In India, the Department of Telecommunications (DoT) refers to them as Captive Non-Public Networks (CNPNs). A CNPN is a dedicated and isolated terrestrial wireless telecommunications network established by an enterprise for exclusive internal communications within a defined and restricted area, such as a manufacturing plant, refinery or corporate campus. The term "captive" reflects two principles: non-public access, limited to authorised employees, devices and machines; and strict geo-fencing, typically confining the network to premises owned or leased by the authorised organisation. In 3GPP terminology, a CNPN is a Non-Public Network (NPN), realised in 5G primarily as a Standalone NPN (SNPN) or a Public Network Integrated NPN (PNI-NPN). 5G-Advanced extends these capabilities through enhanced slicing, edge computing, industrial applications, mobility and automation, while 6G is expected to enable more programmable, intelligent, highly differentiated and potentially sensing-enabled enterprise connectivity, although its final 3GPP definition is still being standardised.

1.2 CNPN versus a public mobile network

Dimension	Public mobile network	CNPN / Private network
Primary objective	Mass-market connectivity over large territories	Operational outcome inside a defined site, corridor or mission area
Users	General subscribers	Authorised staff, machines, sensors, vehicles and partner agencies
Control	TSP controls network and service policies	Enterprise/agency may control core, applications, policies, data and usage
QoS	Optimised across large consumer traffic mix	Priority, pre-emption and SLA by role/application
Integration	Limited enterprise customisation	Deep integration with IMS/PBX, UHF/VHF, PA, SCADA, legacy telecom, cameras, GIS and workflows
Failure mode	Dependent on operator topology and backhaul	Can retain local service using local core/edge and redundant backhaul
Coverage design	Population and traffic-led	Site, corridor, campus, mine, port, tunnel, border or emergency-led

1.3 The communication-island principle

A CNPN can be defined as a "communication island" bounded by geo-coordinates — the logical perimeter of premises owned or leased by the authorised entity — and multiple locations are permitted. Within the island, radio access, the local core, mission-critical services, command functions and local applications continue to operate and remain fully functional even when the external WAN or backhaul is unavailable. This is directly relevant to disaster response, Accident Relief Trains, tunnels, border posts, mines and strategic sites, where the external network may be absent, damaged or congested.

> **A CNPN should be judged by the operational outcome it guarantees and the use case it addresses, not by its radio technology or ownership model.**

2. Why India Needs Private Networks

2.1 Industrial digitalisation and Industry 4.0

A public telecom operator is typically driven by commercial considerations in which a large number of users pay for uniform services. This is not a criticism but the logic of a consumer business, and it has given India one of the largest and most affordable mobile markets in the world. It does, however, mean that large, high-value and nationally important environments can fall outside the operators' commercial map. The business case for a nationwide operator naturally weakens when services must be customised for a specific user — for example, in the interior of mines, refineries, offshore sites, airside zones, container yards, remote utility corridors, defence locations and rural clusters, where the public network may be unavailable or limited. Expectations of a private network are unique and specialised, each requiring different configurations and third-party interfaces that may not be part of a large telecom operator's DNA. This reflects the economics of a national consumer network rather than any shortcoming of public networks.

CNPN fills the gap where value is concentrated in a known site, process or mission rather than in a large subscriber population. These are custom-designed networks that cater to specific customer requirements, which may not be commercially attractive to a public service provider.

India's industrial digitalisation challenge is not simply one of adding broadband capacity. Modern mines, factories, ports, airports, power systems and railways increasingly require deterministic mobility, machine telemetry, video uplink, control traffic, safety alerts, industrial IoT, local processing and integration with operational technology. These requirements are difficult to deliver consistently through a network designed primarily for mass consumer traffic.

2.2 Critical communications and public safety

Railways, metros, police, fire services, disaster-response agencies, utilities and defence users need communications that continue during congestion or infrastructure failure. Use cases that require group voice/video, priority, pre-emption, emergency calling, GIS-based dispatch, device health monitoring, recording and local command are operational controls rather than optional enterprise features to be served by the public operator.

Many of these are precisely the places where connectivity is not a convenience but a lever of productivity, safety and sovereignty. A steel plant or coal mine that cannot run modern automation, sensing and tele-remote operation is an enterprise running below its potential — and that is the gap CNPN addresses.

2.3 Remote, rural and unconnected areas

India's flagship rural programme, BharatNet, is the largest rural-broadband effort in the world and has connected roughly 2.14 lakh gram panchayats. That is a genuine achievement. But a gram panchayat is not a village, and India has about 6.4 lakh villages. The fibre reaches the panchayat headquarters; the revenue villages, hamlets, farms and clusters around it very largely do not have local broadband. PM-WANI can light up the panchayat, but the surrounding settlements stay dark. Running fibre to all 6.4 lakh villages is neither realistic nor necessary.

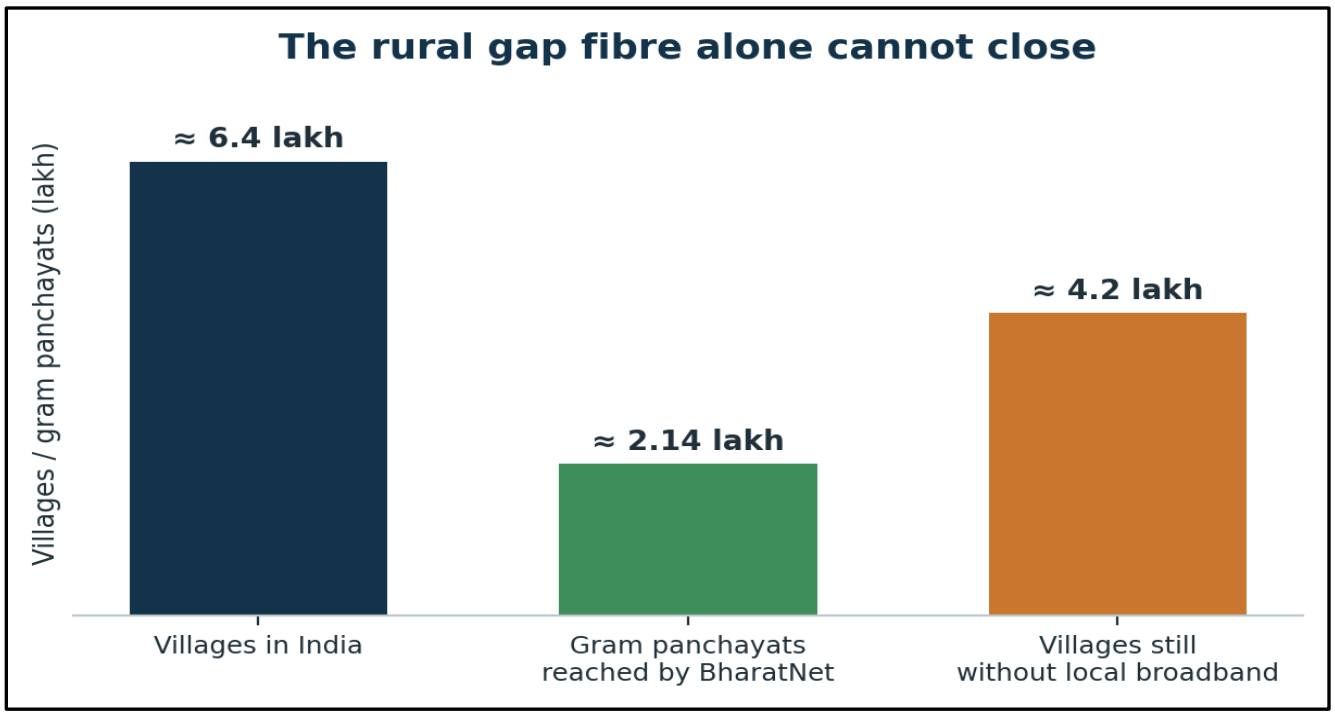


Figure 1 — BharatNet reaches the gram panchayat; the surrounding villages, farms and clusters mostly remain unconnected. Sources: DoT / BharatNet progress statements and Union Cabinet approvals (2023–26). Figures approximate.

CNPN has a strong business case in rural and agricultural clusters. While BharatNet reaches gram panchayats, the surrounding revenue villages, farms, dairy clusters, schools, health centres and cold-chain facilities may still lack local broadband. A locally engineered private or community network can aggregate known demand across a cluster of villages and contribute to the rural economy where a nationwide PLMN is not justified.

2.4 Security, data control and operational sovereignty

Strategic government departments and agencies — such as the Enforcement Directorate (ED), narcotics control and defence — as well as ports, hospitals and other sensitive environments need in-premises hosting of the network, known SIM populations and controlled external interconnection to retain strong operational control. A locally hosted private network can also limit data movement and maintain local services even when cloud or WAN connectivity is degraded.

2.5 A Catalyst for Innovation and Indian IPR

Native AI trained on operational data is potentially Indian IPR that can be protected if all training data is retained on premises. This will become increasingly important with the advent of 6G, which is expected to be natively AI-enabled.

CNPN is a lower-risk environment for customisation and experimentation, and hence provides fertile ground for innovation in 5G-Advanced and 6G. Because the geography, users and traffic are bounded, private networks can be used to develop Indian software, gateways, orchestration, AI, security and sector-specific applications that may not be possible in a far more sensitive public network. That makes CNPN a practical route for creating local IPR and patents as India moves toward 6G.

> **CNPN should be viewed as strategic digital infrastructure for industry, critical operations and innovation, with objectives complementary to public networks — not as a substitute for, or a competitor to, them.**

3. CNPN Architecture and Building Blocks

3.1 The Four Options to Set Up a CNPN

The DoT guidelines notified on 27 June 2022 define CNPN as a network for the captive use of an enterprise inside its own premises, not interconnected with public networks and not offering service to third parties. They set out four ways to establish one:

#	Model (as notified)	Who controls it	Spectrum source
M1	TSP provides a private network as a service over its public network (a slice / dedicated capacity)	TSP	TSP's licensed IMT spectrum
M2	TSP builds a dedicated private network for the enterprise using its own spectrum	TSP	TSP's licensed IMT spectrum
M3	Enterprise leases spectrum from one or more TSPs and runs its own isolated network	Enterprise	Spectrum leased from TSP(s)
M4	**Enterprise obtains spectrum directly from DoT and runs its own isolated network**	**Enterprise**	**Spectrum assigned directly by DoT**

Table 3.1 — The four CNPN routes. M1–M3 run through the operators; M4 is direct assignment.

M1 and M2 are telco-owned and controlled, while M3 may be customer-controlled, with spectrum leased from a TSP on mutually agreed terms; the guidelines avoid heavy conditions such as roll-out obligations or prescribed charges.

For direct assignment (M4), the guidelines require a minimum net worth of ₹100 crore and say DoT will run a demand study and seek TRAI's recommendations before assigning.

> On 23 June 2026, the Department of Telecommunications (DoT) notified the Telecommunication (Authorisation for Captive Telecommunication Services) Rules, 2026 (G.S.R. 511(E)) under the Telecommunications Act, 2023. The Rules make the authorisation side clear and substantially simpler, but spectrum allocation remains unresolved. They provide a dedicated CNPN service authorisation under which an authorised entity may establish, operate, maintain or expand a CNPN within the specified geo-coordinates. Eligible premises have been extended to include leased premises, and multiple locations are allowed as long as no public services are commercially offered. The processing fee is nominal and the authorisation is valid for 20 years. It cannot yet be concluded that the ₹100 crore net-worth requirement has disappeared, since direct spectrum assignment and authorisation are separate issues. Further, as with the 2022 guidelines, the latest policy does not name the bands.

> **The CNPN licence carries no auction cost and only a nominal fee. The applicant must be an Indian company under the Companies Act, 2013 and must own or lease the premises.**

Relevant Facts
February 2025 — TRAI recommended a distinct authorisation for CNPN providers under Section 3 of the Telecommunications Act, 2023, and noted that CNPN services had not picked up in the three years since the guidelines.
30 June 2025 — DoT opened a demand survey, through a module on the Saral Sanchar portal, to identify candidate bands for direct assignment of spectrum to enterprises for CNPN. The survey window closed on 31 July 2025; enterprises with net worth above ₹100 crore were invited to register interest.

Stakeholder Positions
The Cellular Operators Association of India (COAI), on 11 August 2025, opposed direct allocation, arguing India is a "special case" that should not follow international licensing models, citing national revenue, security and interference.
A 2024 GSMA Intelligence study of 51 countries argues that setting aside spectrum for verticals in core mobile bands can threaten the wider success of 5G — including slower roll-outs, worse performance and reduced coverage — lowering average public download speeds by about 25%.

For direct assignment (M4), Section 5.2 sets out why the "real-estate principle" should be the preferred basis for allocating local spectrum.

3.2 Building blocks

Across railway, emergency-response, border, industrial and crowd-management requirements, a common modular architecture emerges. These building blocks remain the same whether the deployment is a fixed campus network, a corridor network, a mine/port network or a deployable Network-in-a-Box (NIB).

Layer	Core components	Operational role
Radio access	Private LTE/5G gNB/eNB; low- or mid-band; indoor/outdoor small cells; portable mast	Dedicated coverage, mobility, QoS and controlled access
Local core	EPC/5GC: AMF, SMF, UPF, PCF, UDM/UDR; local breakout	Authentication, policy, sessions and local survivability
Communications	IMS, VoLTE/VoNR, MCPTT, MCVideo, MCData	Individual/group voice, push-to-video, messaging, files, location and emergency calling
Edge + sensing	Edge compute, VMS, AI analytics, IoT/sensors, drone feeds	Low-latency analytics, event detection and local operation during WAN degradation
Command & control	Dispatcher, GIS, incident dashboard, recording, tasking	Common operational picture and multi-agency coordination
Legacy interworking	LMR/RoIP; UHF/VHF/TETRA/DMR; SIP/PRI/E1; PA; SCADA gateways	Protects installed base and supports phased migration
Resilient backhaul	OFC, microwave, public 4G/5G, satellite/NTN, drone relay	Connectivity to enterprise/HQ with redundancy

3.3 Native AI and orchestration

The architectural direction is moving from static NMS-based configuration toward intent-driven, AI-assisted orchestration. Rather than manually configuring individual radio, core and application elements, operators and enterprises can increasingly express an objective — such as coverage, priority, latency, energy or resilience — and allow the network to analyse telemetry, propose actions and execute them within defined policy controls.

3.4 Network-in-a-Box

A deployable NIB compresses RAN, local core, mission-critical services, edge compute, command functions and resilient backhaul into a rugged system that can quickly create a communication island. The Accident Relief Train concept in this paper is a representative example: local communication and control reside at the incident site, with OFC or satellite links used, when available, to extend connectivity to headquarters.

> **End-to-end concept: Field users / machines → Private RAN → Local 5GC + IMS/MCX → Edge AI / GIS → Enterprise / HQ systems, with legacy gateways and resilient backhaul spanning the chain.**

3.5 6G Migration for Private Networks

As enterprises prepare for 6G, the migration strategy for private networks should be guided by the practical lessons of the 4G-to-5G transition. The experience with 5G demonstrates that offering multiple migration paths can encourage prolonged reliance on transitional architectures. Although 5G non-standalone (NSA) enabled enterprises and communications service providers to introduce 5G radio coverage while continuing to use the 4G core network, it also delayed the move to 5G Standalone (SA) in many deployments.

For private networks, this delay limits the timely realisation of capabilities that are particularly important for industrial operations, including network slicing, advanced quality-of-service control, local traffic handling and support for industrial IoT. It can also leave enterprises managing a fragmented connectivity environment in which legacy systems, transitional 5G deployments and standalone capabilities coexist without a clear long-term architecture. A migration model that is useful as a short-term bridge should not become a permanent constraint on the performance, security and operational efficiency expected from a private network.

For 6G, the preferred approach should therefore be a clear transition towards standalone private-network deployments. The existing 5G Core should evolve to support 6G RAN and 6G user equipment, enabling enterprises to protect their existing core-network investments while avoiding the cost and complexity of maintaining parallel core architectures. This would give industrial users a defined target architecture and a more predictable path for introducing 6G capabilities across campuses, plants, logistics sites and other operational environments.

Dynamic multi-RAT spectrum sharing (MRSS) can provide the necessary flexibility during the transition. By dynamically coordinating spectrum use between 5G and 6G, MRSS can allow private networks to allocate resources according to coverage requirements, traffic demand, criticality of applications and the installed device base. As 6G devices and applications become more prevalent, resources can progressively shift from 5G to 6G without requiring abrupt spectrum refarming or wholesale replacement of the existing private-network infrastructure.

