SIAINDIA
An association for space industry

EY
Building a better working world

Reframing Space From "Enabling Layer" to "Critical Infrastructure"

Securing National Resilience and Defence Readiness



The better the question. The better the answer.
The better the world works.

Contents

1 **Executive Summary** 3

1.1 Key Findings 3

1.2 Principal Recommendations at a Glance 3

2 **Introduction and Strategic Context** 4

2.1 The Changing Character of Space 4

2.2 Why the 'Critical Infrastructure' Designation Matters 4

2.3 The Economic and Industrial Case: CI Designation as a Growth Enabler 4

3 **The Strategic Imperative: Reframing Space** 7

3.1 Four Converging Drivers 7

3.2 Figure 1: Global Space Economy Trajectory 7

4 **Global Perspectives and Comparative Analysis** 8

4.1 Country-by-Country Analysis 8

4.2 Five Key Lessons for India 9

5 **India's Space Ecosystem: Progress, Doctrine, and Persistent Gaps** 10

5.1 A Decade of Policy and Institutional Evolution (2015–2026) 10

5.2 The Policy-Capability Gap: Where India Stands Today 10

5.2.1 No Formal Critical Infrastructure Designation 11

5.2.2 Concentrated, Vulnerable Architecture 11

5.2.3 Space Domain Awareness Deficit 11

5.2.4 Defence-Commercial Integration Lag 11

5.3 Persistent Gaps and Priority Areas 11

5.4 The Budget Reality 12

6 **Counterspace Threat Landscape and CI-Enabled Preparedness** 13

6.1 The Spectrum of Counterspace Threats 13

6.2 How CI Designation Transforms Counterspace Preparedness 14

6.3 Structural Mitigations Unlocked by CI Designation 15

7 **Military Use Cases: Space as a Force Multiplier for National Defence** 16

7.1 Space as Critical Infrastructure — A Boon for Military Effectiveness 17

8 **Challenges and Risks: The Cost of the Heavy Lift** 18

8.1 Fiscal Realities and Sustained Funding Requirements 18

8.2 Talent Risk and Human Capital Deficit 18

8.3 Infrastructure Expertise and Technical Complexity 19

9 **Recommendations** 21

10 **Looking Ahead: The Comprehensive Report** 23

11 **Conclusion** 25

12 **References and Key Sources** 26

1 Executive Summary

Space systems have transcended their historical role as a supporting or 'enabling' layer. They are now foundational elements of critical national infrastructure — a fact that ongoing conflicts, Mission Shakti, and India's 2025 Joint Military Space Doctrine all confirm in their own ways. Disruption of Positioning, Navigation & Timing (PNT), Satellite Communications (SATCOM), Earth Observation (EO), or Space Domain Awareness (SDA) would cascade across every critical sector: power grids, financial systems, defence command-and-control, and disaster response.

1.1 Key Findings

- Space is already de facto critical infrastructure. GPS/NavIC underpins power grid timing, banking, telecom, and precision munitions. A major PNT outage could cost economies billions per day.
- Counterspace activities are accelerating. Countries are fielding the full spectrum — kinetic ASAT, co-orbital, directed energy, EW, and cyber. Formal CI designation is the single most powerful organizational tool to mount a structured national defence against these threats.
- Military use cases demand CI-grade protection. From C4ISR and missile early warning to hypersonic tracking and space-based deterrence, every major military capability now depends on space. CI designation directly unlocks defence budget prioritization, faster acquisition, and integrated civil-military response.
- India's foundations are positive but incomplete. The 2023 Space Policy, the 2025 Doctrine, and the 2026 CERT-In Space Cybersecurity Framework are all strong foundations. But no formal CI designation exists, and critical gaps persist in SDA, proliferated architectures, and defence-commercial integration.
- The risks of getting this wrong are severe. The cost of elevating space to CI — financial, institutional, technological — is real, but the cost of inaction is strategic surprise, degraded military effectiveness, and economic disruption at the worst possible moment.

1.2 Principal Recommendations at a Glance

- **Designate** — Formally recognise space systems as Critical Infrastructure, with a designated lead agency and improved cross-ministry coordination.
- **Proliferate** — Expand LEO/MEO small-satellite constellations to strengthen SATCOM, ISR, and NavIC augmentation capabilities.
- **Watch** — Develop a National Space Domain Awareness framework, incorporating advanced sensors and data-sharing partnerships.
- **Integrate** — Enable faster defence–commercial collaboration and advance secure communication standards, including post-quantum approaches.
- **Invest** — Increase space-defence investments over time and build strong talent pipelines to support long-term capability development.

2 Introduction and Strategic Context

2.1 The Changing Character of Space

For decades, space was primarily viewed through the lens of scientific exploration, socio-economic development, and national prestige. India's space program, pioneered by ISRO, exemplified this ethos — delivering transformative benefits in telecommunications, broadcasting, remote sensing for agriculture and disaster management, and weather forecasting. Space was an enabler of national progress.

That paradigm has fundamentally shifted. Space is now a contested operational domain. The conflict in Europe demonstrated how commercial mega-constellations like Starlink provided resilient military connectivity while GPS jamming and spoofing became routine tactical tools — previewing the next war's space dimension. India's own Mission Shakti ASAT test in 2019 and the release of the Joint Military Space Doctrine in September 2025 confirm that India too has internalised this shift. Yet the pace of adversary capability development demands accelerated systemic action.

2.2 Why the 'Critical Infrastructure' Designation Matters

Critical infrastructure comprises systems so vital that their incapacity would have a debilitating impact on national security, economic stability, public health, or safety. Space systems meet this threshold unequivocally:

- PNT (NavIC/GPS): Synchronises power grids, financial transactions, telecom, and precision munitions.
- SATCOM: Beyond-line-of-sight C2 for military operations; remote connectivity; maritime domain awareness.
- Earth Observation & ISR: Persistent surveillance, border monitoring, targeting, battle damage assessment.
- Space Domain Awareness (SDA/SSA): Foundation for safety, deterrence, and attributed response to threats.
- Emerging: Missile warning, environmental monitoring, cislunar strategic positioning.

