SIA INDIA
An association for space industry

DEFSAT
CONFERENCE & EXPO

SPACE, STRATEGY & THE FUTURE WORLD ORDER

PERSPECTIVES FROM

DEFSAT 2026



www.sia-india.com
info@sia-india.com
+91-11-4604 8743

© 2026 SatCom Industry Association-India (SIA-India). All Rights Reserved.

Acknowledgment

TOC

MESSAGE FROM THE PRESIDENT



It is a privilege to present Space, *Strategy & the Future World Order: Perspectives from DEFSAT 2026*, a publication that captures the strategic insights, debates, and recommendations emerging from one of India's foremost platforms on defence, security, and space.

Over the past four years, DEFSAT has evolved from a focused industry conference into a national forum that brings together military leaders, policymakers, scientists, industry pioneers, technology innovators, and strategic thinkers to examine the rapidly changing relationship between space and national security. What began as a discussion on defence-space capabilities has matured into a broader conversation about resilience, strategic autonomy, technological leadership, industrial capacity, and the future architecture of national power.

This evolution reflects a larger transformation taking place globally. Space is no longer viewed solely as a domain of exploration, scientific achievement, or technological prestige. It has become an essential layer of modern infrastructure underpinning communications, navigation, intelligence, surveillance, disaster response, financial systems, critical services, and military operations. As nations become increasingly dependent on space-enabled capabilities, the security, resilience, and sustainability of these systems are emerging as critical strategic priorities.

India enters this new era from a position of considerable strength. The country's space ecosystem has expanded significantly in recent years, supported by progressive policy reforms, a growing private sector, increasing investment, and a vibrant innovation landscape. The Indian space economy, currently valued at approximately USD 8.4 billion, is projected to exceed USD 40 billion by 2040. More importantly, India is developing the institutional, industrial, and technological foundations necessary to translate space capability into long-term strategic advantage.

The discussions at DEFSAT highlighted several important realities. Future security will depend not only on access to space but on the ability to secure critical infrastructure, sustain persistent capabilities, build resilient industrial ecosystems, leverage artificial intelligence and geospatial intelligence, strengthen international partnerships, and integrate space into broader national security and resilience frameworks. The future contest for advantage will increasingly be defined by resilience, connectivity, decision superiority, and the ability to operate effectively across interconnected domains.

This book reflects how space is reshaping military power, geopolitical competition, industrial development, homeland security, decision-making, and international cooperation.

As India advances towards becoming a leading space power, the challenge before us is no longer simply to build capabilities. It is to build enduring capacity—supported by strong institutions, innovative industries, trusted partnerships, resilient infrastructure, and a clear strategic vision. The decisions taken during the coming decade will shape not only the future of India's space sector but also its role in the evolving global security landscape. It is our hope that this volume contributes meaningfully to that national conversation and helps advance a shared vision of a secure, resilient, and globally competitive Indian space ecosystem.



Dr. Subba Rao Pavuluri
President, SIA-India

Foreword

The strategic character of the twenty-first century is being reshaped by forces that transcend conventional geographical boundaries. Nations are no longer competing solely across land, sea, and air; they are increasingly contesting the invisible yet indispensable domain of outer space. Satellites, orbital communication systems, navigation constellations, surveillance architectures, and cyber-enabled space infrastructure now form the backbone of economic systems, military operations, financial networks, governance mechanisms, and international connectivity. In this rapidly evolving strategic environment, the defence of space infrastructure has emerged not as a niche technological concern but as a foundational requirement for national resilience and sovereignty.

The discussions and deliberations at DEFSAT 2026 reflected this historic transition with remarkable clarity. Across panels involving military leaders, policymakers, technologists, industry experts, and strategic thinkers, one central reality became increasingly evident: the future of warfare, geopolitical competition, and strategic influence will be inseparable from the control, protection, and resilience of space-enabled systems.

This book emerges from that realization. It seeks to examine the changing strategic landscape through three interconnected dimensions. The first explores the growing vulnerability of space as national critical infrastructure and the urgent requirement for cyber resilience, spectrum security, and electronic warfare preparedness. The second examines the transformation of warfare itself, highlighting how military doctrine, strategic competition, and technological evolution are converging within the orbital domain. The third analyses the geopolitical implications of defence-space cooperation, alliance structures, and the emergence of technologically integrated strategic ecosystems.

Together, these chapters present a coherent narrative of a world entering an era of orbital geopolitics and network-centric conflict. The rise of artificial intelligence, autonomous systems, hypersonic weapons, distributed constellations, and integrated ISR architectures is transforming not only the conduct of war but also the nature of alliances, deterrence, and strategic power.

For India, these transformations carry particular significance. As a rising technological and geopolitical power situated at the centre of the Indo-Pacific strategic landscape, India faces both extraordinary opportunities and profound strategic challenges. The nation's future security posture will increasingly depend upon its ability to integrate sovereign technological capability, institutional coordination, resilient infrastructure, and trusted strategic partnerships into a coherent national framework.

The chapters that follow do not merely discuss satellites or military technology. They examine the emerging architecture of power in the modern era. They argue that the defence of invisible orbital networks may ultimately become as important as the defence of physical borders themselves.

Humanity once viewed the stars as symbols of mythology, exploration, and scientific curiosity. Predictably, we eventually converted them into arenas of strategic rivalry, surveillance, and geopolitical competition. Civilizations remain astonishingly consistent in their ability to militarize every frontier they reach. Yet within that reality lies an equally important truth: the nations that understand and adapt to this transformation will shape the future balance of power in the decades ahead.



Lt Gen PJS Pannu
Senior Advisor, SIA-India

Preface

Conferences are often remembered for individual speeches, notable announcements, or moments of debate. Their lasting significance, however, frequently lies elsewhere—in the patterns that emerge when diverse perspectives begin converging around a common set of strategic concerns.
DEFSAT 2026 was one such occasion.

Bringing together military practitioners, policymakers, scientists, industry leaders, technologists, and researchers, the conference examined a broad spectrum of issues spanning defence, technology, resilience, and space. Yet despite the diversity of topics and viewpoints, a striking degree of convergence emerged. Participants frequently approached similar challenges from different institutional perspectives, employed different vocabularies, and proposed different solutions, but many ultimately arrived at remarkably similar concerns regarding preparedness, adaptability, technological sovereignty, and long-term competitiveness.

This book has not been conceived as a conventional set of conference proceedings. The chapters that follow do not reproduce individual presentations, panel discussions, or speaker interventions. Instead, they represent an effort to synthesise the recurring themes, strategic concerns, and emerging ideas that surfaced across multiple sessions and stakeholder groups. In doing so, the volume seeks to move beyond the chronology of the event and focus on the larger questions that repeatedly shaped the conversation.

Many of the issues discussed at DEFSAT proved inherently interdisciplinary. Questions relating to military preparedness frequently intersected with industrial policy. Discussions on cyber security extended into critical infrastructure protection and resilience planning. Debates surrounding artificial intelligence inevitably touched upon decision-making, data governance, and operational effectiveness. Similarly, conversations on space rarely remained confined to satellites or launch systems; they expanded into questions of economics, regulation, diplomacy, national security, and strategic autonomy.

Perhaps more significantly, the discussions revealed the extent to which space can no longer be examined as a standalone sector. Whether the subject was homeland security, military operations, communications, geospatial intelligence, cyber resilience, industrial development, or international cooperation, space increasingly appeared as an enabling layer connecting multiple dimensions of national capability.

Viewed collectively, the deliberations at DEFSAT 2026 repeatedly returned to three fundamental questions. How can nations secure critical infrastructure and maintain resilience in an increasingly contested environment? How will emerging technologies—from artificial intelligence and geospatial intelligence to autonomous systems and advanced communications—reshape military effectiveness and strategic decision-making? And how can states build the industrial, technological, and partnership ecosystems necessary to translate capability into enduring strategic advantage?

While contributors approached these questions from different perspectives, they collectively recognised that the answers will not emerge from any single institution, technology, or policy intervention. The challenges ahead are systemic in nature and will require equally integrated responses.

This volume therefore adopts a thematic rather than chronological structure. Each chapter explores a distinct dimension of the contemporary defence-space landscape while contributing to a broader narrative about the evolving relationship between technology, security, industry, and statecraft. The result is not intended to be a summary of DEFSAT 2026. It is intended to be an intellectual extension of it.

If the conference served as a forum for discussion, debate, and exchange, this book seeks to continue that conversation beyond the confines of the event itself. Its value will ultimately be measured not by the conclusions it presents, but by the insights it generates and the discussions it inspires.The conversations that began at DEFSAT 2026 are far from over. In many respects, they are only beginning.



EXECUTIVE NARRATIVE

PART 1 Emerging Strategic Realities

The world is entering a period of strategic transition that is reshaping the foundations of national power. The assumptions that governed the post-Cold War era are increasingly being challenged by intensifying geopolitical competition, technological disruption, contested supply chains, cyber vulnerabilities, climate-induced instability, and the emergence of new domains of strategic significance. As nations navigate this increasingly complex environment, influence is becoming less dependent on traditional measures of power alone and more contingent upon technological leadership, resilience of critical infrastructure, control of data, industrial capacity, and the ability to operate effectively across interconnected domains.

For much of the twentieth century, space was viewed primarily as a frontier for exploration, scientific discovery, and national prestige. During the Cold War, it evolved into an arena of strategic competition. In the decades that followed, satellite systems became indispensable enablers of communications, navigation, broadcasting, weather forecasting, and military operations. Today, however, space occupies a fundamentally different position. It has become an essential layer of national infrastructure underpinning modern economies, security architectures, governance systems, and digital societies. The infrastructure that enables contemporary life depends upon capabilities operating beyond the atmosphere.

This growing dependence has created a new strategic reality. Nations are no longer simply investing in space capabilities; they are becoming reliant upon them. Consequently, the central challenge is no longer access alone, but resilience. How can critical services be protected against cyber intrusions, electronic interference, spectrum competition, supply-chain disruptions, and increasingly sophisticated threats targeting space systems? How can continuity of operations be ensured when the infrastructure upon which societies depend becomes contested or disrupted?

Beyond this growing dependence, several structural shifts are redefining the contemporary defence-space landscape. Traditional architectures built around a limited number of highly capable assets are increasingly giving way to proliferated constellations designed to ensure resilience through distribution, redundancy, and persistence. Military effectiveness is becoming progressively dependent upon information architectures rather than individual platforms, with strategic advantage increasingly derived from the ability to integrate communications, intelligence, surveillance, navigation, and decision-support systems into coherent operational networks.

At the same time, commercial space enterprises are evolving from suppliers of technology to strategic actors in their own right. Commercial communications networks, Earth observation capabilities, analytics platforms, launch providers, and data services are becoming integral components of national security ecosystems, blurring long-standing distinctions between public and private capability.

A parallel transition is occurring within space architectures themselves. The focus is gradually shifting from discrete missions towards enduring infrastructure. Orbital servicing, logistics, mobility, replenishment, and sustainment capabilities are emerging as critical enablers of long-term operational effectiveness and strategic resilience. Simultaneously, the growing congestion and contestation of the orbital environment are elevating the importance of Space Domain Awareness, making the ability to monitor, characterise, and respond to activities in space an increasingly important determinant of both security and stability.

> *“Space occupies a fundamentally different position. It has become an essential layer of national infrastructure underpinning modern economies, security architectures, governance systems, and digital societies”*

EXECUTIVE NARRATIVE

Over the years, DEFSAT has evolved from a conference focused primarily on defence-space awareness into a strategic platform where military leaders, policymakers, industry executives, scientists, technologists, and strategic thinkers collectively examine the future of security in the space age. The conversations have moved beyond individual technologies to address broader questions of resilience, military preparedness, industrial capacity, technological sovereignty, international cooperation, and national competitiveness.