This approach combines architectural clarity with deployment flexibility: a single long-term standalone direction for private networks, supported by controlled 5G–6G coexistence during migration. It can help enterprises preserve current investments while progressively improving reliability, industrial performance and operational efficiency.

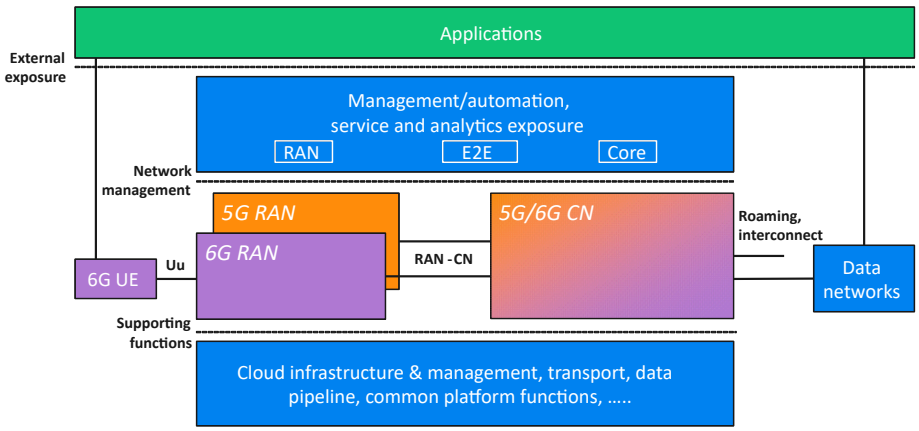


Figure 2 — Proposed 6G architecture, including migration from 5G to 6G

For wide-area networks, migration from 5G to 6G can build on deployed 5G networks. A new 6G RAN can be rolled out, and the 5G core network (CN) can be evolved to integrate the functionality needed to connect 6G UEs via the 6G RAN (see Figure 2). From a spectrum perspective, the 6G RAN can use new spectrum bands, share a band between 5G and 6G via MRSS, or migrate a band from 5G to 6G. 5G UEs connect via the 5G RAN to the evolved 5G/6G CN; 6G UEs connect via the 6G RAN to the same evolved CN, which also includes the new CN functionality required for 6G. Substantial 6G coverage can be provided by applying MRSS with 6G on carriers with good coverage, e.g. in low band.

A similar migration path exists for local private networks. These differ from wide-area networks in that the available spectrum is typically restricted to what is locally available. The migration of a local private network from 5G to 6G is illustrated in Figure 3.

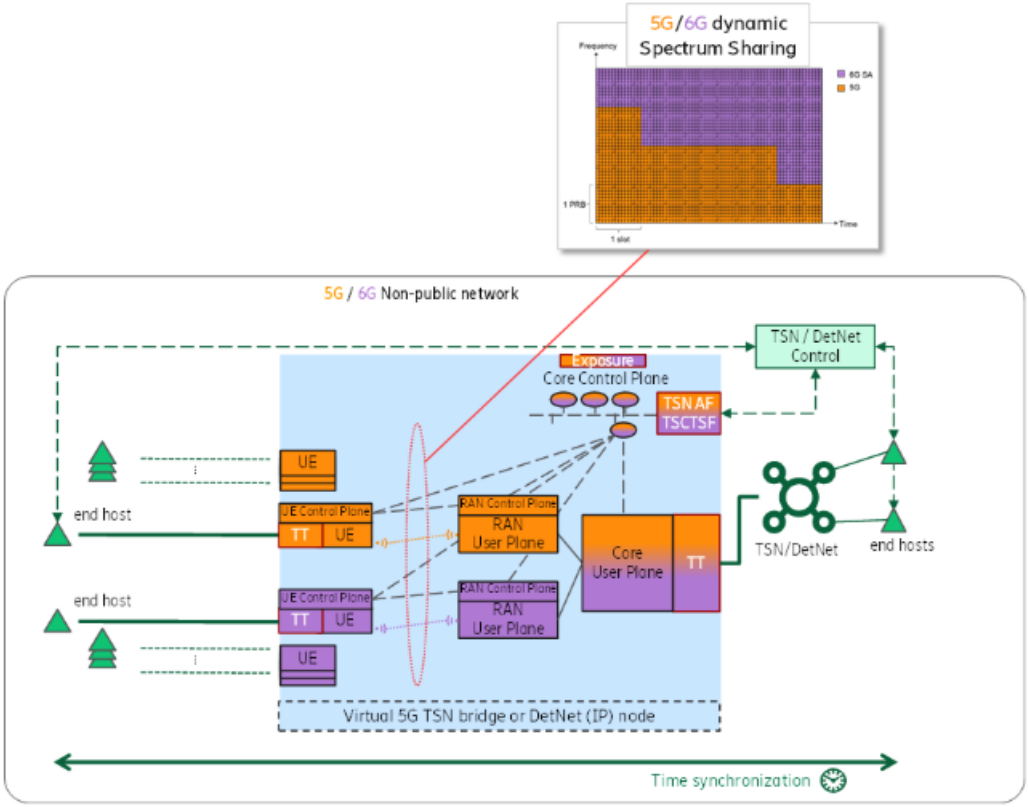


Figure 3 — Migration of a local private network from 5G to 6G using multi-RAT spectrum sharing (MRSS)

In this example, the starting point is a local private 5G network integrated with an IP-DetNet and/or Ethernet-TSN network. A new 6G RAN is then added. The CN comprises the existing 5G CN functionality and is evolved to include the additional functionality required by the 6G RAN and 6G UEs. MRSS is used for the spectrum carriers in the local private network, ensuring that 6G UEs obtain the same coverage as 5G UEs. 5G and 6G UEs can access the network simultaneously: 5G UEs connect to the 5G RAN, while 6G UEs connect to the 6G RAN. Although all UEs connect to a common 5G/6G CN, the functionality provided to them may differ because 6G introduces new capabilities. This enables a smooth migration: deployed 5G devices continue to use 5G with their established characteristics, while new 6G devices take advantage of the novel or enhanced capabilities of 6G.

4. Deployment and Commercial Models

The policy framework should avoid forcing every CNPN into a single ownership, spectrum or commercial structure. Different sites have different requirements for control, capital expenditure, mobility, coverage, security and operational responsibility.

Model	Core / application control	Spectrum / access	Use cases
Fully isolated CNPN	Enterprise / authorised SI	Locally licensed or directly assigned spectrum (set up by SI)	Factories, mines, ports, airports, defence, utilities, campuses, tunnels
Deployable NIB	Enterprise / agency	Local/sectoral/temporary spectrum; portable radio	ART, disaster response, border posts, events, temporary sites
***TSP-managed private network**	TSP with enterprise policy controls	TSP spectrum	Enterprises preferring managed service
MORAN / MOCN (implementation model)	Shared RAN; enterprise may retain services/core	Shared licensed spectrum	Wide campuses, rail/metro corridors, multi-operator environments
APN / network slice (implementation model)	TSP RAN/core with logical isolation	Public network spectrum	Fast rollout, broad mobility and supplementary coverage
Hybrid private + public	Private primary; public fallback/offload	Combination	Railways, utilities, logistics and emergency services

**TSP-managed private networks can leverage a variety of network features and implementation models, such as APN/network slicing and MORAN/MOCN.*

4.1 Flexible Deployment Models and Network Slicing

5G supports three complementary network segments: local dedicated networks, wide-area dedicated networks and general public networks. These segments enable deployment across local, confined wide-area and nationwide environments, serving both enterprise and consumer requirements. For enterprise connectivity, local dedicated networks address bounded industrial or campus environments, while wide-area dedicated networks support distributed operations across corporate sites, utilities, healthcare, public safety, mission-critical services and railways. Wide-area dedicated networks may provide national coverage or operate within a predefined geographical area, depending on the use case. Network slicing, distributed 5G core functions and local user-plane deployment enable service providers to create logically isolated enterprise environments over shared infrastructure, with differentiated quality of experience, security, resilience and traffic policies. This flexible architecture allows enterprises to obtain dedicated network characteristics without necessarily deploying a fully separate physical network, while enabling operators to retain control of the underlying infrastructure and deliver scalable, managed enterprise services.

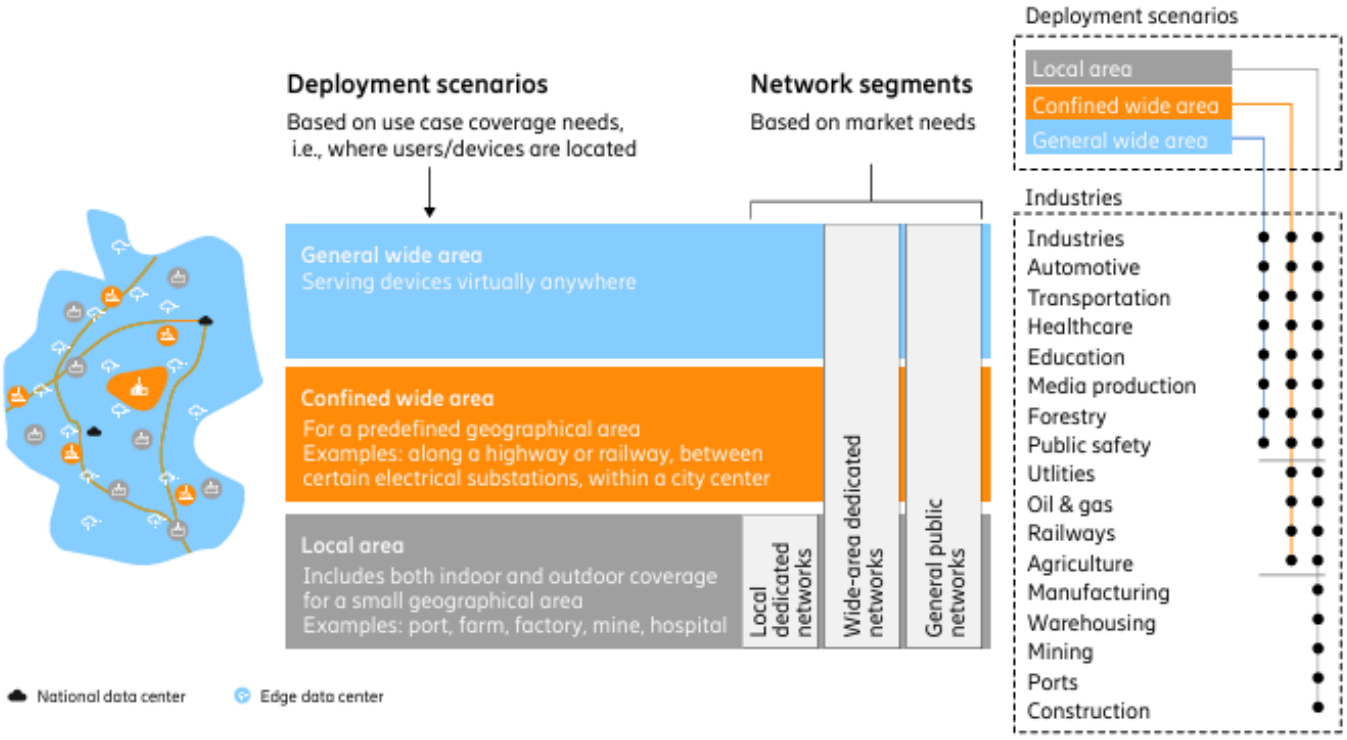


Figure 4 — 5G deployment scenarios and network segments: local dedicated, wide-area dedicated and general public networks

Network slicing as an enabler of differentiated services

Network slicing enables service providers to create logically separated and independently managed networks on top of a shared 5G infrastructure. A slice can be designed to meet the requirements of a particular sector, organisation, or use case while using common underlying network resources.

Network slicing provides a mechanism to differentiate services on both a technical and commercial basis. It can help separate enterprise and public-sector domains, support distinct security and performance policies, and align connectivity services with the requirements of applications ranging from ordinary business communications to critical operational services.

Network slicing does not remove the need for appropriate governance. Effective implementation should include clear service-level commitments, transparent performance measurement, robust security controls, isolation between slices, lifecycle management, and mechanisms for accountability when services support critical national or public-interest functions.

Network APIs and service exposure

By exposing 5G capabilities through standardised network APIs, mobile networks can evolve from connectivity infrastructure into programmable digital platforms for enterprise innovation. APIs enable developers and service providers to integrate capabilities such as quality-on-demand, location verification, silent authentication and device reporting into sector-specific applications. Standards and industry frameworks — including 3GPP, TM Forum, GSMA Open Gateway and CAMARA — help simplify access to network

functions such as the Network Exposure Function (NEF), CAPIF and SEAL. This creates two complementary monetisation opportunities for CSPs: premium subscriptions for differentiated connectivity services and usage-based charging for API consumption, enabling connectivity and network capabilities to generate parallel revenue streams.

A fundamental part of integrating the enterprise network with enterprise connectivity services is the creation of well-designed, enterprise-friendly and standardised service-exposure APIs to the 5G network. On the one hand, these APIs should support enterprise networking services that are common across enterprises; on the other, they should support advanced, customised services that address the specific needs of individual enterprises.

API development should be prioritised through a structured, industry-led process that maps enterprise use cases to defined network capabilities, performance requirements and security needs, and then standardises the APIs with the highest potential for repeatable deployment, cross-industry adoption and measurable business value.

Deployment options for CNPN

Depending on various factors, the deployment can be based on standalone NPN (S-NPN), public network integrated NPN (PNI-NPN) or a hybrid deployment architecture. The factors influencing the deployment architecture can range from use case scenarios and corresponding technical requirements (e.g., indoor vs outdoor deployment, performance requirements, etc.) to regulatory aspects and availability of spectrum.

The first deployment model is a pure standalone NPN (see Figure 5), in which the 5G NPN is deployed as an isolated network. All functions of the 5G network (e.g. RAN and core) are deployed within the logical boundaries of the enterprise, such as a manufacturing site. The network is typically isolated from the public network, and communication with the public network can take place via a firewall if needed.

Deploying a non-public network in conjunction with a public network allows reuse of network infrastructure, efficient utilisation of spectrum and seamless mobility. The network infrastructure can be deployed, in part or in its entirety, inside or outside an enterprise's premises and can be shared between public and non-public users. There are three ways of realising this:

- **Shared RAN:** the RAN is shared between public and non-public users, while the rest of the network's components are kept segregated (all non-public data and control traffic stays within the enterprise's logical premises).
- **Shared RAN and control plane:** a core-network control plane is hosted in the public network in addition to the shared RAN (non-public user data remains local, while control traffic leaves the enterprise's premises, allowing seamless roaming of non-public users).
- **NPN hosted by the public network:** non-public user data leaves the enterprise's premises, while the enterprise still obtains dedicated resources from a CSP's infrastructure (for example, end-to-end dedicated resources across radio, transport and core networks) under a service-level agreement. In this scenario, a CSP can also deploy radio access nodes inside the enterprise's premises for coverage and performance reasons.

Figure 5 illustrates these options alongside the standalone deployment model.

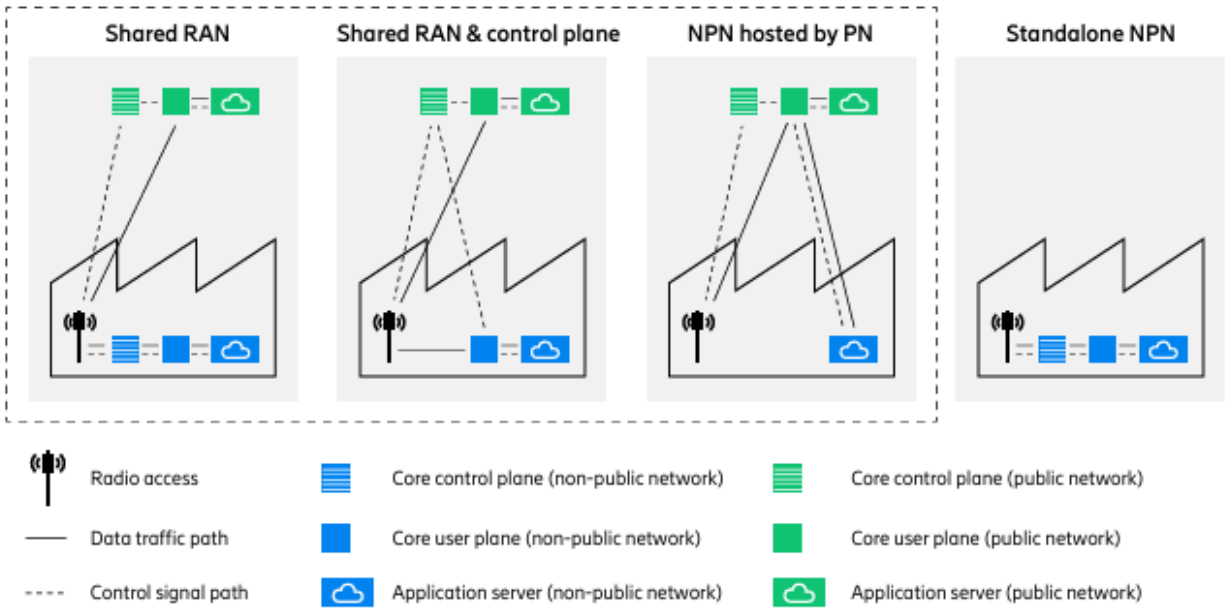


Figure 5 — CNPN deployment options: shared RAN, shared RAN and control plane, NPN hosted by the public network, and standalone NPN

Deployment models and operational models

Beyond the deployment models of 5G NPNs, realising and operating a CNPN requires a good understanding of other, less-explored dimensions, including operational models and business models (Figure 6). Operational models specify the allocation of the roles involved in realising and operating a CNPN — for example, which stakeholder acts as spectrum provider or network operator.