2.3 The Economic and Industrial Case: CI Designation as a Growth Enabler

The security and resilience rationale for CI designation is well-understood. Less discussed — but equally compelling — is the economic and industrial case. Formal designation as critical infrastructure is not merely a protective label: it is a signal to capital markets, insurers, procurement agencies, and international partners that space assets carry the institutional backing and long-term strategic commitment of the state. This signal directly and materially changes the economics of investing in, operating, and innovating within the space sector.

In comparable sectors — power transmission, airports, ports, highways — CI designation and the associated regulatory certainty have been the primary catalysts for attracting long-term institutional capital at infrastructure-grade cost. The same logic applies to space. The table below maps the principal economic and industrial benefits of CI designation, their mechanisms, and their specific pathways in India's context:

Economic/Industrial Benefit	Mechanism	India-Specific Pathway	Impact on Space Sector
Infrastructure-Grade Financing	Access to long-term debt at infrastructure borrowing rates	Bonds, IN-SPACe-authorized NGE project finance	Lower cost of capital directly reduces the total investment required to build and sustain space systems
Sovereign Guarantee & Credit Enhancement	Government-backed guarantees for project debt reduce lender risk and improve credit ratings of space projects	Partial risk guarantees for priority CI space programs	Unlocks institutional investment (insurance companies, pension funds, sovereign wealth) that cannot currently invest in space assets
Specialized Insurance Products	CI designation triggers development of satellite insurance products at competitive rates; government backstop for systemic risks	IRDA framework extension to CI space assets; Pool-based mutual insurance schemes with reinsurance support	Reduces risk premium priced into space investment; encourages commercial operators to invest in resilience
Long-Term Government Procurement Certainty	Multi-year capacity reservation contracts (government as anchor customer) de-risk commercial investment	10–20 year SATCOM, EO, and launch capacity contracts from MoD, DoT, and NDMA as anchor customers	Provides revenue visibility needed for commercial debt financing; de-risks private investment in large-scale constellations
Investor Confidence and ESG Capital	Formal CI status signals institutional commitment, reducing political risk premium; qualifies as ESG/sustainable infrastructure	Green/blue bonds for space resilience infrastructure; impact investing frameworks; Infrastructure Investment Trusts (InvITs) for space	Attracts domestic and international long-term capital pools that are specifically mandated to invest in resilient national infrastructure
PLI and Fiscal Incentives for CI Compliance	Production-Linked Incentive schemes, customs duty exemptions, and accelerated depreciation for space assets meeting CI resilience standards	Extended PLI for space manufacturing; duty relief on CI-compliant ground infrastructure; R&D tax incentives	Reduces financial burden of CI compliance; transforms compliance from a cost into a competitive advantage for Indian manufacturers
Export Credit and DFC Support	Development Finance Corporation financing for space export projects; EXIM Bank support for Indian	DFC/EXIM financing for Indian SATCOM and launch services exports; NavIC receiver	CI designation adds sovereign credibility to Indian space export offerings; enables G2G financing deals

	space services in Global South markets	manufacturing for allied nations	

Figure A: Economic and Industrial Benefits of Space CI Designation – Mechanisms and India-Specific Pathways

Formal CI designation would trigger:

- Prioritized protection and resilience investment
- Structured public-private information sharing and joint exercises
- Clarified roles, red lines, and escalation response thresholds
- International signaling aligned with like-minded nations
- Accelerated adoption of resilience-by-design and cybersecurity standards

3 The Strategic Imperative: Reframing Space

Leading regions such as the United States, Europe, and Israel are investing in next-generation defence technologies to maintain an edge in a complex and evolving security environment. Key areas of focus include AI-enabled systems to support decision-making, surveillance, and autonomous operations; hypersonic technologies that offer high speed and maneuverability; and directed energy systems aimed at improving precision while reducing logistical demands.

There is also continued emphasis on strengthening cybersecurity and exploring quantum communication to better protect critical infrastructure from advanced threats. In parallel, Europe is advancing defence modernization through increased collaboration and alignment within NATO, with growing attention on autonomous systems, AI-driven platforms, and digital capabilities.

3.1 Four Converging Drivers

a) **Deep Interdependence Across Critical Sectors**: Virtually every critical infrastructure sector now depends on space-derived services. A sustained disruption of PNT or SATCOM cascades into power blackouts, halted financial transactions, grounded aviation, degraded emergency services, and compromised military operations- justifying space assets receiving the same protective rigor as power grids.
b) **Contested and Congested Domain**: Countries are fielding both reversible (jamming, spoofing, cyber, directed energy) and irreversible (kinetic ASAT, co-orbital weapons) counterspace capabilities.
c) **Commercialization and Dual-Use Reality**: Commercial actors now operate the majority of satellites. Starlink utilization showed how commercial capacity can surge to support military needs — creating both resilience opportunity and supply chain vulnerability. India's 2023 Space Policy correctly embraces this turn; the security dimension must be fully integrated into authorization and procurement frameworks.
d) **Economic and Strategic Stakes**: The global space economy exceeded USD 626 billion in 2025 and is projected to surpass USD1 trillion by the early 2030s. For India, the space sector is projected to contribute USD200 billion or more to the economy by 2047 — a direct enabler of Viksit Bharat. Losing assured access to space would undermine these gains and India's aspirations for strategic autonomy.

3.2 Figure 1: Global Space Economy Trajectory

Year	Est. Value	Global Space Economy Growth → $1.8T by ~2035 (E = Estimate)
2023	~$630B	
2035E	~$1,800B	

Sources: World Economic Forum, 'E' = Estimate/Projection.