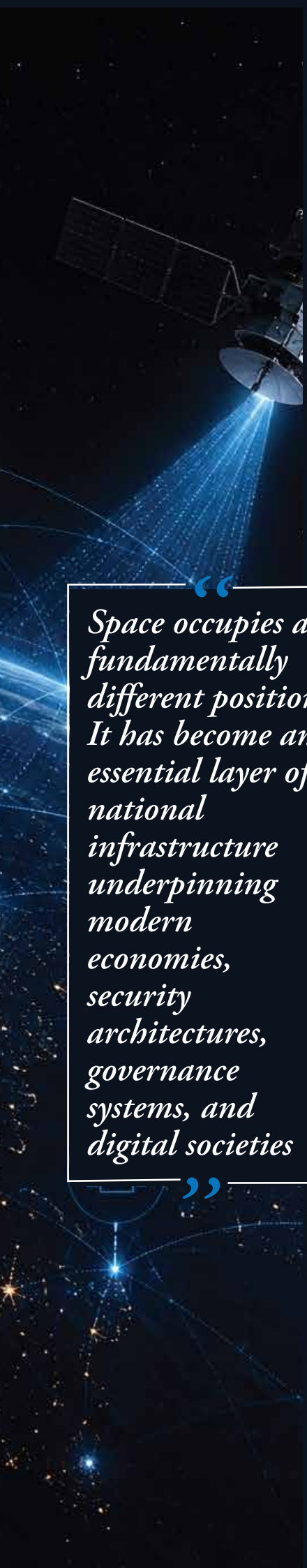
The deliberations at DEFSAT 2026 revealed a remarkable degree of convergence across diverse discussions on cyber security, military space operations, international cooperation, industrial ecosystems, persistent surveillance, homeland security, artificial intelligence, and geospatial intelligence. While participants approached these subjects from different institutional and professional perspectives, they repeatedly returned to a common conclusion: the future strategic environment will be shaped not merely by the possession of space capabilities, but by the ability to integrate those capabilities into broader systems of governance, industry, defence, innovation, and national development.

This volume was conceived to capture those insights. It is not intended to serve as a record of conference proceedings or a compilation of individual viewpoints. Rather, it seeks to distil the strategic conclusions emerging from DEFSAT 2026 and place them within the broader context of a rapidly evolving international environment.

This volume was conceived to capture those insights. It is not intended to serve as a record of conference proceedings or a compilation of individual viewpoints. Rather, it seeks to distil the strategic conclusions emerging from DEFSAT 2026 and place them within the broader context of a rapidly evolving international environment.

The seven conclusions that follow represent an attempt to synthesise the recurring themes, strategic concerns, and emerging realities that surfaced throughout the conference. Collectively, they provide a framework for understanding how space, technology, industry, and security are being reconfigured in the twenty-first century—and what these changes may mean for nations seeking to remain secure, resilient, and competitive in the decades ahead.





PART 2 The Seven Strategic Conclusions Emerging from DEFSAT 2026

1. Space Is Emerging as Critical National Infrastructure

> *"Space occupies a fundamentally different position. It has become an essential layer of national infrastructure underpinning modern economies, security architectures, governance systems, and digital societies"*

Perhaps the most consequential conclusion emerging from DEFSAT 2026 is that space can no longer be understood as a specialised technological domain operating at the periphery of national policy. It has become deeply embedded within the infrastructure that enables contemporary states to function, compete, and govern.

Traditional conceptions of infrastructure were largely confined to tangible assets including, transportation networks, energy systems, telecommunications, ports, and industrial facilities. While these foundations remain essential, the functioning of modern societies increasingly depends upon a parallel layer of infrastructure operating beyond the atmosphere. Space-based systems now underpin communications, navigation, timing services, financial transactions, logistics networks, intelligence architectures, weather forecasting, disaster response mechanisms, environmental monitoring, and military operations.

The significance of this transformation extends beyond the growing utility of space-enabled services. It reflects a deeper structural shift in the organisation of modern economies and security architectures. As societies become more digitised, interconnected, and data-driven, dependence upon space-derived capabilities continues to expand. Critical sectors increasingly rely upon precise positioning, uninterrupted connectivity, real-time situational awareness, and the seamless flow of information across geographically dispersed networks. In many respects, space has become the invisible infrastructure upon which visible infrastructure depends.

This evolution carries profound strategic implications. The disruption of space-enabled services can no longer be viewed solely as a technical or operational concern. It has the potential to affect economic activity, public services, military effectiveness, critical infrastructure, and national resilience simultaneously. As a result, the security of space systems is becoming inseparable from the security of the broader systems they support.

The challenge confronting nations is therefore not simply one of expanding access to space, but of ensuring the resilience, security, and sustainability of the infrastructure that space increasingly provides. Protecting these capabilities is no longer a matter of technological policy alone; it has become a fundamental requirement of national security, economic continuity, and strategic stability.
Recognising this transition is the first step towards understanding the broader changes reshaping the contemporary security environment. Nations that continue to treat space as a niche sector risk underestimating its growing role in determining resilience, competitiveness, and strategic influence in the twenty-first century.

PART 2

The Seven Strategic Conclusions Emerging from DEFSAT 2026

2. Resilience Is Becoming the Primary Measure of Strategic Strength

For decades, strategic planning focused primarily on capability creation. Nations sought to build larger military forces, more advanced technologies, and increasingly sophisticated platforms. While these objectives remain important, the emerging security environment is forcing a broader reassessment of priorities.

The challenge is no longer simply whether capabilities exist. The more important question is whether they can survive disruption. Modern societies depend upon interconnected systems that are increasingly exposed to cyber attacks, spectrum interference, electronic warfare, supply-chain vulnerabilities, infrastructure failures, and information operations. Adversaries are often seeking not physical destruction but operational paralysis. The objective is to disrupt services, degrade confidence, delay decision-making, and exploit dependencies.

In such an environment, resilience becomes a strategic capability in its own right. The ability to absorb shocks, maintain continuity, rapidly recover, and sustain operations under contested conditions may prove as important as the ability to project power. This applies equally to military systems, industrial ecosystems, communications networks, and critical infrastructure.

One of the strongest messages emerging from DEFSAT 2026 was that resilience must be built into systems from the outset rather than added later. Whether through cyber-secure architectures, redundant constellations, responsive launch capabilities, diversified supply chains, or trusted partnerships, future advantage will increasingly belong to nations capable of sustaining capability rather than merely deploying it.





PART 2 **The Seven Strategic Conclusions Emerging from DEFSAT 2026**

3. Military Power Is Becoming Network-Centric and Decision-Driven

The nature of military power is undergoing a fundamental transformation. For much of modern history, military effectiveness was measured through platforms—ships, aircraft, tanks, missiles, and formations. While platforms remain important, their effectiveness increasingly depends upon the networks that connect them.

Satellites, drones, sensors, communications systems, cyber capabilities, and intelligence architectures are generating unprecedented volumes of information. The challenge facing modern militaries is no longer collection. It is integration.

Future conflicts are likely to be characterised by persistent surveillance, distributed operations, multi-domain coordination, and compressed decision cycles. Success will depend on the ability to connect sensors to shooters, fuse intelligence from multiple sources, maintain resilient communications, and generate situational awareness across vast operational environments.

Artificial intelligence, geospatial intelligence, and advanced analytics are accelerating this transformation. The future military advantage will increasingly belong to organisations capable of converting information into understanding and understanding into action faster than their adversaries. Decision superiority is emerging as the new high ground of warfare.

The strategic centre of gravity is therefore shifting from individual platforms to the systems and architectures that connect them.



PART 2 The Seven Strategic Conclusions Emerging from DEFSAT 2026

4. Industrial Capacity Has Re-Emerged as a Strategic Variablen

One of the most consequential lessons emerging from contemporary geopolitical developments is the renewed importance of industrial capacity. For much of the post-Cold War period, strategic discussions were dominated by technological superiority, precision capabilities, and network-centric warfare. Industrial production, manufacturing depth, and supply-chain resilience often received less attention than innovation and operational concepts. Recent conflicts, however, have demonstrated that military effectiveness cannot be sustained without a robust industrial foundation.

This reality is particularly relevant to the space sector. Satellites, launch vehicles, propulsion systems, sensors, semiconductors, advanced materials, communications infrastructure, software platforms, and ground systems all depend upon complex industrial ecosystems. National capability is therefore not determined solely by technological excellence, but by the ability to manufacture, replenish, scale, and sustain that capability over time.

The growing commercialisation of space further reinforces this trend. Private launch providers, satellite manufacturers, geospatial analytics firms, communications operators, software developers, and emerging technology companies are increasingly becoming integral contributors to national capability. The distinction between economic competitiveness and strategic preparedness is narrowing. Industrial ecosystems are no longer merely economic assets; they are becoming instruments of national power.

For countries seeking strategic autonomy, industrial depth is increasingly as important as technological sophistication. Nations capable of designing, producing, and sustaining critical technologies domestically enjoy greater freedom of action during crises, reduced exposure to external disruptions, and enhanced long-term resilience. The future contest for influence will therefore depend not only on innovation, but also on the industrial capacity required to convert innovation into enduring capability.





PART 2 The Seven Strategic Conclusions Emerging from DEFSAT 2026

5. The Boundary Between Civilian and Military Space Is Disappearing

A defining feature of the emerging space era is the growing convergence between civilian and military applications. Historically, security systems and civilian infrastructure often operated in distinct domains. Today, that distinction is becoming increasingly blurred.

Commercial satellite communications support military operations. Navigation systems underpin both civilian transportation and precision-guided munitions. Earth observation data contributes simultaneously to agricultural planning, infrastructure monitoring, disaster management, environmental assessment, and intelligence analysis. The same geospatial platforms that assist governments in responding to floods and wildfires can also support national security planning.

This convergence is transforming how nations think about resilience and preparedness. National security can no longer be viewed solely through a military lens. Critical infrastructure, digital networks, transportation systems, energy grids, financial architectures, and public safety mechanisms are increasingly interconnected with space-enabled services. Vulnerabilities affecting one domain can rapidly generate consequences across multiple sectors.

At the same time, this convergence creates significant opportunities. Investments in space-based infrastructure generate benefits across defence, governance, economic development, environmental management, and public welfare. The expanding role of geospatial intelligence, satellite communications, and Earth observation in homeland security and disaster resilience demonstrates how space is becoming embedded within broader national systems rather than remaining confined to specialised users.

The future security environment will therefore require integrated approaches that recognise the increasingly inseparable nature of economic resilience, societal resilience, and national security.



PART 2 The Seven Strategic Conclusions Emerging from DEFSAT 2026

6.Strategic Partnerships Are BeingReconfigured

The geopolitical landscape is undergoing a period of significant realignment. While traditional military alliances remain important, emerging forms of cooperation are increasingly being shaped by technology, infrastructure, supply chains, data ecosystems, and shared strategic interests.

The space sector offers a clear illustration of this trend. Nations are increasingly collaborating on satellite navigation systems, Earth observation programmes, communications architectures, space situational awareness networks, launch infrastructure, and standards for responsible behaviour in orbit. These partnerships extend beyond conventional defence cooperation and increasingly encompass technology development, industrial collaboration, research, and capacity building.

The Indo-Pacific has emerged as a particularly significant arena for these developments. Growing concerns regarding supply-chain security, critical infrastructure resilience, maritime domain awareness, and technological sovereignty are encouraging greater cooperation among like-minded partners. Similar trends are visible in Europe, where space is increasingly being integrated into broader security and industrial strategies.

Equally important is the growing role of the Global South. As access to space technologies becomes more affordable and commercially accessible, a larger number of nations are seeking to leverage space capabilities for development, resilience, and security. This is creating new opportunities for collaboration, knowledge sharing, and capacity building.

Future partnerships will increasingly be defined not only by geography or ideology, but by participation in trusted networks of technology, infrastructure, innovation, and interoperability. Space is becoming one of the key enablers of these emerging strategic ecosystems.