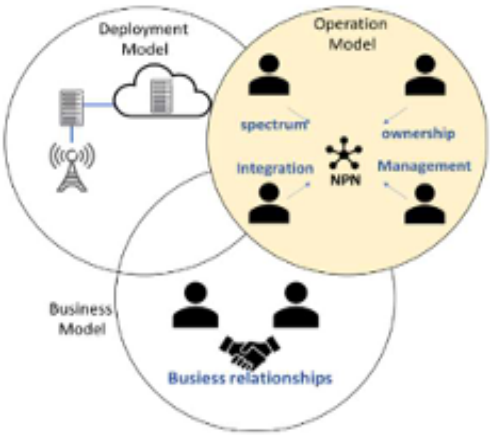


Figure 6 — Different dimensions of CNPN realisation: deployment, operational and business models

To analyse the various aspects of CNPN operational models, we consider the following stakeholders and roles. The stakeholders are: the **CSP**, which owns and manages a public land mobile network (PLMN) and, in the new ecosystem enabled by 5G, also engages in value creation in vertical domains; the **enterprise**, which requests NPN services to perform one or more enterprise tasks; and the **third party**, which provides equipment and/or services for the deployment and management of the NPN and cannot be categorised as either a CSP or an enterprise. The roles are: **CNPN owner**, which owns the CNPN infrastructure, including hardware and software components; **spectrum owner**, which holds the right to transmit radio signals in a given

frequency band; **CNPN integrator**, which sets up the CNPN according to the chosen architecture and makes it ready for use; and **CNPN operator**, which runs the network.

A specific mapping of roles to stakeholders defines an operational model. Except for the role of NPN user, which is always assigned to the enterprise, every role can be taken by any of the three stakeholders, so in theory dozens of distinct operational models could exist. A set of prime examples is listed in Figure 7.

	NPN Owner	Spectrum Owner	NPN Integrator	NPN Operator
OM1	Enterprise	Enterprise	Enterprise	Enterprise
OM2	Enterprise	Enterprise	CSP	CSP
OM3	Enterprise	Enterprise	3rd Party	3rd Party
OM4	Enterprise	Enterprise	3rd Party	CSP
OM5	CSP	Enterprise	CSP	CSP
OM6	CSP	CSP	CSP	CSP
OM7	3rd Party	Enterprise	CSP	CSP
OM8	3rd Party	Enterprise	3rd Party	3rd Party
OM9	3rd Party	CSP	CSP	CSP
OM10	3rd Party	CSP	3rd Party	CSP

Figure 7 — Examples of CNPN operational models (OM1–OM10): allocation of the owner, spectrum, integrator and operator roles

Figure 8 illustrates examples of potential relationships between deployment models and technical realisations/operational models.

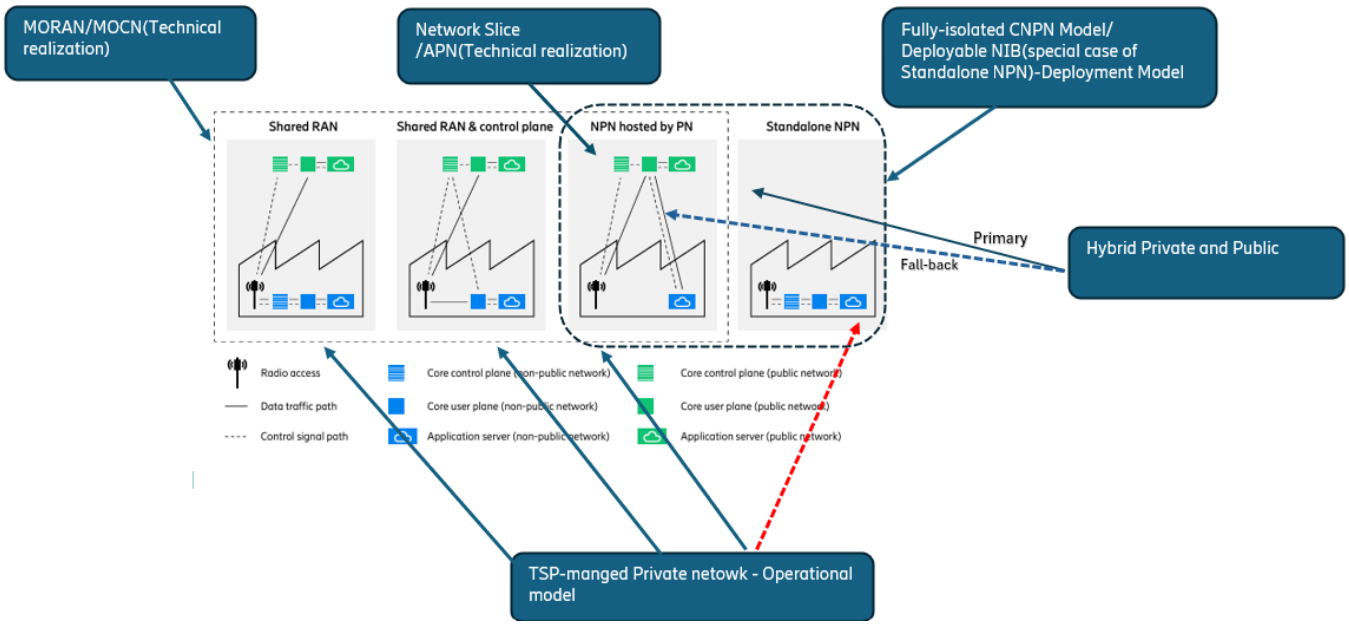


Figure 8 — Mapping deployment models to technical realisations and operational models

4.2 Role of CSPs in the CNPN Ecosystem

As the operational models in Section 4.1 show, CSPs are critical actors in the CNPN ecosystem.

A CNPN is the cellular-era equivalent of a privately controlled enterprise communications system or PABX. It is a complementary product that can expand, rather than reduce, demand for TSP backhaul, leased lines, mobility, spectrum leasing, security, managed operations, APNs, slices and public-network fallback.

A well-designed private-network framework will expand enterprise telecom spending as the solution adds value for the customer. Part of this additional spend will flow to telecom network operators, which provide backhaul, public mobility, roaming, security, hosted core, managed operations, leasing and network integration.

Operator role	What the enterprise may continue to buy
Managed private 5G	Design, build, operate and maintain the network as a service
Core and slicing	Hosted core, APN and slice services
Nationwide mobility / roaming	Handover between private sites and public networks
Backhaul	Fibre, leased line, microwave and satellite connectivity
RAN sharing	MORAN/MOCN for wide campuses and corridors
Spectrum leasing	TSP spectrum under enterprise/private arrangements
Security / operations	SOC, lawful-interception interfaces, patching and 24×7 support

Operator-led models emphasise national mobility, managed operations, spectrum portfolios and security. Enterprise- or SI-led models emphasise site-specific engineering, speed, local control and specialised applications. The framework should encourage both and give customers the flexibility to choose what suits them best.

4.3 What has moved since 2022

When the CNPN guidelines were written, two honest doubts hung over private 5G in India: the mid-band device ecosystem was thin, and private networks were expensive and unproven. Domestically designed solutions were also unavailable. None of these doubts survives the 2026 evidence.

Several Indian design companies, such as Tejas, Lekha, Galore, Signalchip and Coral, have designed and deployed private networks in India. Over 26 system integrators are registered with BSNL to provide CNPN services, and some Indian design companies have set up 5G public networks with BSNL in Delhi, Chennai and other states.

Another sign of maturity is device support for the exact band India is examining. As of March 2026, GSA identified 2,909 announced 5G devices supporting band n77 (3.7 GHz) — essentially level with mainstream public 5G bands such as n78 (3.5 GHz, 3,281 devices) and n1 (2.1 GHz, 2,932 devices). There are now 4,256 announced 5G devices in total, up 24% in a year, with published band support for over 93% of them. The 3.7–4.2 GHz ecosystem — radios, cores, modules, routers and industrial CPEs — is no longer emerging; it has arrived.

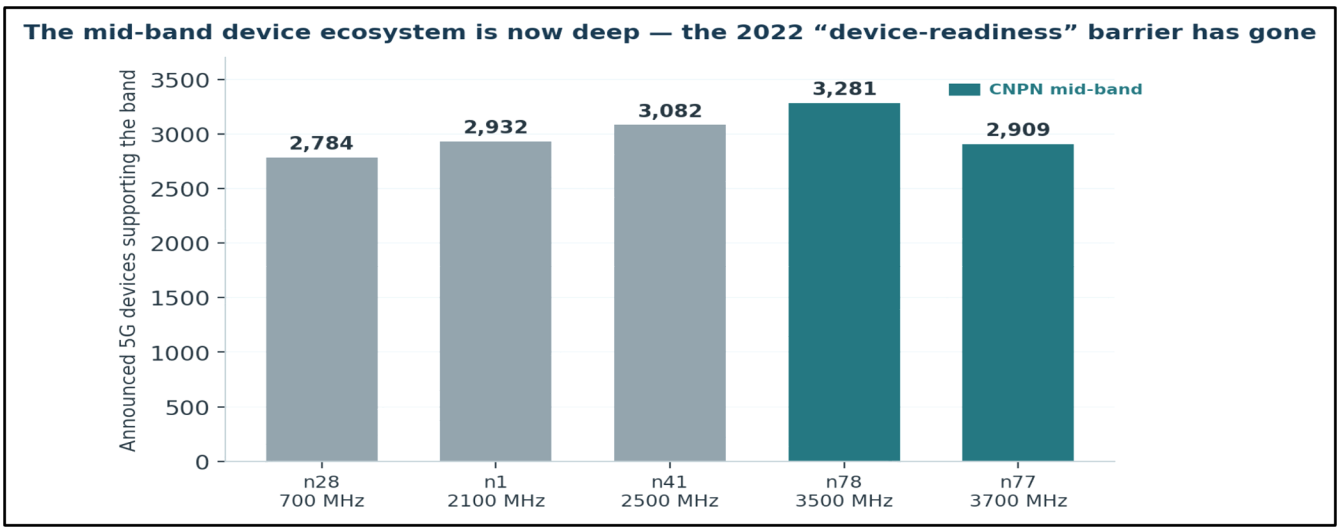


Figure 9 — Announced 5G devices by band. The CNPN mid-band n77 (3.7 GHz) now enjoys device support comparable to the mainstream public bands. Source: GSA State of the Market, March 2026.

4.4 Addressable Market Opportunity

Enterprise digital decision-makers identify operational efficiency as the leading business outcome expected from investment in advanced connectivity as part of their digital-transformation strategies. Among enterprises that have adopted advanced connectivity, 77% reported an improvement of between 11% and 50% in their efficiency metrics. According to GSA's 2026 data, private-network deployments have expanded to 2,003 organisations in 88 countries, a 37% compound annual growth rate since 2019 (Figure 10). Manufacturing is currently the leading adopter, reflecting the sector's demand for secure, deterministic and scalable connectivity to support automation, connected operations and Industry 4.0 applications.

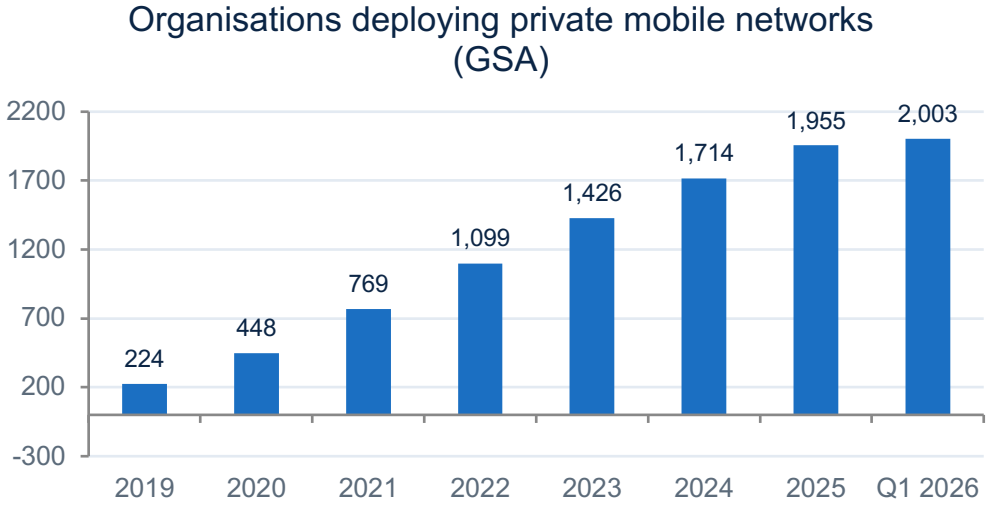
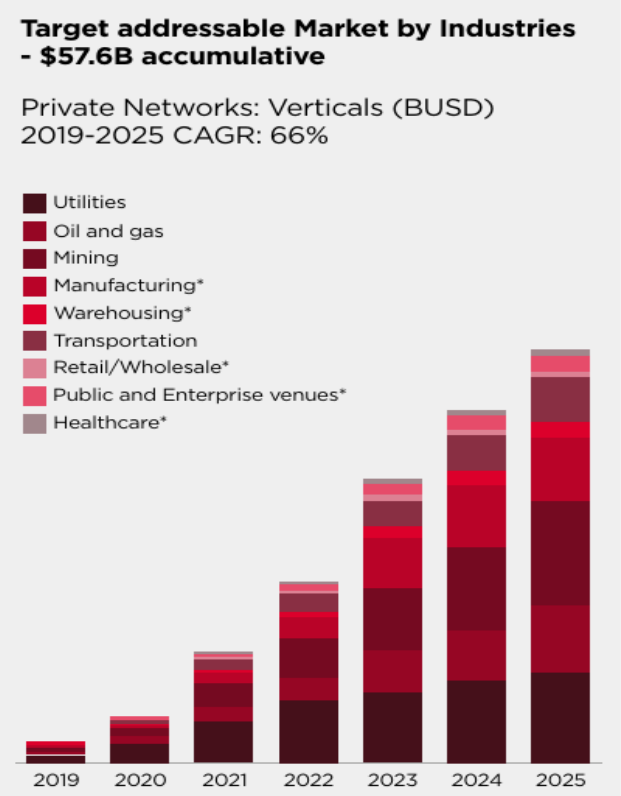


Figure 10 — Organisations deploying private mobile networks worldwide (customer references > €100k), 2019 to Q1 2026. Source: GSA.

Figure 11 indicates that manufacturing will be a significant user of private networks, both in the revenue generated and in the cost savings that 5G private networks deliver.



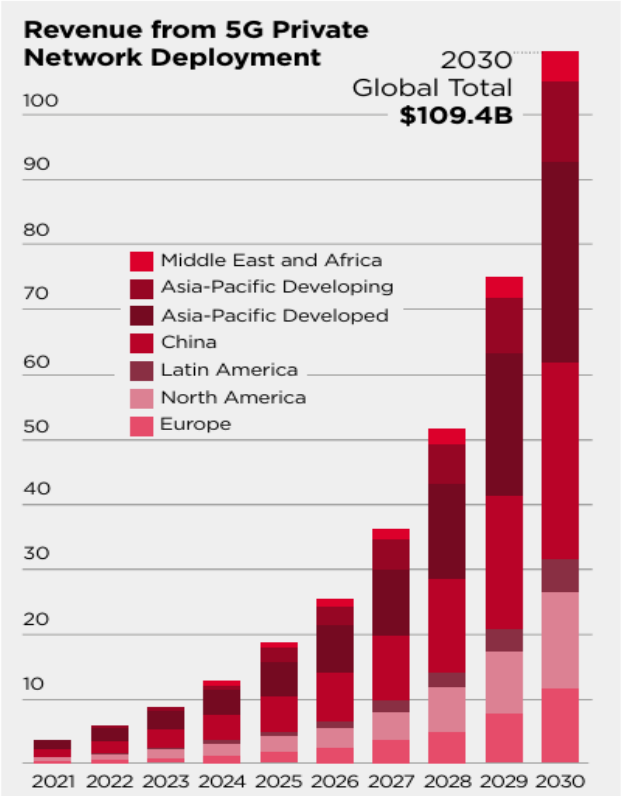


Figure 11 — Target addressable market for private networks by vertical (2019–2025) and revenue from 5G private network deployment by region (to 2030). Source: GSMA.