4 Global Perspectives and Comparative Analysis

The evolution of warfare over the past five years has underscored a dramatic shift in how militaries fight, adapt, and innovate. From Europe to Middle East and the Indo-Pacific, conflicts today are driven less by massed formations and more by networks of precision, autonomy, and real-time data. The following sub-sections examine this transformation through three lenses — weapons actually deployed in warzones, how legacy platforms are adapting, and which disciplines will remain relevant to 2047.

4.1 Country-by-Country Analysis

How leading space powers address the Critical Infrastructure challenge provides essential benchmarks and cautionary lessons for India. The table below provides a structured comparison.

Nation / Bloc	CI Designation Status	Key Institutions & Capabilities
United States	Not yet (active debate)	CISA Space CI WG; SPD-5 Cybersecurity; Space Force est. 2019
United Kingdom	Yes – since 2015	Space as CNI; UK Space Agency; Skynet mil SATCOM
European Union	Yes (EU Space Act)	Space Strategy for Security & Defence; IRIS² constellation
China	Integrated warfighting	PLA Aerospace Force; large ISR constellations; counterspace suite
Russia	Warfighting domain	Kinetic ASAT (2021); GPS jamming/spoofing in Ukraine; EW suite
Japan	Emerging designation	Space Operations Command (2023); SSA satellites; Quasi-Zenith PNT
India	**Not yet designated**	Indian Space Policy 2023; DSA; Joint Space Doctrine 2025; NavIC

4.2 Five Key Lessons for India

- Value of designation: Formal CI status can help strengthen resource allocation, improve coordination frameworks, and signal the importance of space systems within national policy.
- Resilience over concentration: More distributed, multi-orbit architectures with built-in redundancy may offer greater long-term reliability compared to reliance on a small number of high-value satellites.
- Role of commercial integration: Integrating commercial space capabilities into defence frameworks is becoming increasingly important. The US approach, which combines commercial services with a sovereign core, provides a useful reference point.
- Importance of SDA/SSA: Effective space domain awareness is a key enabling factor for monitoring, decision-making, and response planning in the space environment.
- Need for a coordinated approach: Closer alignment across institutions — including ISRO, DSA, and NCIIPC — can support a more cohesive response to evolving space-related challenges.

5 India's Space Ecosystem: Progress, Doctrine, and Persistent Gaps

5.1 A Decade of Policy and Institutional Evolution (2015–2026)

India's space program has undergone the most significant institutional transformation in its history over the past decade. From a largely government-monopoly model centred on ISRO, the ecosystem has diversified into a multi-stakeholder architecture spanning civil, commercial, and defence dimensions.

The Indian Space Policy 2023 is the watershed event. It established IN-SPACe as the single-window authorisation and promotion body for both government and non-government entities (NGEs) across the full space value chain — launch vehicles, satellite manufacturing, ground systems, and applications. NewSpace India Limited (NSIL) serves as ISRO's commercial arm. Together, these instruments have catalysed a vibrant startup ecosystem — with over 250 space startups in India by 2026 — and attracted foreign investment into Indian space manufacturing and services. India has authorised hundreds of NGE activities in just three years, a pace that would have been unthinkable a decade ago.

On the defence side, the Defence Space Agency (DSA), established in 2019 by merging the Defence Imagery Processing and Analysis Centre (DIPAC) and the Defence Satellite Control Centre (DSCC), represents the armed forces' dedicated space organisation. It has conducted India's first space war game — IndSpaceEx — in 2019 and contributed to doctrine development. The landmark Joint Military Space Doctrine, released on 16 September 2025 at the Combined Commanders' Conference, formally elevated space to a warfighting domain alongside land, maritime, air, and cyber. The doctrine emphasises space-centric operations, protection of space assets, risk mitigation, and integrated joint operations.

The February 2026 CERT-In Cybersecurity Framework and Guidelines for Space — issued in collaboration with SIA-India — adds the third pillar: a governance and technical architecture for cybersecurity across the space, ground, link, and user segments. It mandates Security-by-Design, Zero-Trust Architecture, mandatory CSSO appointment, SBOM requirements, 6-hour incident reporting, and a Satellite Security Operations Centre (Sat-SOC) for all space entities. This is the most comprehensive space-sector cyber governance framework India has produced, placing it among the world's leading nations on space cyber policy.

5.2 The Policy-Capability Gap: Where India Stands Today

Despite the strong policy foundation, a significant and widening gap exists between India's policy ambitions and actual in-orbit capability, particularly for defence purposes. This gap is most acute in four areas:

5.2.1 No Formal Critical Infrastructure Designation

Space assets are not currently designated as Critical Infrastructure or Critical Information Infrastructure (CII) under the NCIIPC framework. As a result, there is no clearly defined lead agency for space asset protection, limited formal mechanisms for public-private information sharing on space-related risks, and no uniform requirement for continuous cyber monitoring of civilian space infrastructure. Baseline protection standards for operators, including those authorised by IN-SPACe, are still evolving. While CERT-In provides guidance on cybersecurity, it does not fully replace the broader coordination and risk management role associated with a formal CI designation.

5.2.2 Concentrated, Vulnerable Architecture

India's space capabilities are currently centred around a relatively small number of high-value satellites. This concentration means that disruptions — whether technical, cyber, or otherwise — could have a noticeable impact on critical services, especially given the time required to replace such assets. Efforts to move towards more distributed and resilient architectures (including LEO/MEO systems) are underway but are still at an early stage, and current programmes only address select capability areas.

5.2.3 Space Domain Awareness Deficit

India has made progress in tracking space objects through initiatives such as the ISSA centre, but overall space domain awareness capabilities continue to develop. Limitations in sensor coverage, weather-dependent systems, and data integration affect the ability to monitor and interpret space activities in real time. Dedicated space-based monitoring capabilities and advanced data fusion tools could further strengthen situational awareness over time.