PART 2 The Seven Strategic Conclusions Emerging from DEFSAT 2026

7. Space Power Is Emerging as a New Measure of State Power

Taken together, the trends identified throughout DEFSAT 2026 point towards a broader strategic conclusion. Space is no longer simply a domain of activity. It is becoming an ecosystem through which military capability, economic competitiveness, industrial strength, technological innovation, governance effectiveness, and international influence increasingly interact.

Historically, measures of national power focused on territory, population, industrial output, economic size, and military strength. While these indicators remain relevant, the emerging international system is placing growing emphasis on connectivity, resilience, information advantage, technological sovereignty, and access to strategic infrastructure. Space influences each of these dimensions.

The significance of space power does not lie solely in satellites or launch vehicles. Rather, it lies in the ability to integrate space capabilities into wider systems of national power. Nations that successfully combine resilient infrastructure, advanced technologies, industrial ecosystems, trusted partnerships, secure data architectures, and effective governance frameworks will derive advantages extending far beyond the space sector itself.

This distinction is critical. Capability refers to what a nation possesses. Power reflects what a nation can achieve.

The central challenge facing governments over the coming decades will therefore be converting space capability into enduring space power. Those that succeed will help shape the future international order. Those that fail risk becoming dependent on systems designed, operated, or controlled by others.



PART 3 Strategic Implications for India

Few countries are as well positioned as India to benefit from the transformation currently underway in the global space sector. Over the past six decades, India has built one of the world's most respected space programmes, developed indigenous launch capabilities, established a sophisticated satellite ecosystem, and demonstrated the ability to deliver high-impact space applications at scale. More recently, reforms opening the sector to private participation, the establishment of IN-SPACe, growing international partnerships, and the emergence of a vibrant start-up ecosystem have fundamentally altered the trajectory of India's space ambitions.

Yet the significance of these developments extends beyond the space sector itself.

The world is entering an era in which space capability is becoming increasingly intertwined with national competitiveness, economic resilience, technological leadership, military preparedness, and geopolitical influence. For India, the question is no longer whether space will be important. The question is whether the country can successfully leverage its existing strengths to emerge as one of the defining space powers of the twenty-first century.

India enters this period with several advantages. It possesses an established institutional foundation, a globally respected scientific and engineering workforce, proven launch capabilities, a rapidly expanding digital economy, and a strategic geography that places it at the centre of the Indo-Pacific. The country also enjoys growing credibility across the Global South and increasingly strong relationships with major space-faring nations. These assets provide a strong platform from which to shape the future rather than simply adapt to it.

At the same time, important challenges remain. The strategic environment is becoming more competitive. The pace of technological change is accelerating. Military space capabilities are expanding globally. Commercial constellations are reshaping access to information and communications. Artificial intelligence is transforming intelligence analysis and decision-making. Supply chains are becoming strategic battlegrounds. The challenge for India is not merely to participate in these developments but to lead in selected areas while ensuring long-term strategic autonomy.

One of the most significant opportunities lies in India's ability to integrate space into broader national objectives. Unlike many countries that developed space programmes primarily for strategic competition, India's space journey has long been linked to developmental outcomes. Satellite communications, remote sensing, disaster management, telemedicine, digital inclusion, weather forecasting, and agricultural applications have demonstrated how space can directly contribute to national development. As the distinction between economic resilience and national security continues to narrow, this integrated approach may become one of India's greatest strategic advantages.

The military dimension is equally important. Future conflicts are increasingly likely to depend on space-enabled communications, navigation, intelligence, surveillance, targeting, and decision support. The growing importance of multi-domain operations, network-centric warfare, autonomous systems, and persistent intelligence architectures means that military effectiveness will increasingly depend on resilient space capabilities. India's future deterrence posture, operational effectiveness, and strategic autonomy will therefore be influenced by its ability to secure and sustain these capabilities under contested conditions.



PART 3 Strategic Implications for India

Industrial capacity represents another critical opportunity. The emergence of India's private space sector has created the foundations for a broader defence-space industrial ecosystem capable of supporting innovation, manufacturing, analytics, launch services, and dual-use technologies. Over time, this ecosystem can contribute not only to economic growth but also to national resilience, strategic preparedness, and export competitiveness. The countries that dominate the future space economy are unlikely to be those with the largest government programmes alone. They will be those capable of combining public investment, private innovation, industrial depth, and international partnerships into a coherent ecosystem.

India's geopolitical position further enhances its potential role. The Indo-Pacific is rapidly becoming one of the most strategically significant regions in the world, with increasing emphasis on maritime domain awareness, secure communications, resilient infrastructure, supply-chain security, and trusted technology partnerships. Simultaneously, many countries across the Global South are seeking affordable and reliable access to space-enabled services for development, climate resilience, connectivity, and security. India occupies a unique position at the intersection of these two trends.

This creates an opportunity to shape future norms, build trusted partnerships, support capacity-building initiatives, and contribute to a more inclusive and resilient global space ecosystem. The country's growing role in international forums, collaborative missions, and technology partnerships suggests that India is increasingly viewed not merely as a participant in the global space economy but as a potential architect of its future evolution.

Ultimately, the challenge facing India is not one of capability creation alone. It is one of strategic integration. The country possesses many of the ingredients required for long-term success. The task ahead is to connect these elements into a coherent national framework that aligns technological innovation, industrial growth, military preparedness, economic development, and international engagement.

The future space race will not be won solely through technological achievement. It will be won by nations capable of translating capability into influence, innovation into resilience, and ambition into enduring strategic advantage. India has the opportunity to be one of those nations.

The decisions taken during the coming decade will determine whether it does.



PART 4 Strategic Priorities for the Next Decade

The strategic shifts identified throughout DEFSAT 2026 point towards a clear conclusion: the coming decade will be decisive in determining which nations emerge as leaders in the space age and which become dependent upon capabilities developed elsewhere. For India, the challenge is not simply expanding its presence in space. It is building a resilient, secure, and globally competitive space ecosystem capable of supporting national security, economic growth, technological leadership, and strategic influence simultaneously.

The path forward requires a transition from isolated initiatives to a nationally integrated approach. Space can no longer be viewed solely through the lens of science, commerce, or defence. It has become a strategic domain that intersects with nearly every dimension of national power. The following priorities emerge as critical for the decade ahead.

Protecting Space as Critical National Infrastructure

India must increasingly treat space infrastructure as part of its broader critical national infrastructure architecture. Satellites, ground stations, communication networks, navigation services, and data systems now support functions extending far beyond the space sector itself. Future security frameworks must therefore integrate cyber resilience, space situational awareness, spectrum security, supply-chain protection, and operational continuity into a unified national approach. The objective should be to ensure that space-enabled services remain available even under conditions of disruption, crisis, or conflict.

Building Resilient and Distributed Space Architectures

The era of dependence on a limited number of strategic assets is gradually giving way to distributed and resilient architectures. Future capability will increasingly depend upon proliferated constellations, multi-orbit systems, redundancy, responsive launch mechanisms, and rapid reconstitution capabilities. The focus must shift from asset ownership to mission assurance. India's long-term space strategy should therefore prioritise resilience by design, ensuring continuity of services under both routine and contested conditions.

Accelerating Military-Space Integration

Space has become an operational domain that directly influences military effectiveness. Communications, navigation, intelligence, targeting, and decision support are increasingly dependent upon space-enabled systems. Future military preparedness will therefore require closer integration between space capabilities and operational planning across all services. The objective should be to develop a coherent framework that supports multi-domain operations, persistent situational awareness, and decision superiority while ensuring resilience against emerging threats.



Building a Sovereign GEOINT and AI Ecosystem

The future battlespace will be defined not by information scarcity but by information abundance. Satellites, drones, sensors, cyber systems, and digital platforms are generating unprecedented volumes of data. The strategic advantage will belong to those capable of transforming this data into timely, trusted, and actionable insights. India must therefore prioritise the development of indigenous geospatial intelligence platforms, defence AI architectures, trusted data ecosystems, and decision-support systems that reduce external dependencies while enhancing operational effectiveness.

Strengthening the Defence-Space Industrial Ecosystem

Industrial capacity will increasingly determine strategic autonomy. India has made significant progress in opening the space sector to private participation, but the next phase requires deeper integration between government institutions, industry, start-ups, academia, and investors. The goal should be to create an ecosystem capable of supporting advanced manufacturing, launch services, satellite production, software development, analytics, propulsion technologies, and emerging space applications. Industrial depth must become a strategic objective rather than a by-product of growth.

Expanding International Partnerships

No nation can address the challenges of the emerging space environment alone. Issues such as orbital congestion, space situational awareness, spectrum management, cyber security, disaster resilience, and responsible behaviour require cooperation across borders. India should continue strengthening partnerships with established space powers while simultaneously expanding engagement with the Indo-Pacific, Europe, Africa, Southeast Asia, and the broader Global South. The objective should be to position India as both a trusted partner and a leading contributor to the development of a stable and inclusive space order.

Integrating Space into National Resilience Planning

Space-enabled capabilities should become an integral component of broader national resilience frameworks. Disaster management, critical infrastructure protection, climate adaptation, border management, emergency communications, maritime awareness, and homeland security increasingly depend upon geospatial intelligence and satellite-based services. Integrating these capabilities into national planning will improve preparedness, reduce vulnerabilities, and strengthen societal resilience.

Investing in Human Capital and Future Technologies

Technological leadership ultimately depends upon people. Sustained investment in education, research, innovation, and workforce development will be essential if India is to maintain competitiveness in an increasingly knowledge-driven space economy. Particular emphasis should be placed on emerging fields such as artificial intelligence, quantum technologies, advanced materials, autonomous systems, cybersecurity, in-space manufacturing, and next-generation communications. The objective is not only to adopt future technologies but to contribute to their development.



Creating a National Space Power Strategy

Perhaps the most important priority is the development of an integrated national vision that connects the various elements of India's space ecosystem. Historically, space policy has often been viewed through sector-specific lenses. The future requires a broader perspective that aligns security objectives, industrial development, economic growth, technological innovation, diplomatic engagement, and societal resilience. Such a framework would provide coherence across institutions while ensuring that investments in space contribute directly to long-term national objectives.

The coming decade will be defined by the choices nations make regarding technology, infrastructure, resilience, and strategic preparedness. For India, the opportunity is not merely to participate in the global space economy or expand existing capabilities. It is to shape the architecture of a future in which space increasingly influences every dimension of national power. Achieving that objective will require sustained commitment, coordinated action, and a clear understanding that the strategic value of space extends far beyond the domain itself.



SECURING SPACE AS NATIONAL CRITICAL INFRASTRUCTURE: CYBER, SPECTRUM, AND ELECTRONIC FULL

Introduction: The Strategic Dependence on Space Infrastructure

"Space occupies a fundamentally different position. It has become an essential layer of national infrastructure underpinning modern economies, security architectures, governance systems, and digital societies"

The character of national security is being reshaped by an infrastructure revolution that is largely invisible to the public eye. For much of modern history, military power was measured through visible assets: armies, aircraft, warships, industrial capacity, and territorial control. Strategic advantage was derived from the ability to project force across land, sea, and air domains. While these traditional instruments of power remain essential, they are increasingly dependent upon a less visible layer of infrastructure operating hundreds and sometimes thousands of kilometres above the Earth.

Space has evolved from a domain of scientific achievement and national prestige into an indispensable component of modern security architecture. Satellites today support virtually every aspect of military planning, operational execution, and strategic decision-making. They provide communications across vast distances, enable precision navigation and timing, generate intelligence through Earth observation systems, support missile warning capabilities, facilitate maritime domain awareness, and connect military formations operating across multiple theatres. In many respects, space has become the connective tissue that binds together modern defence ecosystems.