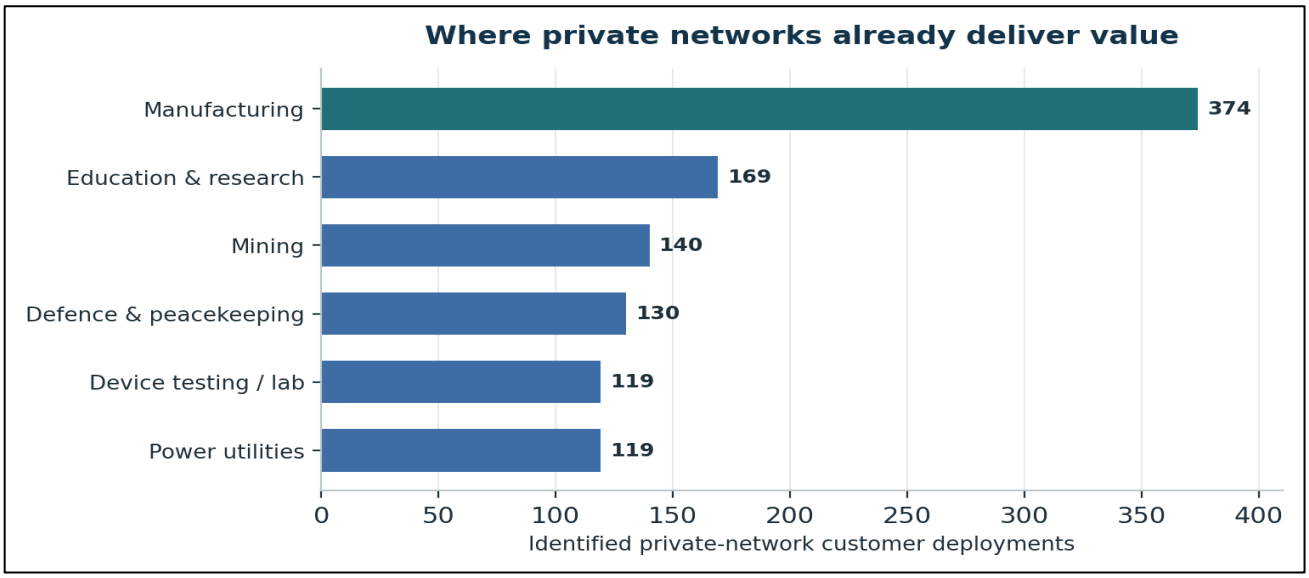


Figure 12 — Identified private-network deployments by sector worldwide. The leading sectors mirror India's PSU and industrial base. Source: GSA, March 2026.

The fastest-growing private-network sectors — mining, ports, manufacturing and utilities — are shifting their operational traffic to private 5G rather than Wi-Fi. The gain is not headline speed; it is a network on which the enterprise can build its processes: a haul truck that holds its control link across the whole pit, a crane driven remotely with millisecond latency, a safety alert that is guaranteed to arrive, and cameras and sensors whose uplink does not collapse under load. Each is a productivity or safety improvement that Wi-Fi, by design, cannot deliver reliably at industrial scale.

4.5 From 5G to 6G: A Framework Where India Can Lead

The 3GPP roadmap prescribes a smooth transition from 5G to 6G. A network built today on a 5G SA core in 3.7–4.2 GHz (candidate band) need not be ripped out when the next generation arrives. It will evolve from 5G to 5G-Advanced (3GPP Releases 18–20), adding native AI, RedCap for low-cost devices, high-precision positioning and integrated sensing, and then to 6G/IMT-2030, building on the same core, the same spectrum and the same investment. The upgrades come largely through software and standards, not forklift replacement.

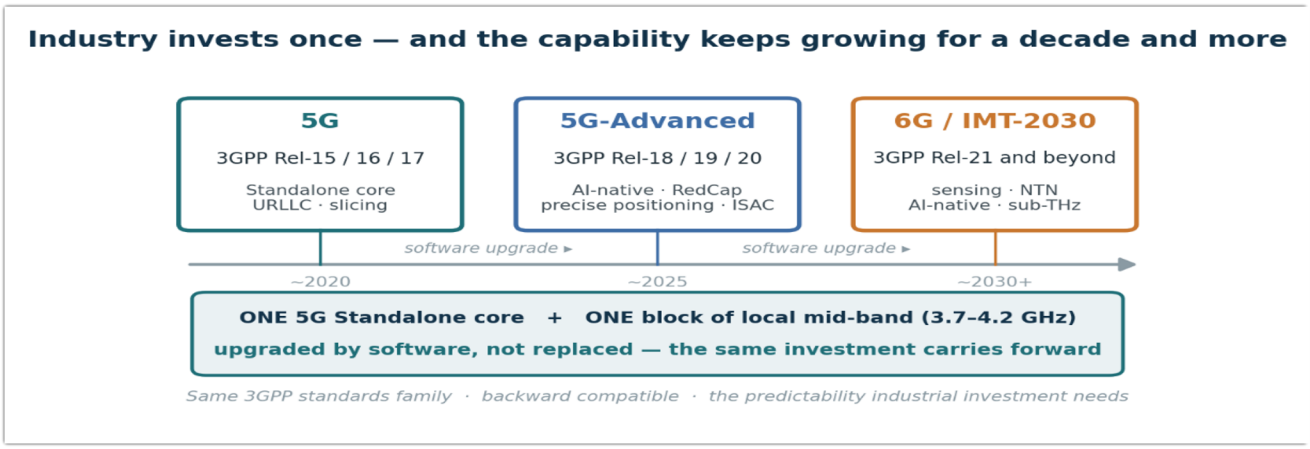


Figure 13 — The 5G-to-6G path is an evolution, not a replacement, providing the multi-decade predictability that industrial investment requires.

Stakeholders: Government, System Integrators and Customers

A CNPN framework in a part of the 3.7–4.2 GHz **(candidate band)** is future-proof: the same assignment that serves 5G today becomes the platform for 5G-Advanced and 6G, so the policy need not be rebuilt every generation. Predictability is precisely what unlocks private investment: enterprises can commit to decade-long digitalisation programmes because the standards, the spectrum and the device ecosystem are on a known, internationally governed path. For the same reason, private networks are India's natural 6G testbed — bounded, measurable environments in which indigenous 6G capability can be developed and proven ahead of the global standard.

5. Spectrum Requirements and Options

5.1 Coverage layer and capacity layer

Spectrum policy must ensure that CNPN becomes deployable infrastructure that is useful to end customers, rather than remaining a laboratory concept. This paper proposes a layered logic: low band where coverage, penetration and site economics dominate; mid band where capacity, compact cells and geographic reuse dominate; and higher bands for hotspot throughput and machine-vision/XR-style applications (Figure 14).

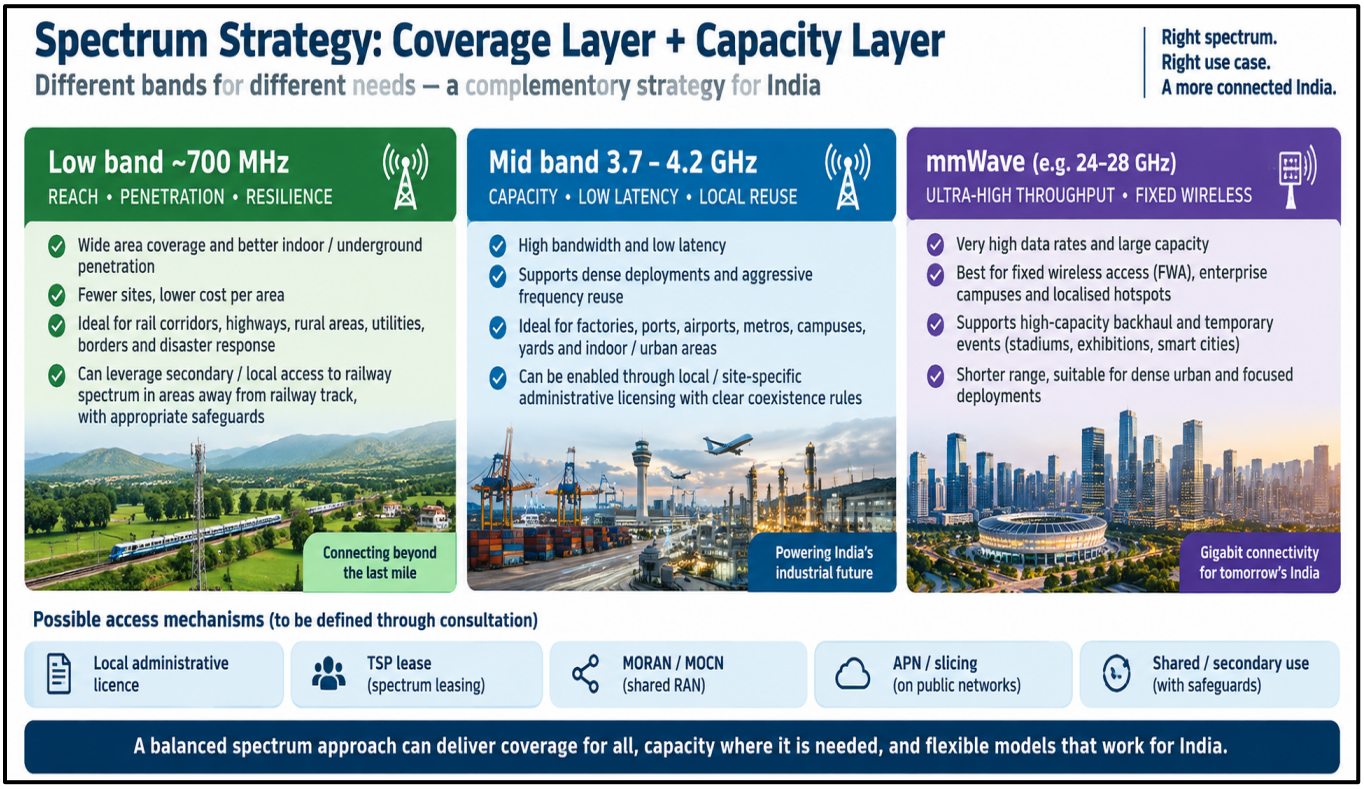


Figure 14 Candidate bands : Secondary use of low band in coordination with primary assignee, small chunks in mid band 3.7 to 4.2 GHz in coordination with other users and small chunks in mmWave.

5.2 Navigating Spectrum Pathways

The CNPN authorisation rules of 23 June 2026 have made the authorisation side clear and substantially simpler, but spectrum allocation remains unresolved. Spectrum may be locally licensed, leased from a TSP, shared on a MORAN/MOCN basis or made available through controlled secondary use; the chosen option should match the footprint, power, incumbent exposure and strategic importance of the use case.

TSPs (CSPs) are well-positioned partners for industry, with several strengths to win enterprise business under options M1–M3. For M4, the "real-estate principle" should be the preferred principle to apply. In short, this links a priority right to acquire a local licence or lease to ownership (or tenancy, depending on national prerequisites) of the relevant real estate. The principle meets three important requirements:

- Access to spectrum must be predictable over a long period to support uninterrupted operation and major investment in production processes and industrial facilities, which typically have a lifecycle of 15–20 years.

- Schemes awarding excessive first-mover advantages should be avoided, so that industries or other players cannot block spectrum through hoarding and late entrants are guaranteed the possibility of acquiring local spectrum.
- Local spectrum not yet licensed or leased to industries should remain available to spectrum licence holders (such as TSPs) to increase utilisation efficiency, with a sufficient safety margin to ensure that existing local networks are not subject to interference.

5.3 Spectrum Assignment

Local networks can reuse the same frequencies across thousands of geographically separated sites, which is fundamentally different from a nationwide assignment. Local spectrum should therefore be evaluated in terms of reuse, coexistence and productive utilisation rather than only through national auction economics.

> **India must decide on the combination of bands and access mechanisms that provides the highest industrial and strategic value while building synergy with telecom service providers and encouraging innovation.**

6. International Experience and Lessons

Advanced economies use a range of private-network models rather than one universal template. The common pattern is local or sector-specific access, predictable administrative rules, engineering-based coexistence and continued participation by telecom operators.

Some countries have allocated spectrum dedicated to industrial use through various regulatory frameworks, whereas others have not. Three broad approaches have been taken:

- Identification of dedicated licensed spectrum for private networks, e.g. the principles applied in Germany and Sweden, among others.
- Identification of spectrum with a leasing option that enables CSPs to lease spectrum to private network operators, e.g. Finland and the Czech Republic.
- No identification of spectrum for private networks, leaving the private-network segment to be addressed by CSPs and their spectrum assets.

The main lessons are summarised below:

Country / region	Band / model cited in source papers	Key feature / lesson
Germany	3.7–3.8 GHz local licensing	Published local licensing and transparent fee formula; industrial/campus focus
United Kingdom	3.8–4.2 GHz Shared Access	Low- and medium-power shared access licences; simple, low-cost online application
Norway	3.8–4.2 GHz local licensing	Low- and medium-power licence classes; per-site coexistence engineering
United States	3.55–3.7 GHz CBRS	Three-tier coordinated sharing via Spectrum Access Systems
Japan	4.6–4.9 GHz / 28 GHz Local 5G	Premises-based local licensing and strong industrial use
South Korea	4.7 GHz / 28.9 GHz e-Um 5G	Site-specific industrial private networks
Finland	Local licences + operator leasing	Multiple routes coexist; operator and enterprise models both supported
Canada	3900–3980 MHz non-competitive local licensing	Published local licensing aimed at enterprises, communities and rural users
China	Operator-led private networks	Very large scale, supported by state direction and funding

6.1 What workable regimes have in common

- Licences are geographically restricted rather than national.
- Pricing is generally administrative, formula-based or flat-fee rather than a national auction construct.
- Applications are handled through defined technical envelopes and, in many regimes, online processes.

- Coexistence is managed through guard bands, power limits, exclusion zones, or per-site calculation.
- Operators actively participate in managed networks through leasing, backhaul, security and integration.

6.2 Global Roadmap: 3.8–4.2 GHz Is Being Harmonised

India is considering this band for CNPN, and it is well tried and widely implemented globally. The upper C-band is where the world is converging for local and vertical use: in the United States, the regulator is planning to auction 3.98–4.2 GHz, and Europe is formally harmonising the whole 3.8–4.2 GHz range for local networks.

Several of the world's most advanced economies have run private networks for years. This paper highlights the two case studies most useful to India: Germany, for its transparent pricing, and Norway, the most instructive of all on coexistence. The list keeps growing: Canada opened local licensing in 3900–3980 MHz in 2024 under a framework aimed squarely at smaller users and rural areas — further evidence that the settled international direction is towards, not away from, local access.

6.3 The International Landscape

Country / band	Regulator & model	Geography & term	Who applies / operator role	Adoption
Germany 3.7–3.8 GHz; 24.25–27.5 GHz	BNetzA. Local licence, administrative formula.	Site/area; up to 10 yrs (renewable to 2040).	Enterprises with rights to the land; operators serve enterprises separately.	431 local 3.7 GHz licences by Nov 2024. Automotive, chemicals, logistics, ports.
Norway 3.8–4.2 GHz	Nkom. Local licence, flat annual fee.	Two types: low-power site licence (indoor or outdoor, 50 m-radius area) and medium-power per-base-station licence for wide-area outdoor use; up to 10 yrs.	No restriction on applicant; standalone only.	Coexists with operator 5G. Energy, offshore, aquaculture, ports.
United Kingdom 1800/2300 MHz, 3.8–4.2 GHz, 26 GHz	Ofcom. Shared Access Licence.	50 m radius (low-power); flexible term.	Any person or business; online, 4–8 weeks.	Among the cheapest and simplest; strong SME/vertical uptake.
Canada 3900–3980 MHz; 26/28/38 GHz	ISED. Non-Competitive Local Licensing (NCL); automated, first-come.	Low-power ≤15 km²; medium-power 75–165 km² (rural); 1-yr, renewable.	Enterprises, verticals, rural ISPs and communities; no auction.	Explicitly aimed at smaller users and rural / remote areas (opened 2024).