5.2.4 Defence-Commercial Integration Lag

India's commercial space ecosystem is expanding, supported by IN-SPACe authorisations, but frameworks for integrating commercial capabilities into defence use are still maturing. Mechanisms for systematically leveraging commercial services — such as satellite imagery, communications, and tracking data — are not yet fully institutionalised. Areas such as long-term contracting models, security clearance processes, and supply chain assurance for defence applications are developing gradually.

5.3 Persistent Gaps and Priority Areas

Capability Area	Current Status	Priority	Lead Action / Remarks
Formal CI Designation	Absent	Critical	NSC/DoS notification
Proliferated LEO SATCOM	Nascent (SBS-III)	Critical	DSA + private sector
Space Domain Awareness (SDA)	Limited	Critical	National SDA Centre
Defence Space Command	DSA (transitional)	High	MoD/CDS mandate

Rapid Reconstitution/Launch	Early (SSLV)	High	ISRO + private launchers
NavIC Global Coverage	Regional	High	DoS / ISRO
Cyber Resilience (Ground)	Framework issued	High	CERT-In / IN-SPACe
Defence-Commercial Integration	Ad hoc	High	MoD / IN-SPACe / DPIIT
Supply Chain Indigenisation	Partial	Medium	PLI + DRDO + industry
Space Human Capital	Scarce	Medium	Education + retention

Figure 3: India Space Capability Gap Matrix — Priority Assessment and Lead Actions.

5.4 The Budget Reality

India's Department of Space budget for FY 2026–27 is approximately INR 13,700 crore (~USD 1.65 billion), covering ISRO's civil, scientific, and commercial programmes, as well as contributions to the defence space ecosystem. In comparison, the United States spends around USD 67 billion annually on government space activities, China about USD 14 billion, and the European Union collectively around USD 12 billion.

India's allocation remains consistent with its current economic scale and stage of space development. However, it also means that pursuing multiple priorities in parallel — including commercial expansion, resilient defence constellations, space domain awareness infrastructure, human spaceflight, and next-generation launch systems — requires careful sequencing and prioritisation.

A calibrated increase in funding, particularly directed towards resilience, space domain awareness, and defence space capabilities, could help support India's longer-term strategic objectives in the space sector.

6 Counterspace Threat Landscape and CI-Enabled Preparedness

India's space security environment is evolving with the steady development of counterspace capabilities by other major powers. These developments highlight a growing set of risks that can affect not only satellites but also the broader systems — economic, civilian, and military — that rely on space-based services.

Understanding these risks is important not only for defence planning but also for shaping policy responses, including the potential designation of space assets as Critical Infrastructure. Counterspace challenges extend beyond individual assets to the wider networks they support, suggesting the need for a comprehensive and system-level approach. Viewed in this broader context, the rationale for considering space as Critical Infrastructure becomes more clearly aligned with long-term resilience and preparedness goals.

6.1 The Spectrum of Counterspace Threats

Counterspace capabilities span a spectrum from reversible (effects are temporary and recoverable) to irreversible (permanent damage or destruction), and from direct (physical attack on a satellite) to indirect (attack on ground infrastructure or communication links). The key threat categories are:

- Kinetic Anti-Satellite (ASAT): This involves physically disabling a satellite using interceptor systems. Several countries have demonstrated such capabilities through tests, highlighting both their strategic significance and the potential risks, including the creation of orbital debris. While these systems may contribute to deterrence, they also raise concerns about escalation and the long-term sustainability of the space environment.
- Co-orbital capabilities: Some space systems are designed to operate in close proximity to other satellites for purposes such as inspection, maintenance, or observation. However, these capabilities could also be used in ways that interfere with or disrupt other satellites, making them difficult to interpret and respond to in the absence of clear operational norms.
- Directed energy systems: Ground-based technologies, such as lasers or high-power microwave systems, have the potential to interfere with satellite sensors or electronics. Depending on their use, these effects can range from temporary disruption to longer-term performance degradation.
- Electronic interference (jamming and spoofing): Techniques such as jamming (overpowering signals) and spoofing (introducing misleading signals) can disrupt satellite-based services like communication and navigation. These methods are relatively accessible compared to other counterspace capabilities and can be difficult to attribute with certainty.
- Cyber vulnerabilities: Space systems rely heavily on ground infrastructure and digital networks, which can be targeted through cyber means. Incidents in recent years have

shown that disruptions to ground systems can significantly affect satellite-enabled services, underlining the importance of robust cybersecurity measures.

- Supply chain risks: The development of space systems involves complex and often global supply chains. This can introduce potential vulnerabilities, such as compromised components or software, which may affect system reliability if not carefully managed.

6.2 How CI Designation Transforms Counterspace Preparedness

The critical insight — and the reason this section deliberately pairs counterspace threats with CI designation — is that formal designation is not just a policy label. It is the institutional mechanism that transforms India's ability to prepare for, resist, and recover from counterspace activities. Here is precisely how:

Threat Vector	Effect / Potential Impact	CI Designation-Enabled Mitigation
Kinetic ASAT	Satellite destruction; catastrophic debris cascade	Disaggregated LEO constellations; rapid reconstitution; deterrence messaging
Co-orbital Weapons	On-orbit surveillance, interference or disabling	SDA tracking; maneuvering; CI designation enables priority response
Directed Energy (DEW)	Sensor dazzling; component damage; communications disruption	Satellite hardening; maneuver capability; anomaly detection via SDA SOC
Electronic Warfare (EW)	Jamming/spoofing of uplink, downlink and PNT signals	Anti-jam FHSS; NavIC redundancy; CI designation triggers EW resilience mandate
Cyber Intrusion	Ground segment / satellite C2 compromise; data exfiltration	CERT-In framework; ZTA; CSSO mandate; segmentation; incident reporting
Signal Spoofing	False PNT/navigation data; misrouting of critical communications	Crypto authentication; multi-constellation PNT; NavIC independence
Supply Chain Attack	Hardware/firmware backdoors in satellites or ground equipment	Trusted supply chain policy; SBOM/HBOM audits; CI designation enables stricter vendor mandates
Cyber-Physical Hybrid	Combined cyber intrusion plus physical proximity operations	Integrated SDA + cyber monitoring; whole-of-government CI response protocols