This transformation has occurred gradually over several decades. Early military space systems were primarily designed to provide strategic communications and reconnaissance capabilities for major powers. Today, however, space-enabled services are deeply integrated into routine military operations. Modern armed forces depend upon continuous access to positioning, navigation, and timing signals; satellite communications; geospatial intelligence; weather forecasting; and persistent surveillance. These capabilities are no longer supplementary enablers. They have become foundational elements of military effectiveness.

The implications of this dependence are particularly evident in the evolution of precision warfare. Contemporary military operations increasingly rely on accurate navigation, real-time situational awareness, and networked command structures. Precision-guided munitions, unmanned systems, long-range strike capabilities, and integrated air and missile defence networks all depend, directly or

The character of national security is being reshaped by an infrastructure revolution that is largely invisible to the public eye. For much of modern history, military power was measured through visible assets: armies, aircraft, warships, industrial capacity, and territorial control. Strategic advantage was derived from the ability to project force across land, sea, and air domains. While these traditional instruments of power remain essential, they are increasingly dependent upon a less visible layer of infrastructure operating hundreds and sometimes thousands of kilometres above the Earth.

Space has evolved from a domain of scientific achievement and national prestige into an indispensable component of modern security architecture. Satellites today support virtually every aspect of military planning, operational execution, and strategic decision-making. They provide communications across vast distances, enable precision navigation and timing, generate intelligence through Earth observation systems, support missile warning capabilities, facilitate maritime domain awareness, and connect military formations operating across multiple theatres. In many respects, space has become the connective tissue that binds together modern defence ecosystems.

This transformation has occurred gradually over several decades. Early military space systems were primarily designed to provide strategic communications and reconnaissance capabilities for major powers. Today, however, space-enabled services are deeply integrated into routine military operations. Modern armed forces depend upon continuous access to positioning, navigation, and timing signals; satellite communications; geospatial intelligence; weather forecasting; and persistent surveillance. These capabilities are no longer supplementary enablers. They have become foundational elements of military effectiveness.

The implications of this dependence are particularly evident in the evolution of precision warfare. Contemporary military operations increasingly rely on accurate navigation, real-time situational awareness, and networked command structures. Precision-guided munitions, unmanned systems, long-range strike capabilities, and integrated air and missile defence networks all depend, directly or indirectly, upon space-enabled infrastructure. The ability to detect, identify, track, communicate, and engage targets with speed and accuracy is increasingly linked to the availability of resilient orbital systems.

Beyond the battlefield, space infrastructure plays a critical role in supporting broader national security objectives. Border surveillance, maritime domain awareness, disaster response, strategic communications, and critical infrastructure monitoring increasingly rely upon satellite-derived information. Governments use Earth observation systems to monitor activities across vast and often inaccessible regions, while communications satellites provide connectivity in remote and contested environments where terrestrial networks may be unavailable or vulnerable

The strategic significance of space is further amplified by the growing integration of civilian, commercial, and military capabilities. The distinction between defence infrastructure and commercial infrastructure is becoming progressively blurred. Commercial Earth observation companies now provide imagery and analytics with direct relevance to national security. Commercial communications networks increasingly support military operations. Private launch providers, satellite operators, cloud service companies, and geospatial analytics firms are becoming integral components of national resilience and operational capability.

Recent geopolitical developments have accelerated this trend. Conflicts around the world

Understanding this growing dependence on space infrastructure is essential because it provides the context for the challenges explored throughout this chapter. As space becomes increasingly embedded within military operations and national security architectures, it is also becoming a focal point for new forms of competition and conflict. The rise of cyber threats, electronic warfare, spectrum contestation, and attacks on critical command networks reflects a broader transformation in the nature of strategic competition. Protecting these systems, ensuring their resilience, and leveraging them effectively for operational advantage will be among the defining security challenges of the coming decades.













The Rise of the Non-Kinetic Battlespace

The growing dependence on space-enabled infrastructure has fundamentally altered the nature of strategic competition. As satellites, communications networks, intelligence architectures, and command systems become increasingly integral to military effectiveness, they also become increasingly attractive targets. Yet unlike previous eras of conflict, the most effective method of neutralising these capabilities may not involve physically destroying them. Instead, adversaries are increasingly seeking to disrupt, degrade, manipulate, or deny access to critical systems through non-kinetic means. This shift represents one of the most significant transformations in modern warfare. For much of the twentieth century, military operations focused on the destruction of physical assets. Aircraft targeted airfields, missiles struck command centres, and naval forces sought to deny access to critical maritime routes. Strategic advantage was often achieved by destroying an adversary's capability to fight.

Today, however, the operational effectiveness of military forces depends as much on information flows as it does on physical platforms. Communications networks, navigation systems, ISR architectures, command centres, cloud infrastructure, and data links collectively form the nervous system of modern military operations. Disrupting these systems can often produce effects comparable to, and sometimes greater than, the destruction of traditional military assets.The result is the emergence of a battlespace in which information, software, networks, and the electromagnetic spectrum have become contested operational environments in their own right.

Cyber Warfare and the Space Ecosystem

Cyber warfare represents one of the most prominent dimensions of this evolving battlespace. Modern satellites are not isolated assets operating independently in orbit. They are connected to mission control centres, software systems, user terminals, cloud infrastructure, and communications networks that collectively support mission operations. Every interface creates a potential point of vulnerability. Adversaries seeking to disrupt space-enabled services may find it considerably easier to target terrestrial infrastructure than the satellites themselves.

The cyberattack on the Viasat communications network in February 2022 demonstrated this reality with remarkable clarity. Rather than attacking orbital assets directly, the operation targeted ground-based infrastructure supporting satellite communications services. Thousands of user terminals were rendered inoperable, disrupting communications across multiple countries and highlighting the vulnerability of the broader ecosystem upon which space-enabled services depend. The incident underscored a critical lesson: the weak-

est point in a space architecture may not be in orbit, but somewhere within the digital infrastructure that supports it.

As military and civilian space systems become increasingly interconnected, cybersecurity can no longer be viewed as a technical function. It has become a strategic requirement for maintaining operational continuity and national resilience.

Situational awareness can no longer be limited to physical domains; it must increasingly encompass spectrum awareness as a core element of operational planning.

Future resilience will depend heavily upon frequency agility—the ability of systems to rapidly shift communication frequencies in response to interference, jamming, or hostile activity. Artificial intelligence-enabled interference detection systems can help distinguish between natural environmental disturbances and deliberate adversarial actions. Cognitive radio architectures capable of autonomous frequency hopping will become essential for maintaining communications superiority in contested environments. The side capable of adapting most effectively within the electromagnetic environment will enjoy a significant operational advantage.

For India, spectrum resilience is not merely a technical requirement; it is a national security imperative. As both a rapidly digitising economy and a major military power, India cannot afford to lose access to critical electromagnetic resources during periods of crisis. The protection of spectrum must therefore be treated with the same strategic seriousness traditionally associated with the defence of territorial borders.

Supply Chain Vulnerabilities and Systemic Risk

A further dimension of the non-kinetic battlespace is the growing vulnerability of supply chains and software ecosystems. Modern space systems are supported by complex global networks of manufacturers, software providers, cloud operators, communications companies, and specialist technology suppliers. While these interconnected ecosystems enable innovation and efficiency, they also create new opportunities for exploitation.

Malicious code inserted into software updates, compromised hardware components, vulnerable third-party applications, or insider threats can provide adversaries with access to systems long before a crisis emerges. Such vulnerabilities are particularly concerning because they often remain undetected until activated. Unlike traditional attacks that produce immediate and visible effects, supply-chain compromises can remain dormant for extended periods, creating strategic uncertainty and reducing confidence in critical systems.

The increasing integration of commercial technologies into military architectures further amplifies these risks, making supply-chain security an increasingly important component of national resilience.



Artificial Intelligence: Force Multiplier and Threat Vector

Artificial intelligence is adding another layer of complexity to this evolving environment. AI is rapidly becoming an indispensable tool for both defence and offence. On the defensive side, AI enables anomaly detection, threat identification, behavioural analytics, predictive maintenance, and real-time network monitoring. On the offensive side, it can automate cyber reconnaissance, identify vulnerabilities, generate sophisticated deception campaigns, and accelerate the speed of attack.

As military and civilian systems become more dependent on AI-enabled processes, ensuring the integrity of data, algorithms, and decision-support systems will become an increasingly important security challenge. The same technologies that strengthen resilience can also be exploited to undermine it.

From Protection to Survivability

The strategic significance of these developments extends beyond individual technologies. Collectively, they reflect a broader transformation in the nature of power and conflict. Modern military advantage is no longer determined solely by the ability to deploy platforms or project force. It increasingly depends on the ability to preserve access to information, maintain connectivity, protect communications, and sustain command architectures under contested conditions.

For space-enabled systems, this reality has profound implications. Satellites are no longer isolated strategic assets operating at a distance from conflict. They are integral components of a larger ecosystem that includes cyber networks, spectrum infrastructure, command systems, data centres, and communications architectures. Consequently, protecting space capability requires protecting the entire ecosystem that supports it.

The challenge for governments, defence organisations, and commercial operators is therefore not simply to prevent attacks. It is to build architectures capable of functioning despite attack. Security can no longer be defined by the absence of disruption; it must increasingly be measured by the ability to absorb shocks, maintain essential services, and recover rapidly when challenged.

The rise of the non-kinetic battlespace marks a fundamental shift in strategic thinking. Conflict is becoming increasingly characterised by competition below the threshold of war, persistent attempts to exploit vulnerabilities, and continuous contestation across digital and electromagnetic domains. In such an environment, resilience becomes as important as capability, continuity becomes as important as performance, and survivability becomes a defining measure of strategic strength.

The nations best positioned to succeed in this new environment will not necessarily be those that possess the most advanced systems. They will be those capable of ensuring that their systems remain operational, adaptable, and resilient when subjected to sustained pressure. In the emerging space age, the ability to survive disruption may prove just as important as the ability to deter it.



The 3D Security Framework: Building a Multi-Dimensional Shield

The emergence of the non-kinetic battlespace has fundamentally altered how security must be understood and implemented. For much of the modern era, critical infrastructure protection was built around a relatively simple principle: prevent adversaries from gaining access to strategic assets. Security was largely measured through the effectiveness of barriers, whether physical, digital, or organisational. If a system could be protected from intrusion, it was considered secure.The evolving threat environment has rendered this assumption increasingly inadequate.

Modern space-enabled architectures operate through highly interconnected networks linking satellites, terrestrial communications infrastructure, cloud environments, software systems, command centres, user terminals, and commercial service providers. This interconnectedness has created unprecedented operational capability, but it has also expanded the attack surface available to adversaries. Cyber intrusions, electronic warfare, spectrum interference, software vulnerabilities, supply-chain compromises, and insider threats can emerge simultaneously across multiple layers of the ecosystem. In such an environment, absolute protection is no longer a realistic objective. The strategic challenge therefore shifts from prevention to survivability.

Historically, security strategies focused on stopping attacks before they occurred. Success was measured by the ability to deny access, eliminate vulnerabilities, and maintain secure perimeters. While these objectives remain important, they are increasingly insufficient in a world characterised by persistent competition and continuous attempts to exploit digital and electromagnetic vulnerabilities. The more relevant question is no longer whether a system can be attacked. The more relevant question is whether it can continue functioning when attacked.

Survivability places operational continuity at the centre of security planning. It acknowledges that disruptions may occur despite the most sophisticated defensive measures and seeks to ensure that critical functions remain available even when portions of the architecture are degraded or compromised. A resilient system absorbs shocks, adapts to changing conditions, isolates failures, and restores functionality rapidly. In doing so, it reduces the strategic value of attacks and strengthens deterrence by denying adversaries the outcomes they seek.

This philosophy is particularly relevant to the space domain, where the disruption of a single component can generate cascading consequences across multiple sectors. Communications networks, ISR systems, com-

mand architectures, navigation services, and military operations are increasingly interconnected. Protecting them requires a broader and more holistic approach to resilience.