Country / band	Regulator & model	Geography & term	Who applies / operator role	Adoption
United States 3.55–3.7 GHz (CBRS)	FCC. Three-tier shared access via SAS.	PAL by county (10-yr); GAA licence-exempt.	Anyone on GAA; PALs auctioned. Operators, enterprises, neutral hosts.	285,000+ CBRS devices by late 2022; mostly GAA-based.
Japan 4.6–4.9 GHz; 28 GHz	MIC. "Local 5G" licence.	Premises; 5-yr.	Local entities only; operators excluded from holding.	Strong manufacturing / logistics base.
South Korea 4.7 GHz; 28.9 GHz	MSIT. "e-Um 5G".	Site-specific; since 2021.	Enterprises and specialised providers.	Deliberate industrial-digitalisation drive.
Finland 2.3 GHz; 3.4–3.8 GHz	Traficom. Local licence + leasing mandate on operators.	Local areas.	Enterprises via local licence or mandated operator lease.	Leads Europe on 5G speed while enabling local access.
China	MIIT. Operator-led; slicing & managed services.	National operator spectrum, used locally.	Operators deliver; no direct enterprise assignment.	Very large scale — with state direction and funding.

Table 6.1 — Local/private-spectrum frameworks in the major economies. Bands and terms are regulatory facts; adoption is an observed outcome.

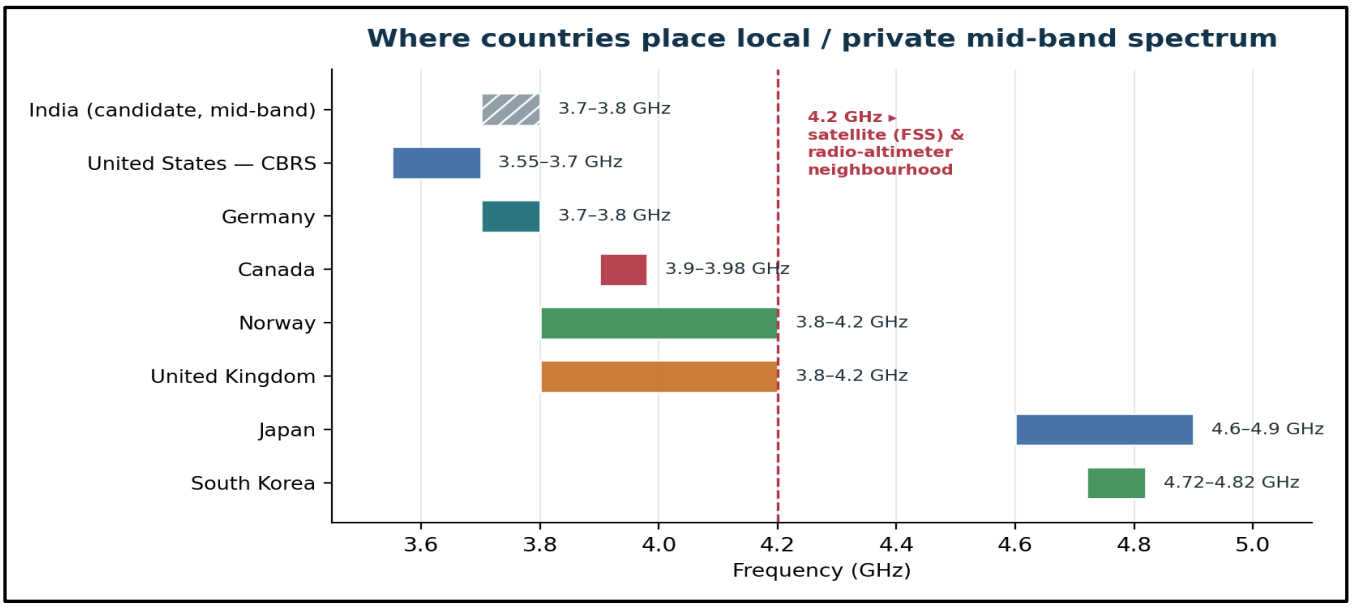


Figure 15 — Where countries place local/private mid-band spectrum. Most local bands sit at or above 3.7 GHz; India's candidate band is under DoT's demand survey, and 3.8–4.2 GHz is now being harmonised across Europe (ECC Decision (24)01).

6.4 A Closer Look at Germany

Germany opened the 3.7–3.8 GHz band for local networks in 2019 and had issued 484 licences by February 2026. The main features of the German licensing framework are:

Licensed area: property-based

Power: negotiable, with a fallback value

Main use cases: Industry 4.0 / IoT

Network planning: by the applicant

QoS guaranteed: yes

Synchronisation: negotiable

Licence term: 10 years, extendable, but not beyond 31 December 2040

Countries offering spectrum for private networks have a similar fee structure, which gives applicants a cost indication in advance. The German framework includes a published formula for calculating the fee:

EVIDENCE

Fee (€) = $1000 + B \times t \times 5 \times (6 \cdot a_1 + a_2)$, where B = bandwidth in MHz (10–100), t = term in years, a_1 = settlement/traffic area (km^2), a_2 = other area (km^2).

For a 100 MHz, 10-year licence over a typical factory footprint this works out to only a few thousand euros for the whole term — a rounding error against the cost of the network itself, and, crucially, a number the enterprise can know in advance.

The German record also carries a caution that India should take in the right spirit: opening a band does not, by itself, create demand. Germany's licence framework was targeted at its industrial base. The lesson for India is to pair a spectrum framework with demand-side measures — lighthouse pilots, PSU adoption and integrator development — that turn a permitted band into deployed networks.

7. Coexistence, Interference and Spectrum Engineering

7.1 Incumbents in and around the candidate band

For private-network deployments that support industrial automation with high reliability and availability, coexistence with other deployments — both macro (public) networks and other local private networks — is essential. Private-network spectrum may be co-channel in geographically separated areas or adjacent-channel in the same or different areas, so appropriate coexistence measures are needed to prevent interference. These measures depend on the frequency band, propagation characteristics, channel relationship, separation distance and mitigations such as building-wall loss, clutter and indoor/outdoor deployment.

For TDD, synchronisation and aligned uplink/downlink patterns are key. Public macro networks often use downlink-heavy patterns, such as a 4:1 DL:UL ratio, whereas industrial applications typically have more balanced traffic and greater uplink demand. A more balanced TDD pattern may therefore be preferable, with alignment maintained across same- and adjacent-band deployments where feasible.

India's upper C-band is not empty. Public 5G occupies auctioned spectrum below the candidate CNPN range, while fixed-satellite-service earth stations and aviation systems must be protected through technical rules. A CNPN framework must therefore be based on measured coexistence, not on an assumption of vacant spectrum.

7.2 Engineering tools

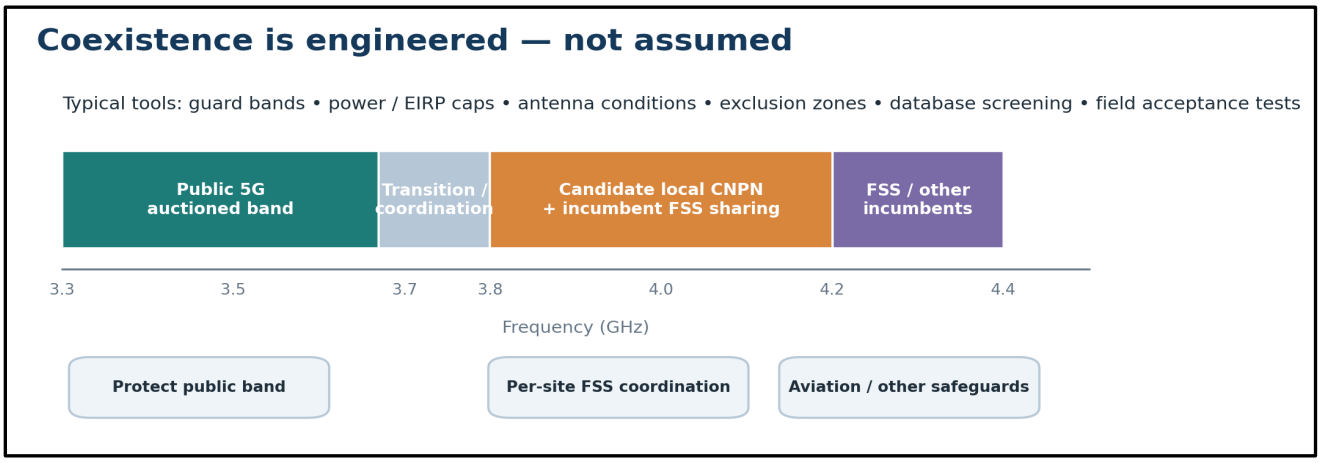


Figure 16 — Candidate CNPN spectrum can be managed through guard bands, power limits, incumbent screening and site-specific coordination.

Tool	Purpose
Guard bands	Separate adjacent services where receiver selectivity or emission limits require additional margin
Power / EIRP limits	Bound interference footprint by licence class and environment
Antenna height / tilt / orientation	Reduce unwanted radiation toward protected receivers and outside the authorised area

Tool	Purpose
Exclusion / coordination zones	Trigger additional review around airports, earth stations and other sensitive sites
Per-site calculation / database	Test the proposed transmitter against known incumbents before grant
Field acceptance testing	Measure actual emissions, propagation and incumbent impact after installation
Remote retuning / shutdown	Provide a rapid operational remedy if interference is detected

7.3 Coexistence Is Engineered: Norway's Approach to Safe Local Mid-Band

The European Union and CEPT share a framework for local-area network connectivity in 3.8–4.2 GHz (see Key Primary Sources). CEPT also provides recommendations for the protection of the fixed service (FS), fixed-satellite service (FSS) and radio altimeters. On this basis, countries in Europe have begun making spectrum available. The Norwegian approach is described below.

The concern raised most often against opening 3.8–4.2 GHz — interference with satellite earth stations below and above the band, and with aircraft radio altimeters near airports — is legitimate and must be taken seriously. But it is a solved class of problem. Norway shows both how the rules are written and, unusually, that they have been tested against real aircraft.

Nkom licenses local networks across 3.8–4.2 GHz and manages coexistence through explicit, per-application engineering rather than exclusion:

- **A 40 MHz guard band** (3800–3840 MHz) protects public mobile below 3800 MHz.
- **Per-site satellite calculation:** Nkom runs a coexistence calculation against fixed-satellite earth stations before each grant.
- **Aviation protection:** pending international altimeter studies, medium-power outdoor use is kept to the lower half of the band, and sites near airports and heliports get case-by-case power, placement and height conditions.
- **Two licence types for two kinds of deployment:** a low-power site licence — indoor or outdoor, over a 50 m-radius area with unlimited base stations — for campuses and buildings; and a higher-power, per-base-station medium-power licence for wide-area outdoor use such as ports, offshore, aquaculture, energy and industrial sites, kept clear of large urban settlements (with exemptions for ports and industrial areas). Norway is not a 50-metre indoor-only regime — its signature deployments are outdoor and wide-area, and the fixed-radius construct simply lets Nkom make reliable interference calculations while packing many users into a geography.
- **Managed identity:** each private network gets mobile network codes under Norway's country code, so it is traceable and manageable.

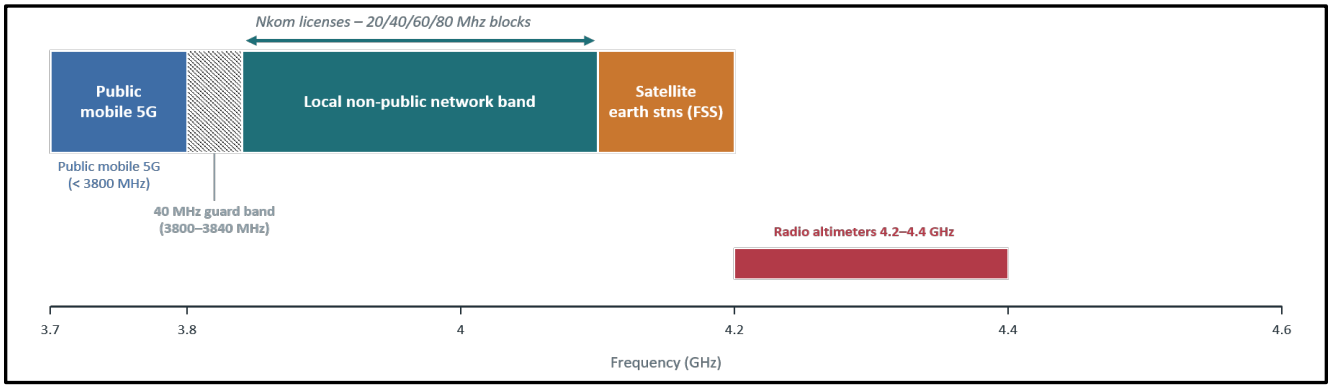


Figure 17 — Norway's 3.8–4.2 GHz band plan: public mobile, the local band, satellite earth stations and aircraft altimeters, separated by a guard band, power caps and per-site interference calculation. Coexistence is engineered, not refused.

Coexistence in this band is not only a paper calculation in Norway; it has been demonstrated. In a test at Kjeller airport, Nkom, together with the Norwegian Defence Research Establishment, the air force, the police helicopter service and the air ambulance service, placed a live 5G transmitter on the runway and flew three helicopters — a police AW169, an air-ambulance H135 and a rescue AW101. No operational constraint was observed, even with the base station as close as about 50 metres — far closer than any real deployment would place a base station to an aircraft.

8. High-Value Indian Use Cases

The strongest CNPN cases are operational systems in which cellular connectivity is fused with communications, sensors, control and legacy networks. The objective is not a generic private-5G demonstration but a measurable improvement in safety, productivity, resilience or service delivery.

Sector	Operational requirement	CNPN capabilities	Why PLMN may be insufficient
Railways / Metro	Guard-driver-station-control voice; tunnels; crowd safety; accident relief	MCX, IMS, cab/dispatcher radios, GIS, PA, cameras/ISAC, UHF/VHF/PBX interworking, NIB	Safety-critical priority, corridor/tunnel coverage, local survivability, legacy integration
PPDR / Disaster	Networks fail or congest during disaster	Deployable NIB, MCX, GIS, responder tracking, sensors, drones, satellite/NTN	Rapid restoration and local multi-agency command
Mines / Oil & Gas	Remote sites, moving equipment, worker safety, SCADA	Private RAN, IoT, telemetry, video, MCX, positioning, edge AI	Sparse public coverage and strong OT/security needs
Ports / Airports	Perimeter security, fire/rescue, docking/airside operations	MCX, video, autonomous vehicles, sensors, PA, GIS, analytics, positioning	Deterministic zones and multi-agency workflows
Utilities	Substations, field crews, telemetry, restoration	Low-band coverage, MCX, SCADA/IoT, resilient backhaul, digital twins	Wide geography, penetration and resilience requirements
Defence / Borders	Remote coverage, patrols, sensing, tactical deployment	Private NIB, low-band RAN, drones, satellite, AI sensing, command	Sovereignty, mobility and no/limited public coverage
Factories	Robotics, AGVs, machine vision, production automation	URLLC-oriented QoS, dense IoT, edge compute, positioning, slicing	Need predictable performance and OT integration
Healthcare	Tele-ICU, imaging, device telemetry, ambulance integration	Private coverage, edge data processing, deterministic QoS, secure identity	Local data control and reliable service
Smart cities / events	Crowd surges, multi-agency response	MCX, GIS, CCTV/ISAC, PA, help desk, NIBs	Public congestion and need for common operating picture
Rural / agriculture	Village/farm/dairy/cold-chain connectivity	FWA, IoT, edge services, local spectrum, shared backhaul	Consumer business case may be weak in low-density clusters

8.1 Railways and Power Plants as Lighthouse Sectors

Railways combine almost every CNPN requirement in one national system: high-speed and linear mobility, stations, yards, tunnels, emergency response, mission-critical group communication, legacy UHF/VHF and PBX integration, CCTV, public address, positioning and a migration path toward FRMCS. A successful railway architecture can therefore generate reusable technology for metros, airports, ports, mines, defence and disaster response.

Power plants are geographically concentrated critical infrastructure that require secure, reliable connectivity and local survivability during wider-network disruptions. A private, standalone 3GPP network can modernise and replace legacy systems such as TETRA, DECT and Wi-Fi while supporting operational technology, safety services, workforce communications, video and sensors. With significant investment in power-generation infrastructure in India and other growth markets, this represents a substantial opportunity for private networks.