Figure 4: Counterspace Threat Vectors and CI Designation-Enabled Mitigations

6.3 Structural Mitigations Unlocked by CI Designation

- Mandated resilience standards: Designating space systems as critical infrastructure can provide a policy basis for establishing minimum resilience requirements across civil, commercial, and defence operators. This may include measures such as redundancy, signal protection, and cybersecurity practices. Such standards could be incorporated into regulatory approvals (e.g., via IN-SPACe) or procurement processes, helping move from largely voluntary practices toward more consistent implementation.
- Cross-sector continuity planning: A critical infrastructure approach can support the development of coordinated continuity plans for services that depend on space systems. This would involve identifying alternative solutions — such as backup navigation or communication options — and preparing them for use during disruptions. At present, such planning is still evolving and may benefit from a more structured, national-level framework.
- Intelligence and warning integration: CI designation can also encourage more regularized information-sharing arrangements among relevant agencies, including technical, intelligence, and cybersecurity bodies. This could improve early awareness of potential threats, such as unusual satellite activity, signal interference, or cyber incidents, while reducing reliance on ad hoc coordination.
- Policy signalling and response posture: Recognizing space assets as critical infrastructure can help clarify their importance within the broader national security framework. It may also signal a commitment to protecting these systems and responding appropriately to disruptions, contributing to clearer expectations among stakeholders.
- Coordinated response mechanisms: Establishing CI status can support the creation of pre-defined processes for managing incidents affecting space systems, including clear roles, escalation pathways, and response options. This can help reduce uncertainty and improve coordination during time-sensitive situations, compared to relying on improvised responses.

Key Insight: Counterspace risks extend beyond the military domain.

Disruptions to civilian systems like GPS can affect multiple sectors at once, including power, banking, aviation, and telecom. Cyber incidents targeting civilian infrastructure may also affect defence operations, while supply chain vulnerabilities in commercial systems can have wider implications.

These overlaps suggest the need for a coordinated, cross-sector approach. A critical infrastructure framework can help align stakeholders and improve overall resilience.

7 Military Use Cases: Space as a Force Multiplier for National Defence

The 2025 Joint Military Space Doctrine correctly identifies space as a warfighting domain — not merely a support function. But the doctrine's significance is best understood by mapping the concrete military use cases that depend on space, understanding how CI designation amplifies each one, and identifying how India can be better prepared. Space is not one military capability; it is the connective tissue binding together all modern military operations.

The table below provides a comprehensive mapping of India's military space use cases, their strategic purpose, the current capability development pathway, and the direct benefit that CI designation would deliver for each:

Military Use Case	Strategic Purpose	India Capability Path	CI Designation Benefit
C4ISR & Battlefield Connectivity	Continuous, jam-resistant SATCOM for joint ops across LAC, IOR, Indo-Pacific	Secure military SATCOM constellation; BLOS data links for all commands	CI designation enables priority hardening and defence budget ring-fencing
Precision Navigation (PNT)	Guidance for precision munitions, drone swarms, autonomous vehicles	NavIC + LEO PNT augmentation; anti-jam receivers in all platforms	CI status compels investment in NavIC redundancy and user equipment mandates
Space-Based ISR	Persistent wide-area surveillance for border, maritime, targeting and BDA	Cartosat-3, RISAT successors; hyperspectral + SAR constellation	CI designation unlocks faster MoD-DoS acquisition pathways for ISR satellites
Missile Early Warning	Detection of ballistic and hypersonic missile launches for air defence cueing	Space-based IR sensors + integration with Prithvi Air Defence	CI framework mandates continuous monitoring and inter-agency data sharing
Electronic Intelligence (ELINT)	Collection of adversary radar, communication and EW signatures	SIGINT/ELINT small satellites in LEO; rapid data downlink	CI status justifies dedicated classified commercial-defence partnerships
Space Domain Awareness (SDA)	Real-time tracking of threats, debris, and adversary satellite manoeuvres	National SDA Centre; optical + radar sensors; AI/ML fusion	CI designation creates the legal and institutional mandate for a national SDA Centre

Cyber & EW Support	Space relay for cyber operations; EW geolocation and spectrum management	Dedicated communication relay satellites; SIGINT payloads	CI framework integrates CERT-In space security mandates into military procurement
Disaster & Civil-Military Ops	Rapid imagery and communications for HADR and domestic security	Dual-use EO and SATCOM constellations accessible to all agencies	CI designation enables pre-authorized civil-military data sharing protocols

Figure 5: Military Space Use Cases — Strategic Purpose, Capability Path, and CI Designation Benefit

7.1 Space as Critical Infrastructure — A Boon for Military Effectiveness

The argument for CI designation is often framed in defensive, risk-mitigation terms. But the military dimension reveals an equally compelling offensive-effectiveness case: CI designation is not only about protecting what we have — it is about accelerating what we need.