One useful framework for understanding this challenge is the Three-Dimensional Security Framework, which approaches resilience through three complementary dimensions: Defence in Depth, Defence in Breadth, and Defence in Height. Together, these dimensions create a comprehensive model for securing the increasingly complex architectures that underpin modern military and national security capability.

Defence in Depth: Layering Security Across the Architecture

The first dimension of resilience recognises that no single defensive mechanism can provide complete protection. Encryption alone is insufficient. Firewalls alone are insufficient. Intrusion detection systems alone are insufficient. Modern security requires multiple layers of protection operating simultaneously throughout the architecture.

Within the space domain, Defence in Depth involves securing satellites, communications links, mission control systems, software environments, cloud infrastructure, data networks, and user terminals as part of a unified security ecosystem. Modern satellites contain millions of lines of software code and depend upon continuous interaction with terrestrial systems. Every interface represents a potential point of vulnerability.

A vulnerability within a software update mechanism, a compromised user terminal, or an insecure communications gateway can provide access to systems that are otherwise physically secure. Consequently, resilience requires overlapping layers of protection that limit the consequences of any single failure.

Encryption safeguards communications. Authentication mechanisms verify identity and access. Network segmentation restricts lateral movement within systems. Behavioural analytics detect abnormal activity. Intrusion detection systems monitor threats continuously, while redundant communications pathways preserve operational continuity during disruptions. Together, these mechanisms create a layered architecture that increases the complexity, cost, and uncertainty associated with attack.

The objective is not to create impenetrable systems. Rather, it is to ensure that the compromise of one layer does not result in the collapse of the entire architecture.



Defence in Breadth: Securing the Entire Ecosystem

Historically, security planning focused primarily on protecting satellites, launch facilities, and mission control centres. Today, such an approach is insufficient because operational capability depends upon a far broader ecosystem of interconnected stakeholders and technologies.

The contemporary space sector encompasses launch providers, satellite manufacturers, software developers, cloud infrastructure companies, telecommunications operators, analytics providers, component suppliers, and end users across both civilian and military environments. Each contributes to the functioning of the overall architecture, and each represents a potential source of vulnerability.

Recent cyber incidents across multiple industries have demonstrated how supply-chain compromises can provide adversaries with access to highly protected systems. Malicious software updates, compromised hardware components, vulnerable third-party applications, and insider threats have all emerged as significant security concerns. Similar risks exist within the space domain, where operational architectures increasingly rely on commercial technologies and globally distributed supply chains.

The security of a modern military network is therefore influenced not only by the resilience of satellites and command centres, but also by the integrity of software providers, communications networks, cloud platforms, logistics systems, and connected devices. A vulnerability at any point within this ecosystem can affect operational effectiveness.

Defence in Breadth expands the concept of security beyond organisational boundaries. It recognises that resilience must extend across the full ecosystem supporting national capability. Every supplier, service provider, software platform, communications network, and connected endpoint contributes to the overall security posture. In network-centric operations, resilience is determined not solely by the strength of individual components but by the robustness of the relationships between them.



Defence in Height: Securing the Vertical Battlespace

The third dimension addresses a challenge unique to the space domain: modern operations increasingly extend vertically across multiple layers of the atmosphere and beyond.

Future military and civilian architectures will not depend on a single platform or orbital regime. Instead, they will operate through integrated ecosystems comprising terrestrial networks, High Altitude Platform Systems (HAPS), Low Earth Orbit constellations, Medium Earth Orbit systems, Geostationary satellites, and, eventually, cislunar infrastructure.

Each layer contributes distinct capabilities while enhancing overall resilience. Terrestrial networks provide scale and accessibility but remain vulnerable to physical disruption and cyber attack. Low Earth Orbit constellations offer redundancy and low latency. Geostationary satellites provide broad coverage and strategic communications capability. HAPS platforms deliver persistent regional surveillance and communications support while offering operational flexibility unavailable to traditional orbital systems.

The strategic significance of Defence in Height lies in its ability to reduce dependence on any single layer of infrastructure. If one layer is degraded or denied, others can compensate. Communications can be rerouted, surveillance functions redistributed, and operational continuity maintained despite the loss of individual assets.

This layered approach is becoming increasingly important as nations seek to reduce single points of failure and build more resilient architectures. Future military operations are likely to depend not on individual platforms, but on integrated ecosystems capable of adapting dynamically to disruption.

For India, this dimension carries particular relevance. Investments in indigenous HAPS capabilities, distributed satellite constellations, resilient communications architectures, and integrated terrestrial-space networks could significantly enhance border surveillance, maritime domain awareness, disaster response, and military resilience.

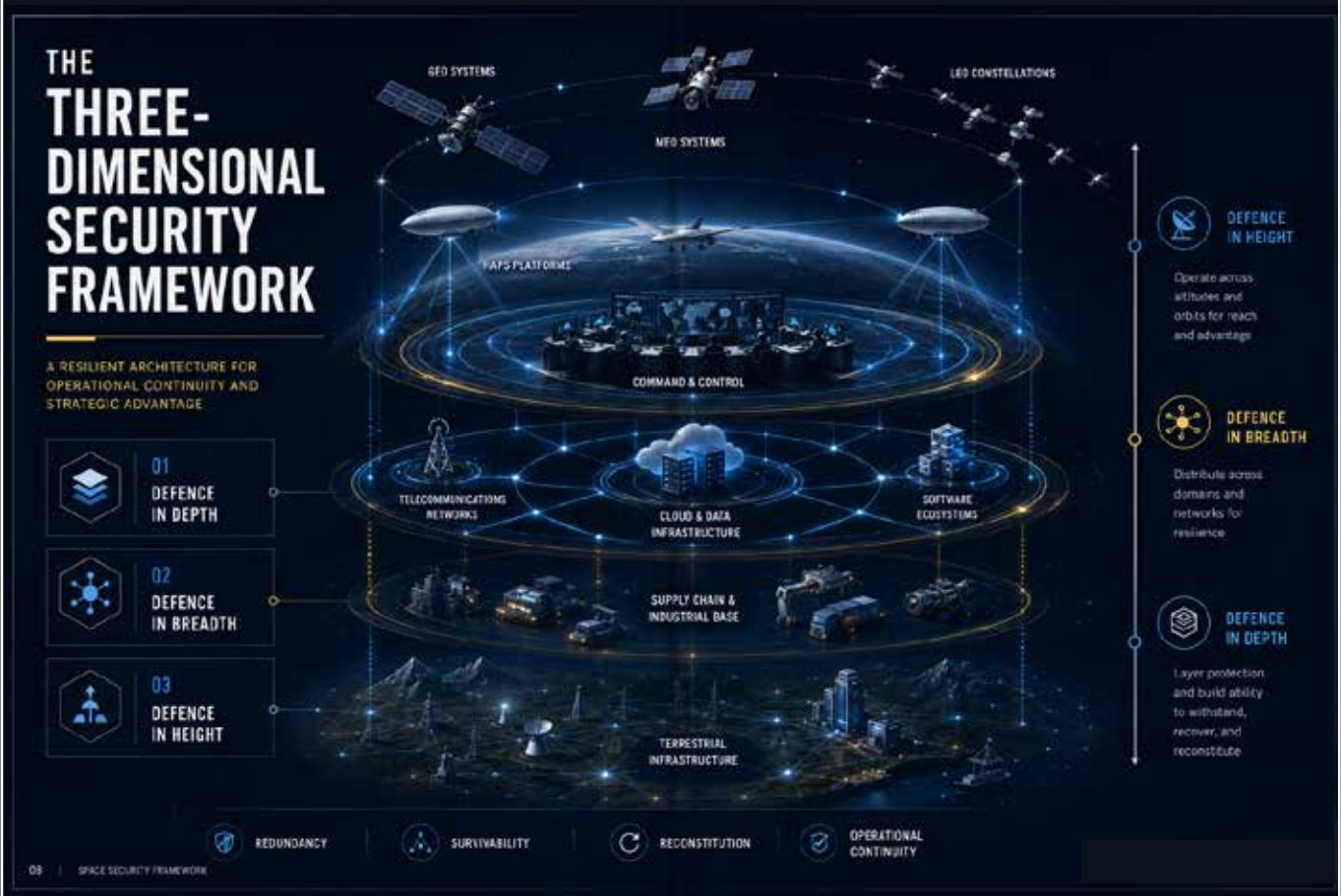
Resilience as a Strategic Capability

Taken together, Defence in Depth, Defence in Breadth, and Defence in Height represent more than a technical security framework. They reflect a broader shift in strategic thinking. The objective of modern security is no longer simply to prevent attacks. It is to ensure that critical capabilities remain available under contested conditions.

This evolution is already influencing the design of future space architectures. Large monolithic satellites are gradually giving way to distributed constellations. Centralised command systems are being complemented by cloud-enabled operations and distributed mission control. Artificial intelligence is being integrated into monitoring and anomaly detection systems. Rapid launch capabilities are creating pathways for reconstitution and recovery following disruption.

Perhaps most importantly, resilience itself is emerging as a form of deterrence. Adversaries are less likely to attack systems that can absorb disruption, recover rapidly, and continue functioning despite pressure. By reducing the effectiveness of hostile actions and increasing the uncertainty associated with attack, resilient architectures diminish the strategic value of aggression.

In an era defined by persistent competition and continuous contestation across cyber, spectrum, and space domains, survivability is becoming as important as capability itself. The nations best positioned to succeed will not necessarily be those with the most sophisticated technologies or the largest constellations. They will be those capable of building systems that endure, adapt, and remain operational when challenged.





Command Networks and the C5ISR Backbone: From Information to Decision Advantage

The ultimate purpose of resilience is not simply survival. While protecting satellites, communications networks, and digital infrastructure is essential, security alone does not generate strategic advantage. Resilience preserves capability; it does not, by itself, create superiority. The true value of modern space-enabled infrastructure lies in its ability to transform information into operational awareness, operational awareness into decisions, and decisions into decisive action.

Throughout history, military effectiveness has depended upon the ability to gather information, understand the operating environment, and coordinate action across dispersed forces. What has changed in the twenty-first century is the speed, scale, and complexity of this process. Modern military operations generate unprecedented volumes of data from satellites, unmanned systems, airborne sensors, maritime platforms, cyber networks, electronic intelligence systems, and open-source information streams. The challenge is no longer the collection of information. The challenge is converting information into actionable insight quickly enough to influence outcomes.

This requirement has elevated the importance of Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance—collectively known as C5ISR. Once viewed primarily as a military support function, C5ISR has become the operational backbone of modern defence architectures.

It provides the mechanisms through which information is collected, transmitted, processed, analysed, and transformed into decisions. In many respects, C5ISR functions as the nervous system of contemporary military operations, connecting sensors, commanders, platforms, and decision-makers within a single operational ecosystem.

The growing importance of C5ISR reflects a broader transformation in the character of warfare. Traditional military operations were often organised around individual platforms. Aircraft operated within air campaigns, naval vessels within maritime operations, and ground forces within land campaigns. Information moved through hierarchical structures, often resulting in delays between observation and action. Modern conflict increasingly demands integration across multiple domains simultaneously. Military forces must coordinate activities across land, sea, air, cyber, and space environments in real time, often while operating under conditions of uncertainty and disruption.

This shift has given rise to network-centric warfare, in which connectivity becomes as important as firepower. In a network-centric environment,

The ultimate purpose of resilience is not simply survival. While protecting satellites, communications networks, and digital infrastructure is essential, security alone does not generate strategic advantage. Resilience preserves capability; it does not, by itself, create superiority. The true value of modern space-enabled infrastructure lies in its ability to transform information into operational awareness, operational awareness into decisions, and decisions into decisive action.