5G and 5G-Advanced can lower opex by replacing multiple legacy networks (e.g. TETRA, DECT, Wi-Fi and LoRa) with a single reliable network for all needs.

9. Standards, Interoperability and Migration

A credible CNPN ecosystem must avoid proprietary islands. The network may be highly customised at the application and integration layer, but the underlying interfaces should align with widely adopted global standards so that enterprises can migrate progressively and preserve installed assets.

Capability	Standards / interfaces	Practical outcome
Mission-critical voice	3GPP MCPTT / MCX	Group calls, floor control, emergency priority and late join
Mission-critical video/data	MCVideo / MCData	Push-to-video, live feeds, messages, files, status and location
Packet voice	IMS, VoLTE, VoNR, SIP	Enterprise/railway telephony integration and standard call features
Railway evolution	3GPP railway requirements; FRMCS concepts	Structured migration rather than forklift replacement
Legacy radio interworking	MCX-LMR / RoIP gateways	UHF/VHF/TETRA/DMR users interwork with LTE/5G users
Security / identity	SIM/eSIM, UDM/AUSF, role-based profiles	Known device population and auditable privileges
GIS / command	Location services and geospatial APIs	Geofencing, tasking and common operating picture
Video / OT	RTSP/ONVIF, SIP/IP gateways, SCADA/IoT APIs	Convergence of cameras, PA, sensors and operations

9.1 Migration principle

Private mobile infrastructure should be an additive convergence layer that does not create yet another silo of mobile devices, but seamlessly interconnects existing radios, phones, exchanges, PA, SCADA and sensors while users migrate at a pace justified by reliability, economics and certification. This is especially important in railways, utilities, defence and public safety, where legacy systems remain operationally embedded.

9.2 Multi-vendor interoperability

India should define profiles, APIs and certification that allow components from multiple vendors to work together. This reduces lock-in, expands the domestic supplier base and gives Indian products a clear roadmap for global deployment, including seamless interconnection with third-party products worldwide.

10. Security, Sovereignty, Governance and Compliance

10.1 Private networks can be strongly governed

A CNPN has a known owner, a bounded geography and an enrolled population of SIMs and devices, all within the control of the user. These characteristics can simplify attribution, access control and audit compared with use of the national public network. Depending on the deployment architecture, this may not remove cyber-security or lawful-interception obligations, but the governing rules can be proportionate to the risk and the architecture.

Risk / concern	Potential safeguard
Unauthorised use	Site-specific authorisation; enterprise-issued SIM/eSIM; dedicated PLMN/NID; audit logs
Radiation beyond authorised area	Defined EIRP, antenna conditions, RF survey and compliance testing
Cyber compromise	3GPP security, role-based access, secure gateways, patching and vulnerability management
Lawful interception / compliance	Standard interfaces where legally required; controlled external interconnection
Interference	Coordination database/frequency plan, exclusion zones where justified and coexistence masks
Data sovereignty	Local UPF/edge breakout, on-premise processing and defined retention/access policy
Vendor lock-in	Open APIs, standards-based interfaces, portable identity/user data and multi-vendor certification

10.2 Sovereignty across the full stack

India should position CNPNs as foundational infrastructure for the country's next phase of digital transformation. By providing secure, reliable and intelligent connectivity across factories, ports, mines, hospitals, campuses and critical infrastructure, CNPNs can help companies increase productivity, automate operations, improve worker safety and develop new services, while enabling public institutions to deliver more inclusive, resilient and responsive services to citizens. This requires a trusted and resilient technology foundation, with appropriate attention to data residency, operational control, supply-chain resilience and the progressive development of domestic capabilities where strategically important.

10.3 Proportionate governance

Security obligations should be proportionate to the footprint and risk of the network. A small indoor factory network need not be regulated identically to a wide-area strategic network, but both should have clear identity, accountability, interference contacts and cyber hygiene. A risk-tiered licensing approach can align regulatory burden with actual exposure.

11. CNPN as India's 5G-Advanced and 6G Testbed

Future networks will not only connect people and machines; they will sense, reason and orchestrate operations. With native AI, CNPNs will in effect have a mind of their own. Private networks are therefore a natural environment in which such innovations can be validated, because the geography, users, assets and operational KPIs are bounded and measurable. These networks need to be actively promoted, and spectrum assignment should be simplified accordingly.

6G-ready capability	What it changes in CNPN	Illustrative applications
AI-native orchestration	Network predicts demand, faults and operational priorities and optimises radio, core, edge and backhaul towards autonomous operation	Railways, mines, factories, airports, utilities
ISAC	Communications fabric becomes part of sensing and situational awareness	Crowd sensing, intrusion, tunnels, perimeter security
TN + NTN	Terrestrial, satellite and aerial relay operate as one resilient fabric	Disasters, borders, offshore, rail accidents
Digital twins	Live virtual model predicts congestion, faults and outcomes before action	Railways, factories, ports, power grids
Ultra-reliable low latency	Extends private networks toward selected machine/process control	Robotics, autonomous vehicles, remote machinery
High-precision positioning	Makes the network a location platform as well as communications	Workers, responders, trains, robots, vehicles
Advanced slicing	Share resources by operational function and criticality	Security, fire, signalling, CCTV, SCADA
Edge intelligence	Processes data locally and maintains essential intelligence	Video analytics, predictive maintenance, hazards
Massive machine connectivity	Connects dense populations of sensors and industrial endpoints	Factories, utilities, mines, logistics
Self-healing resilience	Detects failures and automatically reroutes/reconfigures	Railways, PPDR, utilities, defence
Energy-aware networking	Optimises radio and compute energy needs	Battery NIBs, border posts, remote sites
Sovereign/auditable AI	AI recommendations/actions remain attributable to rules, evidence and authorised data	Safety-critical rail, defence, utilities and public safety

11.1 Strategic role of 6G-ready CNPN

The strategic value of a 6G-ready CNPN is that intelligence, sensing and simulation become part of the operational network. AI-native orchestration can translate natural-language intent into policy-bounded network actions; ISAC can add awareness of movement and the environment; and digital twins can test likely outcomes before changes are applied. These capabilities are summarised here as the strategic direction for CNPN; the detailed capability grouping and sector implications are consolidated in Section 14.4.

12. Recommended Indian CNPN Framework

Policy pillar	Recommended action	Expected outcome
Spectrum	Local/administrative licensing of small chanks in 3.7–4.2 GHz; structured low-band secondary use/local access for coverage-critical use; transparent coordination rules	Lower entry cost, quick approvals, faster deployment and efficient reuse
Permission for CNPN	Offshore areas and areas not covered or connected by TSPs, where the national spectrum resource is not optimally used	New applications and coverage in unserved areas
Licensing workflow	Online geographic application, defined technical envelope and time-bound approval	Predictable approval timelines and low transaction cost
Identity	Dedicated PLMN/NID framework for authorised private networks	Traceability, security management and device ecosystem clarity
TSP participation	Explicitly support NaaS, leasing, MORAN/MOCN, APN and slicing	New enterprise revenue and broader customer choice
Interoperability	Indian profiles for MCX, IMS/SIP, legacy radio, PA, common configuration NMS and recording systems, SCADA and GIS	Certified APIs for integrating third-party devices, solutions and media gateways with India-centric needs
Testing & certification	Coexistence labs, MCX/FRMCS plugtests, legacy-system interoperability certification, security validation and sector-specific certification	Evidence-based policy and exportable credentials
PoC funding	2–3 lighthouse PoCs per priority sector with measurable operational KPIs	Demand creation, standards and product references
Domestic value addition	Preference for design-led Indian products and source-controlled software in strategic deployments	Sovereign capability and export-ready IP

12.1 What the Policy Should Enable

- Network slicing should be considered one of several complementary solutions for meeting mission-critical, customised and sovereignty-related requirements.
- CNPN should become a driver of the Indian design ecosystem, so domestic design and technology, interoperability and migration must be mandatory design goals.
- Low-band access can be purposefully planned and coordinated for use cases where coverage and penetration are priorities, supported by clear coexistence frameworks and robust interference safeguards.

13. Design in India for Global Leadership

13.1 Why CNPN Aligns with Indian Strengths

Private mobile networks are software- and integration-intensive. Value is distributed across RAN, core, IMS/MCX, gateways, rugged devices, GIS, edge compute, AI, cyber security, testing, integration and lifecycle services. This profile aligns well with India's strengths in software engineering, systems integration and large-scale operational infrastructure.

Indian advantage	How to convert it into market leadership
Large lighthouse customers	Use railways, metros, airports, mines, utilities, defence and disaster agencies as reference deployments
Software and systems talent	Own orchestration, MCX, GIS, sovereign AI, knowledge graphs, APIs and integration layers
Diverse environments	Develop products that work in cities, mines, deserts, coasts, tunnels and high-speed rail
Test/certification ecosystem	Create Indian interoperability and sector profiles with reciprocal recognition
Design-led manufacturing	Tie strategic deployments to measurable domestic design, source control and value addition
Global South relevance	Export rugged, cost-optimised and mixed-legacy solutions to markets with similar constraints

13.2 A Domestic Market Creates Capability

India's historical telecom demand was concentrated in a few large operator procurements, which limited the opportunity for a broad domestic equipment and integration ecosystem. Local private networks create thousands of smaller, varied deployments in which Indian core, applications, gateways, edge platforms, devices and integrators can win business, learn and improve.

13.3 Customers Need Solutions, Not Isolated Boxes

Project benchmarking material indicates substantial private-network activity in China, Germany, the United States, Japan, South Korea, the UK and France, with manufacturing, mining, ports, automotive, utilities, defence, railways and airports among the dominant segments. The direction is unambiguous: captive private cellular networks for enterprises are an important part of the future. Customers need solutions, not isolated boxes of CUs, DUs or RUs — or even standalone MCX or IMS — so India should focus on building complete solutions.

India's strongest differentiation is likely to lie in augmented solutions that combine mission-critical applications, network orchestration, legacy gateway integration, GIS, security, domain data and sovereign AI. Domestic deployments should be structured so that these layers become reusable products and exportable reference architectures.

14. B6GA Solution Portfolio and Priority 6G Capabilities

14.1 Six B6GA Lighthouse Use-Case Papers

The Bharat 6G Alliance has prepared six detailed white papers on use cases in India where domestic companies can take the lead and deploy solutions for the global market. This compendium is intended not merely as a set of research notes but as a coherent portfolio of solutions that Indian companies can build, validate in Indian conditions and take to global markets. Together, the papers cover emergency connectivity, border security, a cross-cutting 6G scenario framework, railway accident relief, crowd management and railway operational communication. The common philosophy is to solve a real Indian requirement with deployable 4G/5G technology today, while creating standards, software, data, AI and system architectures that are ready for migration to 6G.

6G-Ready Emergency Connectivity and Disaster Response Command

This paper addresses the operational gap that begins after a disaster warning has been issued and field teams are deployed. It proposes a portable private-network platform that can restore connectivity when terrestrial networks are damaged, overloaded or absent. The architecture combines a portable 5G/private access node, satellite or NTN backhaul, drone relay, responder smartphones and rugged devices, field sensors, edge AI and a GIS command dashboard. Its value lies in the integration of communication, sensing, tracking and multi-agency coordination rather than in any single component. The platform would include a common NMS configuration dashboard and a central CDRS for recording. Indian companies can build the portable NIB, local core, MCX services, responder application, GIS platform, sensor gateways, drone integration and edge-AI modules. India offers an immediate domestic market through NDMA, SDRFs, police and fire services and district administrations, while the same solution is exportable to disaster-prone countries in Asia, Africa and the wider Global South, where terrestrial infrastructure is vulnerable or sparse.

6G-Ready Border Connectivity, Surveillance and Intrusion Detection

The second paper applies the private-network architecture to remote land and coastal borders. It combines man-packable or portable communication nodes, private LTE/5G access, satellite backhaul, drone relay, rugged patrol devices equipped with seismic or motion sensors, thermal and optical cameras, edge AI and a command-centre GIS platform. The proposed Space-Air-Ground Integrated Network approach is particularly relevant where no single communication layer can provide continuous coverage. Indian industry can build rugged radio nodes, sensor integration, AI classification, drone-relay payloads, secure command software and interoperable field devices. The domestic demand spans BSF, ITBP, SSB, Coast Guard and other security agencies. Globally, a modular border-connectivity and surveillance system has relevance to long land borders, coastlines, pipelines, wildlife reserves and other remote-security applications.

Interference Use Case for Feasibility in the Indian Context

The third paper is a cross-cutting framework rather than a single operational product. It maps 3GPP 6G scenarios to Indian requirements in dense urban areas, indoor hotspots, rural and extreme long-distance coverage, high-speed rail, factories, NTN, highways and other environments. Its strategic value is that it identifies where Indian companies should focus product development: long-range and rural connectivity, high-

speed mobility, industrial systems, AI-native networking, integrated sensing, NTN and energy efficiency. The paper can therefore be positioned as the demand map that links the other five solution papers into a broader Indian 6G programme. For industry, it provides a basis for testbeds, radios, edge platforms, AI orchestration, positioning, sensing, satellite integration and sector-specific applications that can be validated domestically and exported later.

Accident Relief Train and Emergency Communication System

The Accident Relief Train paper is one of the strongest examples of a near-term Indian product opportunity. It proposes a rugged Network-in-a-Box carried on the Accident Relief Train that creates an autonomous communication island at an accident site. The system combines a 4G/5G radio, local core, IMS, MCPTT, MCVideo, MCData, dispatcher and GIS functions, 700 MHz coverage, a portable mast, OFC and satellite backhaul, battery power and gateways to UHF/VHF, railway VoIP and PA. The architecture is aligned with 3GPP mission-critical services and FRMCS concepts, and can work seamlessly with legacy communication systems specific to Indian Railways. Indian companies can manufacture the NIB, radios, rugged terminals and gateways, while Indian software firms can provide the core, MCX, GIS, VMS, CDRS, AI and integration. The same product can be adapted beyond railways for disaster response, defence, mines, remote construction, large events and emergency restoration in global markets.

Crowd Management for Smart Cities, Railways, Airports and Large Congregations

This paper turns crowd management from a passive CCTV-monitoring problem into an integrated communication and action platform. It combines private LTE/5G, MCX, GIS, dispatcher consoles, live camera feeds, PA, help desks, geofencing, personnel location, battery and signal monitoring, man-down and SOS alerts, and multi-agency coordination. The proposed 6G evolution adds ISAC, AI-based crowd-density estimation, GNSS-based abnormal-movement detection, network slicing, sensing-assisted awareness and edge intelligence. Indian companies can build both the communications platform and the domain applications, including analytics, multilingual help desks, command software and device management. The solution has immediate relevance to Indian Railways, metros, airports, stadiums, pilgrimage sites, religious gatherings and smart cities, and it is directly exportable to countries facing similar high-density event and transport challenges.

Railway Tunnel Communication: Guard, Engine Driver, Station and Control

The sixth paper proposes a unified operational communication layer for the railway chain: loco pilot, guard or train manager, station master, dispatcher, field staff and control offices. It integrates VoLTE and VoNR, IMS, MCX handsets, cab radios, dispatcher consoles, railway exchanges, TCCS, PBX and IP phones, together with UHF/VHF interworking and redundant OFC, public-network or satellite backhaul. The approach is evolutionary: legacy assets remain in service while a standards-aligned private LTE/5G layer is added and progressively migrated while retaining the FRMCS and 6G structure. Indian companies can build cab and dispatcher products, IMS/MCX platforms, gateways, recording systems, GIS, orchestration and sovereign AI assistants grounded in railway rules and SOPs. Because railways worldwide are moving from legacy railway radio toward broadband mission-critical communication, this is also a substantial export opportunity if India develops interoperable and certified products early.

Taken together, these six papers suggest a clear industrial strategy. India should not approach 6G only as a future radio standard or as a laboratory research programme. It should use large national infrastructure systems as living testbeds in which Indian companies solve real problems with 5G today and progressively add sensing, NTN, AI, orchestration and 6G capabilities. The reusable outputs should include private-core software, MCX platforms, rugged NIBs, edge-compute appliances, GIS and dispatcher applications, legacy gateways, Indian language models, rule libraries, data schemas, test benches, security profiles and certification methods. These building blocks can then be recombined across sectors rather than being reinvented for every project.

The export opportunity is especially important. Many countries in Asia, Africa, the Middle East and Latin America have railways, ports, mines, disaster-prone regions, long borders and public-safety agencies with requirements similar to India but with limited budgets. Solutions engineered in India for cost, ruggedness, interoperability and mixed legacy environments can therefore have a natural global market. B6GA can help by converting Indian deployments into standards-aligned reference architectures and by promoting reciprocal recognition of testing and certification.