- Budget prioritization and ring-fencing: Designating space systems as critical infrastructure can provide a stronger basis for allocating dedicated funding within the defence budget. This may help reduce the impact of competing priorities that often affect long-term capability development, and could support more consistent investment in space-related programs.
- Acquisition pathway acceleration: Such a designation could allow greater use of expedited procurement mechanisms, including streamlined approval processes or mission-mode programs, for space capabilities that support essential defence functions. This is particularly relevant in contexts where conventional acquisition cycles tend to be lengthy relative to the pace of technological change.
- Civil-military data integration: Critical infrastructure status can help enable clearer frameworks for data sharing between civil space agencies (such as ISRO), commercial operators, and defence organizations during contingency situations. Advance arrangements for accessing commercial imagery or communication bandwidth may improve responsiveness in time-sensitive scenarios.
- Interoperability with allies: As India deepens cooperation with Global South partners and others, aligning governance approaches with those of countries that already treat space systems as critical infrastructure could support smoother collaboration. This may include enhanced data sharing, joint activities, and gradual improvements in interoperability.
- Deterrence through demonstrated commitment: Clearly signaling the importance of space systems, along with building mechanisms to protect and sustain them, may contribute to shaping how potential adversaries assess risks. Strengthening resilience and response capabilities can play a role in discouraging disruptive actions by increasing uncertainty about their effectiveness.

8 Challenges and Risks: The Cost of the Heavy Lift

Making space Critical Infrastructure is not a costless policy choice. It demands sustained, multi-decade investment; institutional reorganization; and the resolution of genuine technical, human, and geopolitical challenges. A realistic assessment of these issues is essential to inform credible planning. The following outline the main challenges likely to accompany this transition:

8.1 Fiscal Realities and Sustained Funding Requirements

The level of investment required to more fully position space as critical infrastructure is likely to be considerable. Developing capabilities such as more distributed satellite constellations, improved space domain awareness systems, expanded navigation coverage, and supporting institutional capacity will require sustained and coordinated funding across both civil and defence sectors.

While precise estimates vary, current spending levels may need to increase meaningfully over time to align with evolving requirements and ensure adequate resilience. This underscores the importance of long-term planning, prioritization, and resource allocation to support a broader shift in how space capabilities are developed and maintained.

- Sustaining long-term commitment: Space initiatives typically involve extended development timelines, often spanning multiple years. This makes it important to ensure continuity in policy support and funding across changing priorities, electoral cycles, and economic conditions. More predictable, multi-year funding approaches could help improve planning and execution.
- Managing trade-offs and competing priorities: Investment in space capabilities must be balanced against other national requirements, including broader defence modernization and socio-economic priorities. As a result, decisions on resource allocation will need to be carefully evaluated within existing institutional and budgetary processes.
- Balancing commercial and public investment: Greater participation from the private sector can play an important role in expanding space capabilities. However, commercial investment is typically guided by market considerations, which may not always align with strategic or security needs. Public investment may therefore remain necessary to support areas that are less commercially viable but nationally important.

8.2 Talent Risk and Human Capital Deficit

Space systems engineering is among the most specialized technical disciplines in the world. Building and operating a resilient, multi-orbit, AI-enabled national space architecture requires deep expertise across orbital mechanics, RF systems, onboard software, cybersecurity, AI/ML operations, and space policy — a combination that does not emerge from general STEM education pipelines. India faces a specific talent challenge in this domain:

- Limited talent pipeline: While India produces a large number of engineering graduates annually, the subset with specialized expertise in space systems remains relatively

small. Public institutions and private players often draw from the same talent pool, which can create constraints in meeting growing demand.

- Talent retention challenges: Highly skilled professionals in the space sector are increasingly mobile and may be attracted by opportunities abroad or in the private sector. Ensuring competitive compensation, meaningful roles, and clear career progression within domestic institutions will be important for retention.
- Gaps in specialized skills: Certain niche areas—such as space cybersecurity and advanced systems operations—currently have a limited talent base. Building capacity in these domains may take time, particularly as new frameworks and requirements are introduced.
- Training and institutional development needs: The evolution of space as an operational domain will require corresponding investments in training, professional specialization, and organizational structures. Developing dedicated career pathways and deep expertise will be a gradual but necessary process to support emerging frameworks and doctrines.

8.3 Infrastructure Expertise and Technical Complexity

Space systems are arguably the most complex engineering systems humans build. The gap between writing policy and fielding capability is wide, and filled with technical pitfalls:

- **Ground infrastructure concentration:** India's space ground infrastructure — including TT&C stations, mission control centres, and data reception facilities — is currently concentrated in a limited number of locations, which could present potential vulnerabilities. Expanding and strengthening this network through additional sites, redundancy, and improved security measures would require considerable investment and technical effort.
- **Legacy system integration:** Much of India's existing satellite fleet was developed without modern cybersecurity and resilience requirements in mind. Updating these systems with newer approaches — such as advanced encryption, Zero-Trust frameworks, and monitoring tools — can be technically challenging and may need careful execution to avoid operational disruptions. While CERT-In provides guiding standards, implementation capabilities vary across stakeholders.
- **Private sector capability maturity:** India's space startup ecosystem is growing quickly but remains at an early stage. Some new entrants authorized by IN-SPACe may still be developing the technical and organizational depth needed for high cybersecurity and resilience standards. Supporting this growth while maintaining security expectations may require continued regulatory guidance, skill development, and possibly shared support mechanisms.
- **Interoperability challenges:** Creating a coordinated system where satellites from different operators and orbits can work together involves developing common technical standards — for data handling, communication protocols, and system interfaces. These standards are still evolving within India's emerging space ecosystem, which may pose gradual integration challenges.

Summary: The Cost of Inaction Exceeds the Cost of Action

The challenges outlined above are real. But they are manageable with political will, sustained investment, and institutional reform.

The alternative — continuing without CI designation, with concentrated vulnerable assets, inadequate SDA, and no continuity planning — is not a stable equilibrium.

In a conflict scenario, the cost of space disruption — measured in degraded military effectiveness, cascading civilian impacts, and lost strategic autonomy — would dwarf any investment India makes today in getting this right.