Throughout history, military effectiveness has depended upon the ability to gather information, understand the operating environment, and coordinate action across dispersed forces. What has changed in the twenty-first century is the speed, scale, and complexity of this process. Modern military operations generate unprecedented volumes of data from satellites, unmanned systems, airborne sensors, maritime platforms, cyber networks, electronic intelligence systems, and open-source information streams. The challenge is no longer the collection of information. The challenge is converting information into actionable insight quickly enough to influence outcomes.

This requirement has elevated the
importance of Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance—collectively known as C5ISR. Once viewed primarily as a military support function, C5ISR has become the operational backbone of modern defence architectures.

It provides the mechanisms through which information is collected, transmitted, processed, analysed, and transformed into decisions. In many respects, C5ISR functions as the nervous system of contemporary military operations, connecting sensors, commanders, platforms, and decision-makers within a single operational ecosystem.

The growing importance of C5ISR reflects a broader transformation in the character of warfare. Traditional military operations were often organised around individual platforms. Aircraft operated within air campaigns, naval vessels within maritime operations, and ground forces within land campaigns. Information moved through hierarchical structures, often resulting in delays between observation and action. Modern conflict increasingly demands integration across multiple domains simultaneously. Military forces must coordinate activities across land, sea, air, cyber, and space environments in real time, often while operating under conditions of uncertainty and disruption.

This shift has given rise to network-centric warfare, in which connectivity becomes as important as firepower. In a network-centric environment, every platform contributes to and benefits from a shared information architecture. Satellites provide communications and navigation. UAVs collect intelligence. Ground sensors monitor activity. Cyber networks provide situational awareness. Command centres integrate information from multiple sources and distribute it to operational units. The effectiveness of the force depends not merely on the performance of individual systems but on the quality of the connections between them.

Space infrastructure occupies a central position within this architecture. Satellites provide the communications links that connect dispersed forces across vast geographic areas. They deliver positioning, navigation, and timing services that enable precision operations. Earth observation systems generate intelligence that informs planning and execution. Secure communications satellites ensure that commanders can maintain connectivity under contested conditions. Without resilient space-enabled services, modern military operations would struggle to sustain the levels of coordination and responsiveness required in contemporary conflict.

The strategic importance of these capabilities is increasingly evident across the world's major militaries. Modern operations are becoming progressively data-driven. Intelligence must be collected continuously, analysed rapidly, and distributed efficiently. The speed at which infor-

resilient command architectures capable of functioning under contested conditions. Communications networks must remain operational despite cyber attacks, electronic warfare, and spectrum interference. Data must continue to flow even when portions of the network are disrupted. Command systems must be designed to adapt dynamically to changing circumstances rather than relying upon rigid and centralised structures.

This requirement is driving a broader transformation in military command architectures. Traditional command systems often relied on centralised decision-making and hierarchical information flows. While effective in relatively stable environments, such models can become vulnerable when communications are disrupted or operational tempos increase. Future command networks are increasingly moving toward distributed, resilient, and data-centric architectures capable of operating effectively even when connectivity is degraded.

For India, these developments carry important strategic implications. The country's evolving defence posture, expanding space capabilities, and growing emphasis on joint operations require increasingly sophisticated command and control architectures. As the armed forces continue their transition toward integrated theatre commands and multi-domain operations, the ability to connect sensors, platforms, commanders, and decision-makers through resilient space-enabled networks will become increasingly important.

The future battlespace will not be defined solely by the quality of weapons systems or the size of military formations. It will be shaped by the ability to collect information, maintain connectivity, generate understanding, and make decisions faster than an adversary. Space infrastructure provides the foundation upon which this capability rests. Protecting that infrastructure is essential, but its ultimate value lies in enabling the command networks that transform information into operational advantage.

As military operations become increasingly data-driven and interconnected, command networks and C5ISR architectures will continue to evolve from supporting functions into strategic assets in their own right. In the emerging security environment, the ability to connect, understand, and act may prove just as important as the ability to fight.



Satellite Operation Centres: The Hidden Nerve Centres of Space Power

Much of the public discourse surrounding space security tends to focus on satellites themselves. Discussions often centre on launch vehicles, orbital constellations, anti-satellite weapons, Earth observation systems, or communications networks operating in space. While these capabilities undoubtedly form the visible face of modern space power, they represent only part of the larger operational ecosystem. Behind every satellite constellation, communications architecture, and ISR network lies a less visible but equally critical component: the command infrastructure that manages, controls, and sustains operations in orbit.

At the heart of this infrastructure are Satellite Operation Centres (SOCs). Traditionally, Satellite Operation Centres were viewed primarily as technical facilities responsible for spacecraft monitoring and control. Their core functions included tracking satellite health, monitoring payload performance, executing orbital manoeuvres, managing communications links, and ensuring mission continuity. In many respects, they were regarded as operational back offices—essential to mission success but largely removed from broader strategic considerations.

This perception is rapidly changing. As space systems become increasingly integrated into military operations, national security architectures, and critical communications networks, Satellite Operation Centres are evolving from technical facilities into strategic command nodes. They now occupy a central position within the broader ecosystem connecting satellites, ground infrastructure, communications networks, intelligence systems, and operational decision-makers. Their role is no longer limited to managing spacecraft; they increasingly facilitate the flow of information that underpins military effectiveness, situational awareness, and national resilience.

In a contemporary operational environment, satellites rarely function as isolated platforms. Communications satellites support military networks spanning vast geographic areas. Earth observation systems generate intelligence used by defence planners, border management agencies, and maritime security organisations. Navigation satellites provide positioning and timing services essential to military operations. These capabilities derive their operational value not merely from their presence in orbit, but from their ability to deliver information reliably to users on the ground. Satellite Operation Centres provide the bridge between orbital assets and terrestrial decision-making systems.

Consequently, the resilience of an SOC can be as important as the resilience of the satellites it controls. An advanced satellite constellation offers limited strategic value if its command infrastruc-

ture is vulnerable to cyber attack, communications disruption, software compromise, or physical interference. Adversaries seeking to degrade national space capability may find it easier to ttarget ground infrastructure than orbital assets themselves. Cyber intrusions into command networks, disruptions to communications pathways, insider threats, and attacks on supporting digital infrastructure can all affect mission operations without requiring direct action against satellites in orbit.

This reality reflects a broader shift in the character of modern conflict. Increasingly, the objective is not necessarily to destroy infrastructure, but to disrupt the systems that enable infrastructure to function. Satellite Operation Centres represent particularly attractive targets because they serve as critical points of coordination, command, and control. A successful attack against an SOC can affect multiple satellites, communications links, and operational services simultaneously, creating disproportionate strategic consequences.

The growing complexity of satellite operations further amplifies this challenge. Modern constellations generate vast quantities of telemetry, operational data, imagery, communications traffic, and system status information. Managing these assets requires sophisticated software platforms, automated monitoring systems, artificial intelligence tools, cloud infrastructure, and secure communications networks. As satellite architectures become more distributed and data-intensive, the role of the SOC expands accordingly.

Artificial intelligence is already beginning to transform satellite operations. AI-enabled monitoring systems can identify anomalies, predict equipment failures, optimise satellite tasking, and support automated decision-making processes. Predictive analytics can reduce operational risk by identifying potential failures before they occur. Automated scheduling systems can optimise communications resources and payload utilisation. These capabilities increase efficiency while enabling operators to manage increasingly complex constellations with greater precision.

At the same time, the integration of AI introduces new considerations regarding security, transparency, and trust. As operational processes become increasingly automated, ensuring the integrity of algorithms, training data, and decision-support systems becomes a critical requirement. Future SOCs will need to balance automation with human oversight, ensuring that efficiency gains do not come at the expense of resilience and accountability.

The evolution of cloud computing is similarly reshaping satellite operations. Historically, mission operations were conducted through highly centralised facilities with dedicated infrastructure and tightly controlled access. While effective in relatively stable environments, such architectures can create vulnerabilities during crises or periods of disruption. The increasing adoption of cloud-enabled mission operations is enabling more flexible and distributed operating models. Data can be processed across multiple locations, mission functions can be transferred between facilities, and operators can maintain continuity even when individual sites experience disruption.

This transition toward distributed operations represents an important element of future resilience strategies. Rather than relying on a single facility, organisations are increasingly exploring architectures that distribute command functions across multiple sites, geographic regions, and cloud environments. Such approaches reduce dependence on individual facilities and improve the ability to sustain operations under contested conditions.

The concept of distributed SOCs is particularly relevant in an era characterised by cyber threats, electronic warfare, and spectrum contestation. A resilient architecture may involve multiple interconnected operation centres capable of sharing workloads, assuming operational

Much of the public discourse surrounding space security tends to focus on satellites themselves. Discussions often centre on launch vehicles, orbital constellations, anti-satellite weapons, Earth observation systems, or communications networks operating in space. While these capabilities undoubtedly form the visible face of modern space power, they represent only part of the larger operational ecosystem. Behind every satellite constellation, communications architecture, and ISR network lies a less visible but equally critical component: the command infrastructure that manages, controls, and sustains operations in orbit.

At the heart of this infrastructure are Satellite Operation Centres (SOCs). Traditionally, Satellite Operation Centres were viewed primarily as technical facilities responsible for spacecraft monitoring and control. Their core functions included tracking satellite health, monitoring payload performance, executing orbital manoeuvres, managing communications links, and ensuring mission continuity. In many respects, they were regarded as operational back offices—essential to mission success but largely removed from broader strategic considerations.

This perception is rapidly changing. As space systems become increasingly integrated into military operations, national security architectures, and critical communications networks, Satellite Operation Centres are evolving from technical facilities into strategic command nodes. They now occupy a central position within the broader ecosystem connecting satellites, ground infrastructure, communications networks, intelligence systems, and operational decision-makers. Their role is no longer limited to managing spacecraft; they increasingly facilitate the flow of information that underpins military effectiveness, situational awareness, and national resilience.

In a contemporary operational environment, satellites rarely function as isolated platforms. Communications satellites support military networks spanning vast geographic areas. Earth observation systems generate intelligence used by defence planners, border management agencies, and maritime security organisations. Navigation satellites provide positioning and timing services essential to military operations. These capabilities derive their operational value not merely from their presence in orbit, but from their ability to deliver information reliably to users on the ground. Satellite Operation Centres provide the bridge between orbital assets and terrestrial decision-making systems.

Consequently, the resilience of an SOC can be as important as the resilience of the satellites it controls. An advanced satellite constellation offers limited strategic value if its command infrastructure is vulnerable to cyber attack, communications disruption, software compromise, or physical interference. Adversaries seeking to degrade national space capability may find it easier to ttarget ground infrastructure than orbital assets themselves. Cyber intrusions into command networks, disruptions to communications pathways, insider threats, and attacks on supporting digital infrastructure can all affect mission operations without requiring direct action against satellites in orbit.

This reality reflects a broader shift in the character of modern conflict. Increasingly, the objective is not necessarily to destroy infrastructure, but to disrupt the systems that enable infrastructure to function. Satellite Operation Centres represent particularly attractive targets because they serve as critical points of coordination, command, and control. A successful attack against an SOC can affect multiple satellites, communications links, and operational services simultaneously, creating disproportionate strategic consequences.

The growing complexity of satellite operations further amplifies this challenge. Modern constellations generate vast quantities of telemetry, operational data, imagery, communications traffic, and system status information. Managing these assets requires sophisticated software platforms, automated monitoring systems, artificial



Decision Superiority in the Age of Multi-Domain Operations

The ultimate objective of modern military architectures is not the collection of data, the deployment of satellites, or even the protection of critical infrastructure. These capabilities are enablers. Their true value lies in their ability to generate a decisive operational advantage through faster, better-informed, and more effective decision-making.

For centuries, military success has depended on understanding the operational environment more accurately than an adversary. Generals sought information about troop movements, terrain, weather conditions, and enemy intentions. The side capable of observing more, understanding more, and responding more rapidly often gained the advantage. While the principles remain unchanged, the scale and complexity of the challenge have increased dramatically.