> **B6GA industry message: build innovative solutions that address real Indian use cases, standardise what works, certify it domestically and export 6G-ready solutions to the world.**

14.2 Relevant 5G Enterprise Use Cases in India

India's highest-value CNPN opportunity is to develop repeatable, outcome-based solutions for manufacturing, railways, ports, mining, energy, healthcare, public safety and rural production clusters. Some examples are given below.

Globally proven use cases requiring scale in India

India should scale globally proven mission-critical use cases that remain limited or fragmented domestically, including MCX-enabled public safety, emergency command and control, resilient utility and defence communications, deployable disaster-response networks and FRMCS-ready rail communications. Achieving scale will require regulatory clarity, sustainable procurement, legacy-system interoperability, mission-critical devices, cybersecurity, resilient infrastructure and coordinated execution across government agencies, CSPs and system integrators.

Sector	5G use cases	Value creation	Relevant Indian companies (examples)
Manufacturing	Autonomous material handling (AGVs), predictive maintenance, hyperspectral camera inspections	Eliminates the need to re-cable flexible production lines, prevents equipment failure and automates real-time quality control to increase yield.	Tata Electronics, Micron Technology, Ola Electric, Reliance Industries

Sector	5G use cases	Value creation	Relevant Indian companies (examples)
Logistics & Warehousing	Autonomous Mobile Robots (AMRs), connected handheld scanners	Replaces dense, unreliable Wi-Fi grids with sparse 5G radios, significantly reducing infrastructure capex (by up to 15%) and increasing worker productivity by preventing roaming drop-outs.	IndoSpace, Welspun One Logistics Parks, DHL Supply Chain
Ports & Transshipment	Remote-controlled cranes, autonomous terminal trucks, straddle carriers	Delivers highly available, secure communication across kilometres of quay and metal container stacks, where legacy Wi-Fi frequently suffers from dead zones and latency.	Adani Ports (APSEZ), JSW Infrastructure, Jawaharlal Nehru Port Authority (JNPA)
Mining & Heavy Industry	Tele-remote drilling, autonomous haulage, underground tracking beacons, AR safety audits	Provides robust coverage in hostile RF environments (e.g. highly metallic steel plants or underground mines), replacing inflexible fibre and unreliable legacy systems such as TETRA.	NMDC Ltd., Coal India Ltd., Vedanta Ltd., Hindalco Industries
Energy & Utilities	Massive sensor telemetry, connected EV chargers, drone inspections	Future-proofs critical infrastructure (such as nuclear power plants and hybrid solar parks) by unifying disparate communication systems, enabling efficient predictive maintenance and enhancing worker safety.	NTPC Limited, Adani Green Energy, Reliance Industries

14.3 Probable 6G Use Cases and Value Creation

6G can extend enterprise CNPNs from connectivity platforms into distributed sensing and AI-native operational systems. It will enable applications such as AGV tracking, autonomous mobility and multi-site sensing across factories, ports, mines, logistics hubs and transport networks. To support these use cases efficiently, sensing data should be processed close to the RAN and edge, supported by unified frameworks for observability, data collection and AI management. An AI-enabled 6G core could allow enterprise applications, devices and AI agents to express operational intent, coordinate with one another and dynamically optimise network resources. Standardised data and AI capabilities would accelerate the development of sector-specific solutions without requiring every application to be individually standardised.

In general, 6G will scale up and enhance many of the use cases under way or starting today, and will add energy optimisation through leaner design, new spectrum, a highly optimised uplink, spatial data and native-AI capabilities. The new and enhanced 6G technologies will be applicable to both public and private networks. 6G will be a platform that goes beyond communication, offering solutions to a broad set of problems and delivering services end-to-end to a wider ecosystem of consumers, enterprises and societies.

For a selection of seven use cases, the table below summarises the key opportunities, the Indian ecosystem mapping and what changes in a CNPN.

Priority 6G use case	Brief description	Indian ecosystem mapping	Relevant companies	What changes in a CNPN
Mixed Reality – Immersive Shared Experiences	Enhances XR through higher uplink/downlink capacity, precise positioning, improved battery life, spatial data, and affordable smart glasses and AI-native wearables.	Remote maintenance and training for Indian Railways, factories, mines, utilities, healthcare, and emergency services.	**Factories:** Tata Electronics, Reliance Industries, Adani New Industries **Mines:** NMDC Ltd., Coal India Ltd. (CIL), Vedanta Ltd., Hindalco Industries **Utilities:** NTPC Limited, Tata Power, Adani Green Energy	Requires high uplink capacity, low latency, precise positioning, edge computing, and differentiated QoS.
Global Internet – Digitalisation for Everyone, Everywhere	Enables efficient mobile broadband, improved satellite–terrestrial mobility, and optimised FWA coverage.	Rural, remote, island, Himalayan, border, and disaster-affected regions.	**Remote/Deepwater:** ONGC, Vedanta Ltd. (Cairn Oil & Gas) **Remote Mining:** NMDC Ltd., Coal India Ltd.	Extends connectivity through terrestrial–non-terrestrial integration, FWA, satellite fallback, and resilient coverage.
Autonomous Mobility – Supporting Smart Transport	Improves air and ground connectivity through greater reliability, compute offload, higher uplink capacity, consistent latency, and physical AI support.	Railways, metros, ports, airports, mines, warehouses, agricultural drones, and industrial vehicles.	**Ports:** Adani Ports (APSEZ), JNPA, JSW Infrastructure **Airports:** GMR Airports, Adani Airports, Airports Authority of India (AAI), BIAL **Warehouses:** IndoSpace, Welspun One Logistics Parks, Amazon India, Flipkart **Industrial Vehicles:** Ola Electric, Tata Group	Enables deterministic communication, high-precision positioning, machine connectivity, edge AI, and aerial–terrestrial coordination.
Critical Services – Priority Emergency Communication	Strengthens resilience and security while using ISAC to detect unwanted drones and other connected or unconnected objects that may endanger first responders.	Disaster response, police, fire services, emergency healthcare, defence support, and railway incident management.	**Oil & Gas Infrastructure:** ONGC, IOCL, BPCL, HPCL, Reliance Industries **Nuclear Facilities:** NPCIL	Provides priority traffic, SLA assurance, satellite fallback, deployable coverage, observability, ISAC-based detection, and self-healing.

Priority 6G use case	Brief description	Indian ecosystem mapping	Relevant companies	What changes in a CNPN
Spatial Data – Exposing Data Related to Coordinates	Reuses communication infrastructure for network-based sensing, enabling drone detection, safer flight paths, environmental reconstruction, disaster monitoring, and immersive applications.	Smart cities, rail safety, drone corridors, ports, utilities, infrastructure monitoring, and environmental assessment.	**Ports:** Adani Ports (APSEZ), JNPA **Utilities/Pipelines:** NTPC, Tata Power, GAIL **Infrastructure:** L&T, Tata Projects, ITD Cementation	Turns the CNPN into a spatial-intelligence platform using ISAC, positioning, timing, sensor fusion, and network APIs.
Massive Digital Twin – Data Collection, Management, and Modelling	Combines real-time sensor data with AI to create virtual models for prediction, management, optimisation, and testing before physical changes are implemented.	Digital twins for railways, smart cities, construction, factories, power grids, water systems, logistics, and CSP networks.	**Construction:** L&T, Tata Projects **Factories:** Tata Electronics, Reliance Industries, Ola Electric **Power Grids:** NTPC, Adani Green Energy **Logistics:** IndoSpace, Welspun One Logistics Parks, DHL Supply Chain	Integrates massive IoT, edge/cloud computing, real-time data models, closed-loop optimisation, and enterprise APIs.
AI Communication – Super Awareness and AI Offload	Provides AI-native network functions, optimises RAN and end-to-end performance for AI applications, and supports large volumes of AI-generated uplink and downlink traffic.	Sovereign and multilingual AI for field engineers, industrial workers, healthcare, emergency teams, education, and command centres.	**Manufacturing:** Tata Electronics, Reliance Industries **Mining:** NMDC Ltd., Coal India Ltd. **Oil & Gas:** ONGC, IOCL	Enables AI-native RAN optimisation, edge inference, AI-agent orchestration, network exposure, privacy-preserving processing, and auditable automation.

Use case descriptions

Mixed Reality – Immersive Shared Experiences

Immersive communication combines digital objects, information and overlays with the physical world, and lightweight AR glasses are expected to accelerate adoption. Multiplayer mixed-reality gaming, targeted for the 2030 timeframe, requires synchronised multi-user experiences and differentiated connectivity, including capacity for high user density, high uplink and downlink data rates, QoS tailored to different data streams, predictable low latency and seamless wide-area coverage. Network capabilities and exposed APIs can support spatial data and digital twins for mapping, compute and AI offload, positioning, sensing and interworking with application platforms. Latency is expected to improve from approximately 100 ms today toward 20 ms, while per-player downlink requirements may grow from around 20 Mbps to 50–100 Mbps as rendering, resolution and depth data increase.

Global Internet – Digitalisation for Everyone, Everywhere

Many people and regions remain underserved by mobile broadband (MBB). A cost-efficient combination of high-tower terrestrial cells, satellite-based non-terrestrial networks, fixed wireless access and indoor networks can help bridge this digital divide. Such ubiquitous and resilient connectivity would provide basic MBB services for everyday and sensitive applications, as well as high-speed access at hotspots and homes, potentially delivering video-grade speeds and an area traffic capacity of approximately 50 kbps per square kilometre in remote rural areas.

Autonomous Mobility – Supporting Smart Transport

Autonomous vehicles, collaborative robots and delivery drones require reliable information about their position, the environment and nearby road and airspace users. Predictable time-critical communication, high availability, observability, ubiquitous three-dimensional connectivity, inter-machine communication, spatial data and digital twins, and compute/AI offload can support safe autonomous operation. For drones, resilient network-assisted positioning can complement GNSS, help detect spoofing and — through future 6G positioning — provide the accuracy needed for safer navigation.

Critical Services – Priority Emergency Communication

Critical services require prioritised, secure, and resilient connectivity with end-to-end service guarantees, observability, and automated recovery. Terrestrial networks can be complemented by deployable or satellite-based coverage for remote areas, while fallback and self-healing mechanisms help maintain service continuity; indoor and underground non-line-of-sight areas require additional solutions.

First responders in the field and their remote command-and-control centres can leverage the existing basic coverage and capacity of 3GPP mission-critical services, interworking capabilities with non-3GPP networks, and security features. The prioritisation of critical services is ensured through end-to-end (E2E) service-level agreements (SLAs).

Observable parameters are needed to specify the required details of an E2E SLA between a provider and a consumer. Trust is built by consistently meeting these SLAs. In the future, more demanding public-safety-related SLAs can be supported through improved resilience, fallback, and recovery solutions. Automation will make these solutions faster and more flexible.

Whenever and wherever a critical situation arises, coverage may be needed immediately. However, full terrestrial network (TN) coverage is expensive — especially in very remote locations. Deployable networks can be brought in when needed, but deployment takes time and adds cost. If non-terrestrial network (NTN)

solutions, particularly satellite systems, provide wide-area coverage with limited capacity, they can be used in areas with a line-of-sight link to the satellite. However, non-line-of-sight environments, such as indoor and underground spaces, including tunnels, would still not benefit from this coverage.

Spatial Data – Exposing Data Related to Coordinates

Spatial data services expose information about positions, movement, objects, and physical environments through APIs. Positioning, integrated sensing and communication, timing, compute/AI, and sensor fusion can support applications such as mixed reality and autonomous mobility, although data coverage and accuracy depend on the available radio environment and line of sight.

Spatial information can describe a position, an area, or a three-dimensional space, as well as how objects move. It can relate to connected cars, drones, and other connected objects, as well as unconnected objects such as pedestrians and bicycles. It can also describe the properties and features of a physical environment or concern the interplay between digital and contextual information and spatial data.

The spatial data use case is part of the effort to expand the scope of network services beyond communication.

Networks rely on device positioning and network sensing — radar-like ranging based on signal echoes — to collect spatial data, which is then analysed. The resulting processed data is exposed to consuming services. A key advantage is that the network can reuse communications equipment to capture spatial data while still achieving accuracy on the order of a few metres. However, coverage for this type of data collection is limited to areas with a line-of-sight link to the base station. This may be feasible in dense urban scenarios, but it is not generally available. Fusing the data with streams from other sensors can help improve the services offered.

Massive Digital Twins – Data Collection, Management and Modelling

Massive digital twins connect physical systems with virtual models to support monitoring, control, and configuration across robots, factories, utilities, buildings, and homes. They require scalable, low-cost IoT connectivity, bidirectional communication, and compute/AI; near-real-time applications additionally require reliable, prioritised connections.

An important condition for this use case to take off is cheap and simple-to-use communication, which requires, for example, low-cost communication modules. The systems would then be able to maintain contact with the digital twin and follow the models or configurations customised for the particular application. The system requires two-way communication and a computational platform hosting the digital twin. To meet near-real-time requirements, a high-priority connection specifically configured for this type of communication needs to be established.

The use of digital twins for management of the physical realm can be extended to many use cases, including logistics, management of utilities, factories, and even everyday home tasks.

AI Communication – Unlocking Learning Potential Through Networks

AI communication can enhance personal assistance, sensory capabilities, and image and video experiences through device, edge, and cloud-based AI. Resilient, low-latency, secure, and privacy-preserving connectivity is essential, while edge processing can reduce wearable-device battery consumption and keep sensitive data local. Network-based spatial AI services may improve device awareness but will also increase uplink demand.

As AI evolves, it will further improve human communication with people, devices and surroundings. Examples include hearing aids with complete noise cancellation and the ability to tune in to specific sounds; visual aids enabling recognition beyond normal vision; and communication aids using eye movements or brain interfaces. In image and video applications, AI will increasingly be used to generate and regenerate images

and video, enhance or alter scenes, and convert images to video, 2D video to 3D video, and 3D video to volumetric video. AI will also integrate video into multimodal content, for example lip-syncing and lip-reading.

AI-enhanced senses must work seamlessly everywhere and at all times, which places high demands on connectivity. This includes requirements for resilient and trustworthy networks, low latency, and robust security and privacy measures to safeguard sensitive data.

Image and video processing using edge-based AI processing and rendering could become important to reduce battery consumption of wearable devices, such as AR glasses.

Edge-based AI processing and rendering has an advantage over cloud-based processing. It can provide privacy services by removing sensitive data at the edge, ensuring that it is not communicated back to any central service function.

In addition, AI agents in devices such as smart glasses are expected to make increasing use of network-based (edge or cloud) compute for spatial information, to provide "What am I seeing?" support. This will significantly increase uplink requirements over time as smart glasses gradually evolve into full-featured AR glasses.

14.4 Key Capabilities of 6G for CNPN

For CNPNs and private networks, the contribution of 6G is expected to extend beyond increases in peak data rates. A broader opportunity is to enable networks that are more intelligent, context-aware, resilient, closely integrated with enterprise operations, and capable of supporting increasingly autonomous decision-making.

A 5G private network primarily provides controlled connectivity, quality of service, and support for local applications. A 6G-ready CNPN could evolve into an intelligent operational platform that combines communication, sensing, positioning, prediction, and decision support. Within clearly defined policy, security, and governance boundaries, it could also support the orchestration and automation of selected enterprise processes.

These capabilities include AI-native networking, Integrated Sensing and Communication (ISAC), harmonised terrestrial and non-terrestrial networking, ultra-reliable low-latency communication, high-precision positioning, network slicing, edge intelligence, energy efficiency and resilience-by-design. They are particularly valuable in private networks, where network capabilities can be engineered to meet mission-specific operational priorities and requirements.

Priority 6G feature	Implications for CNPN
AI-native orchestration	The network can predict demand, detect faults and account for operational priorities while automatically optimising RAN, core, edge and backhaul resources. It can also support self-healing and redundancy management.
Integrated Sensing & Communication (ISAC)	The network becomes part of the sensing and situational-awareness system rather than only carrying sensor data. It can reduce the need for camera systems, or improve accuracy when combined with camera data.