9 Recommendations

The following are India's highest-priority, most impactful actions to secure space as Critical Infrastructure, strengthen defence readiness, and address the counterspace threat. These are presented as direct, actionable recommendations – not timelines or phases.

PILLAR 1 – PROTECTION: Securing the Foundation

1. Consider Formal Recognition of Space Systems as Critical Infrastructure

Evaluate the designation of key space-based and ground-based systems—such as satellites, control facilities, and communication networks—as critical national infrastructure. Where appropriate, extend related classifications to relevant digital and information systems to strengthen governance and protection mechanisms.

2. Enhance Resilience Through Diverse Satellite Architectures

Promote the development of more distributed and resilient space systems, including the potential use of multiple orbital layers and constellations. Such approaches can help improve continuity and reduce vulnerabilities

3. Develop a National Capability for Space Domain Awareness

Explore the establishment of a coordinated, multi-agency framework for monitoring activities in space. This could include the integration of terrestrial and space-based sensors, along with advanced data analytics to support timely awareness and response.

4. Review and Prioritize Investment in Space Security and Resilience

Assess current funding frameworks to ensure adequate and sustained investment in areas related to space security, resilience, and operational capability, aligned with evolving requirements.

5. Improve Positioning, Navigation, and Timing (PNT) Capabilities

Continue to expand and reinforce independent navigation systems while exploring complementary technologies and backup options. A diversified approach to PNT can improve reliability and strategic autonomy.

PILLAR 2 – INDUSTRIAL GROWTH: Enabling the Space Economy

1. Strengthen Collaboration Between Defence and Commercial Space Sectors

Create structured mechanisms to facilitate the use of commercial space capabilities for national requirements. This may involve streamlined onboarding processes, clearer regulatory pathways, and measures to ensure supply chain reliability.

2. Space Infrastructure Financing

Expand access to infrastructure financing for strategically significant assets through blended finance and risk-sharing mechanisms, encourage the use of innovative funding models such as investment trusts and market-based bonds to support large-scale development, and establish

dedicated funding vehicles to enhance resilience and enable coordinated, cross-sector investments in critical capabilities

3. PLI and Fiscal Incentives for Compliance

Design PLI extensions, customs duty relief, and accelerated depreciation for space manufacturers meeting CI resilience standards — transforming compliance from a cost into a competitive incentive for the domestic industry

4. Procurement Certainty for Industry

Enable long-term service agreements with public agencies acting as anchor customers to provide demand certainty, thereby improving revenue visibility for service providers and helping attract commercial financing for capacity development in critical infrastructure sectors.

PILLAR 3 — INNOVATION & COMPETITIVENESS: Leading the Future

1. Build and Sustain Specialized Human Capital

Support the development of skilled talent through dedicated training programs, academic partnerships, and clear career pathways in space-related domains. Emphasis on emerging areas such as cybersecurity and advanced analytics can be particularly valuable.

2. AI/ML for Space Operations

Support focused research and innovation efforts in emerging technologies such as autonomous operations, anomaly detection, data fusion, and predictive upkeep systems.

3. Global Norms Leadership

Promote broader international collaboration and capacity-building in responsible operational practices, while using leadership in setting standards to strengthen strategic and diplomatic positioning

10 Looking Ahead: The Comprehensive Report

This white paper is intended as a high-level strategic overview and a catalyst for further dialogue. It outlines the rationale for recognizing space as critical infrastructure, including the policy context, global benchmarks, domestic ecosystem and gaps, emerging threats, defence applications, and potential economic gains.
A more detailed companion report, currently under development, will expand on these themes and provide deeper analysis. Key areas of focus are expected to include:

#	Indicative Focus Areas for the Comprehensive Report	Potential Coverage
1.	Roadmap and Phased Implementation Framework	A phased roadmap outlining institutional setup, regulatory rollout, and investment sequencing—providing a clear pathway for operationalising CI designation.
2.	Global Best Practices, Lessons Learned and Benchmarking	Comparative assessment of how leading space-faring nations have approached CI designation, distilling actionable insights tailored to India's strategic and institutional context
3.	Economic, Industrial and Investment Implications of CI Designation	Evaluation of the broader economic impact, including capital mobilisation, industrial expansion, employment generation, and implications for India's commercial space ecosystem.
4.	Space Infrastructure Financing Framework	Exploration of financing mechanisms aligned with infrastructure status, including long-tenor capital, credit enhancements, blended finance structures, and institutional funding channels
5.	Incentives versus Compliance Obligations	Balanced framework aligning resilience and security obligations with fiscal, regulatory, and market-based incentives to ensure industry participation and investment attractiveness.
6.	Governance and Institutional Architecture	View of the governance model, including roles of key agencies, inter-ministerial coordination, and decision-making structures required for effective implementation.
7.	Critical Asset Identification and Classification Methodology	Identification and classification of space assets based on criticality, substitutability, and risk exposure—informing differentiated protection and compliance requirements
8.	Public-Private Partnership Models	Evaluation of partnership structures and risk-sharing models to enable private sector

		participation while safeguarding strategic control.
9.	Strategic Procurement and Market-Creation Opportunities	Analysis of how long-term government procurement can be leveraged to create demand certainty, crowd-in private investment, and scale domestic capabilities.
10.	Supply-Chain Resilience and Industrial Base Strengthening	Identification of critical supply chain vulnerabilities and development of strategies for indigenisation, diversification, and resilience-building.
11.	International Cooperation, Interoperability and Cross-Border Best Practices	Exploration of strategic partnerships, interoperability frameworks, and cross-border collaboration models to strengthen India's position in the global space ecosystem.