Modern military operations are conducted across multiple domains simultaneously. Land forces, naval assets, air platforms, cyber operations, electronic warfare units, and space-based capabilities increasingly operate as part of an interconnected battlespace. Events occurring in one domain can rapidly influence outcomes in another. A cyber intrusion may disrupt communications supporting maritime operations. Electronic warfare may degrade navigation systems affecting air operations. Space-enabled intelligence may alter tactical decisions on the ground. The interconnected nature of modern conflict demands an unprecedented level of coordination and situational awareness.

This evolution has given rise to the concept of multi-domain operations. Unlike traditional approaches that treated operational domains independently, multi-domain operations seek to integrate capabilities across land, sea, air, cyber, and space environments into a unified operational framework. The objective is not merely coordination, but synchronisation ensuring that information, resources, and decisions flow seamlessly across domains to create cumulative operational effects.

Achieving this objective requires a level of situational awareness that would have been unimaginable only a decade ago. Satellites continuously monitor activity across vast geographic regions. Unmanned aerial systems provide persistent surveillance over areas of interest. Ground-based sensors monitor movement, communications, and environmental conditions. Maritime platforms collect intelligence across sea lanes and strategic chokepoints. Cyber systems generate indicators of activity within digital networks. Together, these systems produce an enormous volume of information that must be transformed into operational understanding.
The challenge is increasingly one

of information management rather than information collection.

Military organisations today face a paradox. They possess access to more information than ever before, yet the ability to process, interpret, and utilise that information effectively has become a defining challenge. Vast quantities of data are of limited value unless they can be converted into actionable intelligence. This requirement has elevated the importance of data fusion, artificial intelligence, and advanced analytics within modern command architectures.
Data fusion involves integrating information from multiple sources into a coherent operational picture. Satellite imagery, signals intelligence, radar feeds, UAV surveillance, cyber indicators, and open-source information may individually provide only partial insight. When combined and analysed collectively, however, they can reveal patterns, identify anomalies, and generate a far more comprehensive understanding of the operational environment.

Artificial intelligence is becoming increasingly important in enabling this process. Modern ISR architectures generate data volumes that far exceed the capacity of human analysts alone. AI systems can rapidly process imagery, identify objects, detect unusual activity, prioritise threats, and support predictive analysis. They can assist commanders in identifying opportunities, assessing risks, and understanding emerging situations in near real time.

Importantly, the role of AI is not to replace human judgement. Strategic decision-making remains inherently human. Political considerations, escalation risks, operational trade-offs, and ethical responsibilities require human oversight and accountability. AI functions as a force multiplier, augmenting the ability of decision-makers to understand increasingly complex operational environments and respond more effectively.

The compression of decision cycles is becoming one of the defining characteristics of modern warfare. Adversaries are increasingly seeking to accelerate operations, overwhelm traditional command structures, and exploit delays in decision-making. The side capable of processing information and acting faster often gains a disproportionate advantage.

This concept is frequently described through the OODA Loop. In contemporary operations, satellites, ISR systems, communications networks, and command architectures collectively contribute to accelerating this cycle. Space-enabled communications reduce delays in information sharing. Persistent surveillance improves situational awareness. AI-assisted analytics support rapid interpretation. Resilient command networks facilitate timely decision-making. Together, these capabilities enable military organisations to operate inside an adversary's decision cycle, forcing them into a reactive posture.

A critical enabler of this transformation is the emergence of tactical cloud infrastructure and edge computing. Traditional command architectures often relied upon centralised processing centres where information was collected, analysed, and disseminated. While effective in relatively stable environments, such models can become vulnerable when communications are disrupted or operational tempos increase.

Tactical cloud architectures distribute computing resources across the operational environment, enabling information to be stored, processed, and shared closer to the point of need. Edge computing allows data to be analysed at or near the source of collection rather than being transmitted to distant processing facilities. These capabilities reduce latency, improve resilience, and enable faster decision-making in contested environments.

High Altitude Platform Systems (HAPS) are also emerging as important components of future multi-domain architectures. Operating between conventional aircraft and satellites, HAPS platforms can provide persistent surveillance, communications relay, and ISR support over specific geographic regions. Their ability to

remain airborne for extended periods while carrying sophisticated payloads makes them valuable additions to resilient information architectures. When integrated with satellites, UAVs, and terrestrial networks, HAPS platforms contribute to a layered operational ecosystem capable of sustaining situational awareness even under contested conditions.

Commercial capabilities are increasingly becoming part of this ecosystem as well. The growing availability of commercial Earth observation data, satellite communications services, and geospatial analytics is expanding access to information across both civilian and military sectors. Recent conflicts have demonstrated how commercial space systems can provide critical support for communications, intelligence gathering, and operational planning. This trend is likely to accelerate as commercial constellations continue to expand and mature.

For India, the implications are particularly significant. The country's expanding space capabilities, growing defence modernisation efforts, and movement toward integrated theatre commands create opportunities to leverage space-enabled information architectures more effectively. The ability to integrate military and civilian space assets, combine data from multiple sources, and enable real-time decision-making will become increasingly important in future operational environments.

Decision superiority is ultimately not a technological outcome; it is a strategic capability. It emerges when resilient infrastructure, advanced communications, persistent ISR, intelligent data fusion, and effective command architectures operate together as part of an integrated system. Satellites, command networks, SOCs, AI-enabled analytics, tactical cloud infrastructure, and multi-domain operations are not separate capabilities. They are interconnected components of a larger ecosystem designed to enable understanding, accelerate decision-making, and improve operational effectiveness.

The future battlespace will be characterised by speed, complexity, and information abundance. In such an environment, the decisive advantage will belong not necessarily to the side with the largest number of platforms or the greatest volume of data, but to the side capable of transforming information into understanding and understanding into action faster than its adversaries. Decision superiority, enabled by resilient space-enabled architectures, may therefore become one of the most important determinants of military effectiveness in the decades ahead.

Conclusion: Securing the Invisible Backbone

Space has transitioned from a specialised technological domain into a foundational pillar of modern military capability and national resilience. Communications, intelligence, surveillance, navigation, command and control, and increasingly decision-making itself are now dependent upon resilient space-enabled infrastructure. As this dependence deepens, the consequences of disruption become increasingly significant, extending beyond the battlefield to affect national security, economic stability, and sovereign decision-making.

The strategic challenge confronting nations is therefore no longer limited to developing advanced space capabilities. It is ensuring that those capabilities remain available, trusted, and operational in an environment characterised by persistent competition and continuous contestation. The rise of cyber threats, electronic warfare, spectrum denial, supply-chain vulnerabilities, and information manipulation has fundamentally altered the nature of conflict. Adversaries no longer need to destroy satellites to generate strategic effects; they need only disrupt the networks, systems, and infrastructure upon which those satellites depend.

In this environment, resilience emerges as the defining principle of future space security. The ability to absorb disruption, maintain operational continuity, adapt to changing conditions, and recover rapidly from attack is becoming as important as the capabilities themselves. The Three-Dimensional Security Framework Defence in Depth, Defence in Breadth, and Defence in Heightprovides a useful lens through which to understand this challenge. It recognises that security can no longer be confined to individual platforms, organisations, or domains. Instead, resilience must be embedded across the entire ecosystem, from satellites and ground stations to software networks, supply chains, command systems, and spectrum resources.

At the same time, resilient infrastructure is not an end in itself. Its ultimate purpose is to enable operational effectiveness. Modern military advantage increasingly depends upon the ability to collect information, maintain connectivity, fuse data, and transform knowledge into timely action. Command networks, C5ISR architectures, Satellite Operation Centres, artificial intelligence, and distributed communications systems collectively form the backbone of this capability. Together, they enable decision superiority the ability to understand, decide, and act faster than an adversary.

For India, the implications are profound. As the country's military capabilities, commercial space ecosystem, and strategic ambitions continue to expand, the protection of space-enabled infrastructure will become an increasingly important component of national security planning. Future resilience will depend not only on technological innovation, but also on institutional coordination, policy coherence, spectrum protection, commercial participation, and the integration of space capabilities within broader defence architectures.

The future contest for advantage will not be determined solely by who possesses the most satellites or the most sophisticated technologies. It will be shaped by who can ensure that their systems continue to function under conditions of disruption, uncertainty, and conflict. In an era where information is power and connectivity is capability, resilience is no longer a supporting requirement. It is becoming the foundation of national power itself.

Strategic Recommendations

1. Establish a National Space Security Architecture
India should develop an integrated national framework that brings together space security, cyber resilience, electronic warfare preparedness, spectrum management, and space situational awareness under a coordinated architecture. Future threats will span multiple domains simultaneously and require a unified response mechanism.

2. Recognise Space Systems as Critical National Security Infrastructure
Space-enabled communications, navigation, Earth observation, and military support systems should be formally treated as strategic national infrastructure. This would enable structured resilience planning, continuity frameworks, risk assessments, and dedicated protection mechanisms

3. Prioritise Spectrum Security and Frequency Agility
The electromagnetic spectrum must be recognised as a strategic resource essential to military operations and national resilience. Investments should focus on spectrum monitoring, anti-jamming capabilities, cognitive radio systems, and dynamic frequency management to ensure operational continuity in contested environments.

4. Build Resilient and Distributed Space Architectures
Future architectures should reduce dependence on single points of failure through distributed constellations, redundant communications pathways, responsive launch capabilities, and multi-layered systems integrating terrestrial networks, HAPS, LEO, and GEO assets.

5. Strengthen Satellite Operation Centres as Strategic Assets
Satellite Operation Centres should evolve into resilient, distributed, and cyber-secure mission management hubs capable of sustaining operations during disruption. Investments in cloud-enabled operations, AI-assisted monitoring, and geographically distributed backup facilities should be prioritised.

6. Accelerate Integration of Space within C5ISR Architectures
Space-enabled capabilities should be deeply embedded within future command, control, communications, intelligence, surveillance, and reconnaissance frameworks. This integration will be essential for supporting multi-domain operations and future theatre command structures.

7. Develop Trusted Artificial Intelligence for Space Operations
AI will increasingly underpin satellite operations, ISR analysis, spectrum management, and decision-support systems. India should invest in trusted AI frameworks, secure data architectures, and human-machine teaming models that enhance effectiveness while preserving accountability.

8. Trusted Commercial Space Ecosystem
Commercial operators are becoming important contributors to national resilience through communications, Earth observation, launch services, analytics, and digital infrastructure. Stronger collaboration between government, defence, academia, and industry will be essential for building a secure and innovative space ecosystem.

9. Invest in Indigenous High Altitude Platform Systems (HAPS)
HAPS can provide an additional layer of resilience between terrestrial and orbital systems. Their integration with satellite networks can strengthen communications, ISR, border surveillance, maritime monitoring, and disaster response capabilities.



MILITARY SPACE POWER AND THE OPERATIONALISATION OF INDIA'S MILITARY SPACE DOCTRINE

Introduction: The New Grammar of Military Power

This chapter begins with a simple but profound reality: the character of warfare is undergoing a fundamental transformation. Throughout history, military advantage was largely determined by the ability to mobilise manpower, project force, and control territory. Industrial-age warfare rewarded scale, logistics, and firepower. The twentieth century witnessed the rise of air power, mechanised warfare, precision munitions, and nuclear deterrence, each reshaping the strategic balance among nations.

The twenty-first century is witnessing a different revolution. Military effectiveness is increasingly being determined not only by the ability to destroy targets, but by the ability to acquire information, process it rapidly, make decisions faster than an adversary, and translate those decisions into coordinated action. Information has become a strategic resource, and the infrastructure that enables information superiority is emerging as one of the defining determinants of national power.

TAt the centre of this transformation lies space. For decades, space was viewed primarily as a supporting domain. Satellites provided communications, weather forecasting, navigation, and reconnaissance capabilities that enhanced military operations conducted elsewhere. Space enabled military effectiveness, but it was rarely considered a warfighting domain in its own right. Today, that distinction is disappearing. Space has evolved from a support function into a strategic domain that increasingly shapes the conduct, tempo, and outcomes of military operations.