Priority 6G feature	Implications for CNPN
TN + NTN integration	The private terrestrial network can integrate with satellite and aerial relay systems to provide a unified, resilient connectivity fabric.
Digital twins	A live virtual model of the network, assets and operations can predict congestion, detect potential faults and assess likely outcomes before changes are implemented.
Ultra-reliable low-latency communication	URLLC can extend the role of a CNPN beyond voice, video and data services to support selected machine-to-machine communication and process-control applications.
High-precision positioning	Extends the role of a private network beyond connectivity, making it a platform for high-precision positioning, location services and asset tracking.
Advanced slicing / deterministic QoS	Enables differentiated resource allocation by operational function, and dynamically prioritises and protects safety-critical traffic.
Edge intelligence / distributed AI	Processes data locally, reduces bandwidth consumption and enables essential intelligence and decision-support functions to continue operating during WAN failure.
Massive IoT / machine connectivity	Enables large-scale connectivity for sensors, machines and industrial endpoints through a unified, controlled connectivity fabric.
Advanced beamforming / intelligent radio	Dynamically directs radio resources to where they are most needed, improving reliability, capacity and energy efficiency.
Self-healing / resilience-by-design	Enables the CNPN to detect failures and automatically reroute traffic or reconfigure network resources to maintain the continuity of critical services.
Energy-aware networking	Extends battery life and supports remote-site operation through intelligent radio and compute management.
Sovereign / auditable agentic AI	Allows AI agents to assist or automate operations while preserving human authority and oversight, and maintaining explainable, auditable decision trails.
Extreme uplink capacity	Supports uplink-intensive traffic from cameras, drones, sensors and machines — traffic patterns that differ significantly from those of consumer networks.

Intelligence, orchestration and deterministic QoS

AI-native orchestration is the operational brain of a 6G-ready CNPN. It can continuously combine network telemetry, application demand, location and enterprise schedules to predict congestion or faults, allocate radio/core/edge resources, and protect safety-critical traffic through dynamic QoS and slicing. Edge

intelligence keeps essential analytics local and allows critical functions to continue even when WAN or cloud connectivity is degraded.

Sensing, positioning and digital twins

ISAC, high-precision positioning and digital twins together turn the private network into an awareness platform. Radio sensing can complement cameras and specialist sensors for movement, intrusion and occupancy awareness; positioning can track workers, vehicles, trains and robots; and a digital twin can rehearse the likely impact of a network or operational action before it is applied. The value is strongest in bounded environments such as stations, tunnels, mines, factories, ports and airports where the physical domain is known.

Resilient connectivity and low-latency control

Terrestrial and non-terrestrial integration allows private RAN, public-network fallback, satellite and drone relay to operate as one resilient fabric. Ultra-reliable low-latency communication can extend CNPN into selected machine and process-control functions, while self-healing mechanisms reroute traffic, activate alternate backhaul or relocate functions when a link or node fails. These capabilities are particularly relevant to PPDR, railways, utilities, defence, offshore sites and remote mines.

Scale, radio efficiency and machine-heavy traffic

Massive machine connectivity, advanced beamforming and higher uplink capacity address the traffic pattern of private networks, where cameras, drones, sensors and machines may generate more uplink than downlink. Intelligent radio and energy-aware operation can focus capacity where it is needed, improve difficult-area coverage and extend battery endurance for NIBs, border posts and temporary sites. The objective is efficient, reliable service rather than headline speed alone.

Trusted and auditable agentic AI

For safety-critical sectors, autonomy must remain attributable and governed. Agentic AI may supervise radio, video, PA, crowd management, maintenance or other subsystems, but material actions should be traceable to authorised rules, trusted data and a defined decision path. Sovereign, auditable AI is therefore a core requirement for railways, defence, public safety, utilities and other mission-critical CNPN deployments.

14.5 Role of the Indian Ecosystem in 6G

The combined effect of these capabilities is a fundamental change in the role of CNPN. The first generation of private LTE/5G networks was largely about reliable enterprise connectivity; the next stage added mission-critical applications, local survivability, legacy integration and edge intelligence. A 6G-ready CNPN becomes an intelligent operational system that, being natively AI-enabled, in effect has a mind of its own. It can communicate, sense, locate, predict, decide and heal itself within trusted limits, and orchestrate enterprise operations while optimising network resources. 6G will be an evolving network that learns by itself and becomes more effective over time.

Learning systems based on sovereign AI could become Indian IPR, built on knowledge gathered by Indians over many years of running large legacy networks, some of which are among the largest in the world. Indian Railways operates one of the world’s largest rail networks, so its sovereign control and learning algorithms must remain under Indian control. Similarly, network data generated in the most critical networks — such as space, atomic energy research and defence applications — must remain in Indian hands, and the B6GA roadmap is the cornerstone for achieving global leadership on this basis.

For Indian industry, this is particularly important because the value increasingly moves toward software, system integration, data models, AI, command applications, trust mechanisms and sector-specific intelligence. These are areas in which Indian companies can create substantial domestic intellectual property even when some underlying radio components are part of a global ecosystem.

Priority 6G capabilities for Indian CNPN development

In the near term, Indian CNPN development must give the highest priority to building capabilities in AI-native orchestration, Integrated Sensing and Communication, terrestrial and non-terrestrial integration, digital twins, ultra-reliable low-latency communication, high-precision positioning and trusted agentic AI. Other enabling technologies that allow these higher-level capabilities to work reliably are network slicing, edge intelligence, advanced beamforming, massive IoT and energy-aware operation, for which PoC sites must be upgraded at the earliest opportunity.

This prioritisation will prevent the 6G programme from becoming a series of demonstrations of speed alone. Each PoC should demonstrate a measurable operational improvement: lower response time, better situational awareness, improved safety, reduced site count, longer battery life, more reliable control, improved positioning or automated decision support with a complete audit trail using a sovereign, auditable AI model.

Sector mapping for 6G capabilities

Sector	Most relevant 6G capabilities	CNPN outcome
Railways / Metro	AI orchestration, digital twins, slicing, mobility, positioning, ISAC, trusted dispatcher AI, TN/NTN	Converged safety, operations, communication and situational awareness in tunnel communication and crowd management
Mines / Oil & Gas	ISAC, low-latency control, worker/vehicle positioning, massive IoT, edge AI	Safer autonomous and remote operations in sparse-coverage environments
Airports / Ports	Precise positioning, uplink video, autonomous vehicles, perimeter sensing, slicing, edge AI	One private operational fabric across agencies, assets and surveillance
PPDR / Disaster	TN/NTN, NIBs, drone relay, edge AI, responder positioning, resilience	Rapidly deployable intelligent communications when normal infrastructure fails
Utilities	Low-band reach, massive sensing, digital twins, self-healing networks, edge analytics	More observable, resilient and predictive field operations
Defence / Borders	Sovereign AI, space-air-ground integration, ISAC, drone relay, precise tracking	Trusted tactical communication and surveillance in remote areas
Factories / Campuses	URLLC, precise positioning, robotics, machine vision, digital twins, dense IoT	Private network becomes part of production automation

15. Conclusion

Captive Non-Public Networks are no longer an experiment. They are becoming core digital infrastructure for the parts of India's economy where connectivity decides safety, productivity and sovereignty: railways, mines, ports, airports, power plants, factories, defence sites, disaster zones and rural production clusters. Public networks were built for mass-market mobility. CNPNs are built for guaranteed operational outcomes within a defined site, corridor or mission, so they complement the public networks rather than compete with them.

The conditions for scale are now in place. The Telecommunication (Authorisation for Captive Telecommunication Services) Rules, 2026 have made authorisation clear and simple. The 3.7–4.2 GHz device ecosystem has matured. Indian design companies and system integrators have shown that they can build and deploy private networks at home. International experience in Germany, Norway, the United Kingdom, Japan and elsewhere shows that local access to spectrum, transparent pricing and engineered coexistence can work together with a strong operator market.

One critical gap remains: a predictable spectrum framework. Until candidate bands, access mechanisms, coexistence rules and pricing are defined, enterprises cannot commit to the decade-long investments that industrial digitalisation requires. The framework should allow several routes to coexist:

- TSP-managed networks, slicing, leasing and MORAN/MOCN, alongside direct local assignment based on the real-estate principle
- mid-band spectrum for capacity
- structured low-band access where coverage and penetration matter most

Telecom operators remain essential partners in this model. Private networks increase demand for their backhaul, mobility, managed services and spectrum.

CNPN also gives India a strategic opportunity that goes beyond connectivity. Private networks have bounded geography, known users and measurable KPIs, which makes them the country's most practical testbed for 5G-Advanced and 6G. In these settings, capabilities such as AI-native orchestration, ISAC, digital twins, terrestrial and non-terrestrial integration, and sovereign, auditable AI can be proven against real operational results. The intelligence built on Indian operational data can become Indian intellectual property. The complete solutions engineered for Indian conditions — rugged, cost-optimised and able to work with legacy systems — can be exported to the many countries that face similar challenges.

B6GA therefore recommends five priorities:

1. **Finalise the spectrum framework.** Publish candidate bands, technical envelopes, a transparent fee formula and a time-bound online application process for local CNPN spectrum.
2. **Enable every deployment model.** Recognise TSP-led, enterprise-led, shared and hybrid routes so that each user can choose the architecture that fits its operational need.
3. **Launch lighthouse deployments.** Fund two to three proofs of concept in each priority sector, starting with railways, power, mining, ports and public safety, and measure operational KPIs, coexistence and security.
4. **Build interoperability and certification.** Develop Indian profiles for MCX, IMS, legacy interworking and APIs, with testing that is recognised internationally.

5. **Design for 6G and for export.** Require open, AI-ready and upgradable architectures, and give preference to design-led Indian products in strategic deployments.

India has the demand, the engineering talent and the policy momentum. By acting decisively now, it can turn its infrastructure needs into a proving ground for globally competitive private-network and 6G solutions. CNPN would then be not just a way to connect enterprises, but a foundation for India's leadership in the next generation of intelligent networks.

Terminology and Short Forms

Term	Meaning
3GPP	3rd Generation Partnership Project
5GC	5G Core network
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
API	Application Programming Interface
APN	Access Point Name
AUSF	Authentication Server Function
B6GA	Bharat 6G Alliance
CBRS	Citizens Broadband Radio Service
CDRS	Call / Communication Detail Recording System
CN	Core Network
CNPN	Captive Non-Public Network / captive private mobile network
COAI	Cellular Operators Association of India
CSP	Communications Service Provider
DMR	Digital Mobile Radio
DoT	Department of Telecommunications, Government of India
E1	Digital telephony transmission interface (2.048 Mbit/s)
EIRP	Equivalent Isotropically Radiated Power
eNB	Evolved NodeB (LTE base station)
EPC	Evolved Packet Core
eSIM	Embedded SIM
FCC	Federal Communications Commission, United States

Term	Meaning
FRMCS	Future Railway Mobile Communication System
FSS	Fixed-Satellite Service
FWA	Fixed Wireless Access
GAA	General Authorized Access (CBRS)
GIS	Geographic Information System
gNB	5G NR base station
GNSS	Global Navigation Satellite System
GSA	Global mobile Suppliers Association
GSMA	GSM Association
IMS	IP Multimedia Subsystem
IMT	International Mobile Telecommunications
IoT	Internet of Things
IPR	Intellectual Property Rights
ISAC	Integrated Sensing and Communication
ISED	Innovation, Science and Economic Development Canada
KPI	Key Performance Indicator
LMR	Land Mobile Radio
MCData	3GPP Mission Critical Data
MCPTT	3GPP Mission Critical Push-to-Talk
MCVideo	3GPP Mission Critical Video
MCX	3GPP Mission Critical Services (MCPTT, MCVideo and MCData)
MIC	Ministry of Internal Affairs and Communications, Japan
MOCN	Multi-Operator Core Network

Term	Meaning
MORAN	Multi-Operator Radio Access Network
MRSS	Multi-RAT Spectrum Sharing
MSIT	Ministry of Science and ICT, South Korea
NaaS	Network as a Service
NEF	Network Exposure Function
NIB	Network-in-a-Box
NID	Network Identifier
NMS	Network Management System
NPN	Non-Public Network
NR	New Radio (5G radio interface)
NTN	Non-Terrestrial Network
OFC	Optical Fibre Cable
OT	Operational Technology
PA	Public Address
PABX / PBX	Private Automatic Branch Exchange / Private Branch Exchange
PAL	Priority Access Licence (CBRS)
PCF	Policy Control Function
PLMN	Public Land Mobile Network
PNI-NPN	Public Network Integrated Non-Public Network
PoC	Proof of Concept
PPDR	Public Protection and Disaster Relief
PRI	Primary Rate Interface
QoS	Quality of Service
RAN	Radio Access Network

Term	Meaning
RedCap	Reduced Capability NR device class
RoIP	Radio over IP
SA	Standalone 5G architecture
SAS	Spectrum Access System
SCADA	Supervisory Control and Data Acquisition
SDRF	State Disaster Response Force
SI	System Integrator
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMF	Session Management Function
SNPN	Standalone Non-Public Network
SOC	Security Operations Centre
TDD	Time Division Duplex
TN	Terrestrial Network
TRAI	Telecom Regulatory Authority of India
TSP	Telecom Service Provider
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UHF	Ultra High Frequency
UPF	User Plane Function
URLLC	Ultra-Reliable Low-Latency Communication
VHF	Very High Frequency
VMS	Video Management System

Term	Meaning
VoLTE	Voice over LTE
VoNR	Voice over New Radio
XR	Extended Reality

References

India — framework and recent developments

- DoT CNPN Guidelines (27 Jun 2022): https://dot.gov.in/circulars/guidelines-captive-non-public-network-cnpn-license
- Telecommunication (Authorisation for Captive Telecommunication Services) Rules, 2026 (G.S.R. 511(E)), notified by DoT on 23 June 2026 under the Telecommunications Act, 2023: https://www.eservices.dot.gov.in/captive-non-public-network-cnpn-service-authorisation
- TRAI Recommendations on Network Authorisations under the Telecom Act 2023 (14 Feb 2025): https://www.trai.gov.in/sites/default/files/2025-02/PR_No.12of2025.pdf
- PIB release on the TRAI recommendations: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2104157
- DoT CNPN demand survey (Saral Sanchar portal): https://saralsanchar.gov.in/
- Telecommunications Act 2023 / Trusted Telecom Portal: https://trustedtelecom.gov.in/
- TEC MTCTE (type approval): https://mtcte.tec.gov.in/
- Indian Railways – Kavach: https://indianrailways.gov.in/

International frameworks

- Germany – Bundesnetzagentur (local 3.7–3.8 GHz): https://www.bundesnetzagentur.de/
- Norway – Nkom (3.8–4.2 GHz local licensing & altimeter tests): https://www.nkom.no/
- UK – Ofcom Shared Access Licence: https://www.ofcom.org.uk/
- Canada – ISED Non-Competitive Local Licensing (3900–3980 MHz): https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/spectrum-allocation/decision-non-competitive-local-licensing-framework-including-spectrum-3900-3980-mhz-band-and
- USA – FCC (CBRS Part 96; Lower 4 GHz proceeding): https://www.fcc.gov/
- Netherlands – RDI: https://www.rdi.nl/

Europe harmonisation (3.8–4.2 GHz)

- CEPT ECC Decision (24)01: https://docdb.cept.org/download/4573
- CEPT ECC Report 358 (coexistence): https://docdb.cept.org/document/28615
- Commission Implementing Decision (EU) 2025/2425: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025D2425
- ECC Recommendation (25)03 on protection of FS and FSS in 3.8–4.2 GHz: https://docdb.cept.org/document/28659
- ECC Recommendation (26)02 on protection of altimeters in 3.8–4.2 GHz: https://docdb.cept.org/document/28673
- ECC Recommendation (26)03 on coordination between low- and medium-power terrestrial wireless broadband systems (WBB LMP) in 3800–4200 MHz and protection of MFCN in 3400–3800 MHz (in progress)

Field evidence — Norway altimeter test

- Nkom (primary): https://www.nkom.no/

- Secondary summary (Tarifica): https://tarifica.com/norwegian-test-find-no-5g-interference-with-helicopter-altimeters

Market and device data

- GSA (5G devices & private-network trackers): https://gsacom.com/

Stakeholder positions and the set-aside study

- GSMA – Impact of Spectrum Set-Asides on Private and Public Mobile Networks (2024, PDF): https://www.gsma.com/connectivity-for-good/spectrum/wp-content/uploads/2024/05/Impact-of-Spectrum-Set-Asides-on-Private-and-Public-Mobile-Networks.pdf
- GSMA – Cost of reserving spectrum for private networks (the ~25% claim): https://www.gsma.com/spectrum/examining-the-cost-of-reserving-spectrum-for-private-networks/

Standards (5G → 6G)

- 3GPP (Releases 18–20): https://www.3gpp.org/
- ITU-R M.2160 – IMT-2030 (6G) framework: https://www.itu.int/

Industry bodies

5G Alliance for Connected Industries and Automation (5G-ACIA): https://5g-acia.org

Bharat6G Alliance

Bharat 6G Alliance
2nd Floor, C DoT Campus,
Mandi Road, Mehrauli,
New Delhi- 110030 (INDIA)

info@bharat6galliance.com

www.bharat6galliance.com