11 Conclusion

The evolving role of space—from a supporting enabler to a more central element of national capability—is increasingly apparent. India has made important progress in this direction, including policy measures that encourage commercial participation, the formal acknowledgment of space in military thinking, and the introduction of cybersecurity frameworks to strengthen technical governance.

These developments are best understood as foundational steps rather than final milestones. The broader strategic environment suggests that many countries are expanding and integrating capabilities related to space, including measures designed to counter or contest its use. As a result, space is gradually being incorporated into wider security and operational considerations.

Recognizing space as critical infrastructure could have several implications. It may influence how risks are assessed, how resources are prioritized, and how resilience and coordination mechanisms are developed across institutions. It can also help signal intent and commitment to domestic stakeholders and international partners.

At the same time, there are practical challenges, including funding constraints, talent availability, infrastructure demands, and the balance between norms and capabilities. These considerations highlight the importance of a sustained, well-coordinated approach rather than acting as reasons to delay progress. The potential consequences of insufficient preparation—across security, economic stability, and operational effectiveness — underscore the need for thoughtful planning and investment.

India's experience in space has demonstrated its ability to pursue long-term objectives with efficiency and clarity. Building on that foundation, the next phase will likely require a combination of institutional adaptation, private-sector participation, and evolving strategic frameworks suited to a changing environment.

The Bottom Line:

Space is not a luxury — it is load-bearing infrastructure for the Indian state.
It is the backbone of modern warfare, economic continuity, and sovereign decision-making.
Treating it as anything less than Critical Infrastructure is a strategic choice India can no longer afford to make.

12 References and Key Sources

- Indian Space Policy 2023, Department of Space, Government of India.
- Joint Military Space Doctrine, Headquarters Integrated Defence Staff, September 2025.
- CERT-In: Cyber Security Framework and Guidelines for Space including Satellite Communication, February 2026 (in collaboration with SIA-India).
- Space Critical Infrastructure White Paper: Reframing Space from Enabling Layer to Critical Infrastructure, June 2026 (companion document).
- 'Time to Designate Space Systems as Critical Infrastructure,' Cybersolarium Commission / CSC 2.0, 2023.
- 'Designating the U.S. Space Sector as Critical Infrastructure,' Intelligence and National Security Alliance (INSA), 2022.
- Space Policy Directive-5: Cybersecurity Principles for Space Systems, The White House, 2020.
- EU Space Strategy for Security and Defence, European Union, 2023.
- ENISA Space Threat Landscape 2025.
- CISA Recommendations to Space System Operators for Improving Cybersecurity, 2025.
- NIST: Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN); NIST IR 8270.
- MITRE: Cyber Best Practices for Small Satellites; MITRE ATT&CK for Space Systems.
- Novaspace Space Economy Reports; Space Foundation The Space Report (2024–2025).
- World Economic Forum Space Report
- CSIS Aerospace Security Project — Space Threat Assessments and Counterspace Reports (2023–2026).
- CCSDS 355.0-B-2: Space Data Link Security. ECSS-E-ST-80C: Space Systems Cybersecurity.
- Union Budget documents: Department of Space allocations, FY 2025-26 and 2026-27.

Our offices

Ahmedabad

22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind Iskcon Temple
Off SG Highway
Ahmedabad - 380 059
Tel: + 91 79 6608 3800

8th Floor, Building No. 14A
Block 14, Zone 1
Brigade International Financial Centre
GIFT City SEZ
Gandhinagar - 382355, Gujarat
Tel +91 79 6608 3800

Bengaluru

12th & 13th Floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground & 1st Floor
11, 'A' wing
Divyasree Chambers
Langford Town
Bengaluru - 560 025
Tel: + 91 80 6727 5000

3rd & 4th Floor
MARKSQUARE
#61, St. Mark's Road
Shantala Nagar
Bengaluru - 560 001
Tel: + 91 80 6727 5000

1st & 8th Floor, Tower A
Prestige Shantiniketan
Mahadevapura Post
Whitefield,
Bengaluru - 560 048
Tel: + 91 80 6727 5000

Bhubaneswar

8th Floor, O-Hub, Tower A
Chandaka SEZ, Bhubaneswar
Odisha – 751024
Tel: + 91 674 274 4490

Chandigarh

Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai

6th & 7th Floor, A Block,
Tidel Park, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR

Aikyam
Ground Floor
67, Institutional Area
Sector 44, Gurugram - 122 003
Haryana
Tel: +91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel: + 91 120 671 7000

Hyderabad

THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jaipur

9th floor, Jewel of India
Horizon Tower, JLN Marg
Opp Jaipur Stock Exchange
Jaipur, Rajasthan – 302018

Kochi

9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata

22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

Mumbai

14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

3rd Floor, Unit No.301
Building No.1, Mindspace-Gigaplex
IT Park, MIDC, Plot No. IT-5
Airoli Knowledge Park
Airoli West, Navi Mumbai - 400 708
Tel: + 91 22 6192 0003

Altimus, 18th Floor
Pandurang Budhkar Marg
Worli, Mumbai - 400 018
Tel: +91 22 6192 0503

Pune

C-401, 4th Floor
Panchshil Tech Park, Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

10th Floor, Smartworks
M-Agile, Pan Card Club Road
Baner, Taluka Haveli
Pune - 411 045
Tel: + 91 20 4912 6800

Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram - 122 003, Haryana, India.

© 2025 Ernst & Young LLP. Published in India.
All Rights Reserved.

ED None.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ey.com/en_in

@EY_India EY YouTube EY India EY Careers India @ey_indiacareers

SIA-INDIA

SIA-India is a non-profit organization representing the interests of the space industry in India. Our membership includes satellite operators, manufacturers, suppliers, startups, academic institutions, and law firms. The association is committed to serve as a voice for the industry and represent the industry's interests at policy making and regulatory bodies. SIA-India also offers a platform to forge international collaborations and provides an interface with the government.