Modern armed forces depend on space-enabled systems for intelligence collection, communications, navigation, targeting, surveillance, missile warning, and command and control. Every stage of the modern kill chain from detecting a target to engaging it with precision relies on information that is often generated, transmitted, or validated through space-based systems. Military formations operating across land, sea, air, cyber, and electromagnetic domains are increasingly connected through orbital infrastructure that enables situational awareness and operational coordination on an unprecedented scale.

This growing dependence has transformed the strategic value of space. It has also transformed the nature of military competition. Major powers no longer view space merely as an environment

for scientific exploration or technological achievement. It is increasingly regarded as a domain of strategic contestation, where access to information, freedom of operation, and decision advantage can determine military outcomes. The emergence of counterspace capabilities, persistent surveillance architectures, electronic warfare systems, cyber operations, and precision strike networks reflects this broader evolution.

Yet the significance of space extends beyond technology and hardware. The most consequential change underway is the shift from platform-centric warfare to decision-centric warfare. Historically, military power was measured through platforms—tanks, aircraft, warships, missile systems, and other visible instruments of force. Today, military effectiveness is increasingly influenced by the ability to connect those platforms through networks, fuse information from multiple sources, and generate superior decisions at speed and scale.

This evolution is compressing the time available for military decision-making. Advances in space-based surveillance, artificial intelligence, data fusion, onboard processing, and communications networks are accelerating the pace of operations. The side capable of observing first, understanding first, deciding first, and acting first gains a disproportionate advantage. Military competition is therefore becoming a contest not only of capabilities, but of decision architectures.

For India, these developments carry profound implications. The country's expanding space capabilities, evolving security environment, and growing emphasis on joint military operations require a more integrated understanding of how space contributes to national power. While India has made significant progress in developing launch systems, satellite capabilities, and defence space institutions, the next phase of growth will require something more fundamental: the effective implementation of India's Joint Doctrine for Military Space and the continued refinement of frameworks linking capability development with strategic objectives.

The release of India's Joint Doctrine for Military Space in September 2025 represents an important milestone in the country's evolution as a space power. It reflects a growing recognition that space must be understood not merely as a technological domain, but as an operational and strategic enabler of military effectiveness. The significance of the doctrine lies not only in its publication, but in its potential to guide future force development, joint operations, resilience planning, and multi-domain integration.

The adoption of India's Joint Doctrine for Military Space marks an important step in recognising that space can no longer be viewed solely through the lens of technology or infrastructure. The next challenge lies in translating doctrinal principles into operational capability. This chapter therefore examines the evolving military role of space through three interconnected lenses: the emergence of an increasingly contested and adversarial space environment, the growing importance of space-enabled precision warfare and A2AD architectures, and the need for a distinctly Indian approach to military space doctrine. Together, these themes offer insight into how the future battlespace is being reshaped and what it means for India's strategic posture in the decades ahead.



The Adversarial Space Domain: From Strategic Sanctuary to Strategic Contest

For much of the space age, outer space was viewed as a relatively benign operating environment. Competition certainly existed, particularly during the Cold War, but space largely remained a domain associated with strategic signalling, technological prestige, scientific exploration, and intelligence collection. Satellites provided critical support to military operations, yet the domain itself was rarely perceived as an active battlefield.

That assumption is rapidly changing. The growing dependence of modern militaries on space-enabled services has fundamentally altered the strategic value of space. Communications, intelligence collection, missile warning, navigation, targeting, and command and control now rely heavily on orbital infrastructure. As a result, space systems are no longer simply enablers of military power; they are becoming critical components of military power itself.

This transformation has created a powerful incentive for nations to develop capabilities that can influence, disrupt, or deny an adversary's access to space-enabled advantages. Consequently, the contemporary space environment is increasingly characterised by strategic competition, operational contestation, and military planning that extends well beyond the Earth's atmosphere.

The emergence of this adversarial space domain reflects a broader shift in military thinking. Historically, strategic competition focused primarily on land, maritime, and air domains. Today, military planners increasingly recognise that operational success within these traditional domains depends upon information and connectivity generated from space. The ability to observe, communicate, navigate, and coordinate forces often determines the effectiveness of military operations. Consequently, the ability to influence an adversary's space architecture can generate effects throughout the broader battlespace.

This reality is particularly evident in the evolving military space strategies of major powers. Space is no longer viewed merely as a support function for terrestrial operations. It is increasingly treated as an operational domain in its own right one that must be protected, defended, and, if necessary, contested.

Among emerging space powers, China represents perhaps the most comprehensive example of this transformation. Over the past two decades, China has pursued a systematic effort to integrate space capabilities into its broader military modernisation programme. This effort extends far beyond the acquisition of satellites. It encompasses intelligence, surveillance, and reconnaissance constellations; communications networks; navigation systems; space situational awareness capabilities; counter-

space technologies; and increasingly sophisticated command architectures.

The significance of these developments lies not simply in the number of satellites deployed, but in the strategic philosophy underpinning them. China's military space programme reflects a recognition that future military advantage will depend upon information superiority, precision engagement, and the ability to operate effectively across multiple domains simultaneously. Space serves as the connective infrastructure enabling these capabilities.

Consequently, the distinction between support systems and combat systems is becoming increasingly blurred. A satellite that provides imagery, communications, or navigation may not be a weapon in the traditional sense, yet its contribution to military effectiveness can be decisive. This dual-use nature of space systems complicates traditional assumptions about deterrence, escalation, and military competition.

The adversarial space domain is therefore not defined solely by weapons designed to destroy satellites. It is increasingly characterised by competition over information itself. Nations seek to preserve their own access to information while denying, degrading, manipulating, or disrupting the information architectures upon which adversaries depend. This competition spans multiple dimensions, including cyber operations, electronic warfare, spectrum contestation, space situational awareness, and counterspace capabilities.

An important consequence of this evolution is the growing vulnerability of military operations to disruptions originating far beyond the immediate battlefield. A disruption to communications satellites may affect command networks. Interference with navigation systems may degrade precision strike capabilities. The compromise of space-enabled intelligence systems may reduce situational awareness and decision quality. In each case, the objective is not necessarily physical destruction but the degradation of military effectiveness through the disruption of information flows.

This dynamic is giving rise to a new strategic reality. Military competition is increasingly becoming a contest between interconnected systems rather than isolated platforms. Space occupies a central position within these systems because it provides the infrastructure through which information is collected, transmitted, processed, and distributed. As dependence on this infrastructure grows, so too does the incentive to contest it.

For India, the emergence of an adversarial space domain presents both challenges and opportunities. The country's expanding military, economic, and technological interests increasingly depend upon access to resilient space-enabled capabilities. At the same time, India's strategic environment is becoming more complex as neighbouring states and major powers continue to expand their military space capabilities.

Understanding this evolving environment is therefore not merely an academic exercise. It is essential for shaping future approaches to deterrence, resilience, force modernisation, and military doctrine. The challenge is no longer simply to participate in the space domain. It is to operate effectively within an environment that is becoming progressively more contested, competitive, and strategically significant.

The implications of this transformation extend far beyond orbital competition itself. They are reshaping the character of warfare, influencing military doctrine, and redefining how nations generate strategic advantage. The next phase of this evolution can be seen in the rise of precision warfare, where space-enabled information increasingly determines how military force is applied and how future conflicts are likely to be fought.



The Changing Character of Warfare: From Industrial Firepower to Information Dominance

The history of warfare can be understood as a succession of revolutions in how military power is generated and applied. Each era has been shaped by a dominant source of advantage. In the industrial age, military effectiveness was determined largely by mass, production capacity, logistics, and the ability to mobilise large forces. The world wars demonstrated the importance of industrial power, where victory often depended upon the ability to outproduce and outlast an adversary.

The latter half of the twentieth century introduced a different paradigm. Advances in air power, precision-guided munitions, electronic warfare, and communications networks enabled militaries to achieve effects that were disproportionate to the size of the forces employed. The emphasis gradually shifted from mass to precision, from quantity to effectiveness, and from attrition to information-enabled operations.

The 1991 Gulf War is often regarded as a watershed moment in this transformation. For the first time, the world witnessed the large-scale integration of space-based navigation, satellite communications, precision-guided weapons, and real-time intelligence. The conflict demonstrated that superior information and precision engagement could dramatically alter the conduct of military operations. It became evident that the future battlefield would be shaped not only by weapons systems, but by the networks that connected them.

Three decades later, that transformation has accelerated significantly. Modern warfare is increasingly defined by the ability to acquire, process, distribute, and exploit information faster than an adversary. Military success now depends as much on situational awareness and decision-making as it does on traditional combat power. The side capable of understanding the battlefield more comprehensively and responding more rapidly often gains a decisive advantage.

This evolution has given rise to what many strategists describe as information-centric warfare. In this model, information becomes both a resource and a weapon. Sensors, communications networks, intelligence platforms, cyber capabilities, and space-based systems combine to create an interconnected operational environment where data flows continuously between platforms, commanders, and decision-makers.

Space occupies a central position within this architecture. Satellites provide the persistent surveillance that enables situational awareness. Navigation systems support precision operations. Communications satellites connect dispersed forces across vast geographic areas. Earth observation constellations generate intelligence that informs operational planning and targeting decisions. Together, these capabilities create an information infra-

The history of warfare can be understood as a succession of revolutions in how military power is generated and applied. Each era has been shaped by a dominant source of advantage. In the industrial age, military effectiveness was determined largely by mass, production capacity, logistics, and the ability to mobilise large forces. The world wars demonstrated the importance of industrial power, where victory often depended upon the ability to outproduce and outlast an adversary.

The latter half of the twentieth century introduced a different paradigm. Advances in air power, precision-guided munitions, electronic warfare, and communications networks enabled militaries to achieve effects that were disproportionate to the size of the forces employed. The emphasis gradually shifted from mass to precision, from quantity to effectiveness, and from attrition to information-enabled operations.

The 1991 Gulf War is often regarded as a watershed moment
in this transformation. For the first time, the world witnessed the large-scale integration of space-based navigation, satellite communications, precision-guided weapons, and real-time intelligence. The conflict demonstrated that superior information and precision engagement could dramatically alter the conduct of military operations. It became evident that the future battlefield would be shaped not only by weapons systems, but by the networks that connected them.

Three decades later, that transformation has accelerated significantly. Modern warfare is increasingly defined by the ability to acquire, process, distribute, and exploit information faster than an adversary. Military success now depends as much on situational awareness and decision-making as it does on traditional combat power. The side capable of understanding the battlefield more comprehensively and responding more rapidly often gains a decisive advantage.

This evolution has given rise to what many strategists describe as information-centric warfare. In this model, information becomes both a resource and a weapon. Sensors,communications networks, intelligence platforms, cyber capabilities, and space-based systems combine to create an interconnected operational environment where data flows continuously between platforms, commanders, and decision-makers.

Space occupies a central position within this architecture. Satellites provide the persistent surveillance that enables situational awareness. Navigation systems support precision operations. Communications satellites connect dispersed forces across vast geographic areas. Earth observation constellations generate intelligence that informs operational planning and targeting decisions. Together, these capabilities create an information infrastructure upon which modern military operations increasingly depend.

The significance of this transformation lies in its impact on decision-making. Historically, commanders often operated with incomplete information and significant delays between observation and action. Intelligence collection, analysis, dissemination, and execution were frequently separated by hours or even days. Modern space-enabled architectures are steadily compressing these timelines.

Advances in satellite imagery, synthetic aperture radar, signals intelligence, cloud computing, artificial intelligence, and data fusion technologies now allow information to move through military organisations at unprecedented speeds. Events occurring on the battlefield can increasingly be detected, analysed, and acted upon in near real time. This acceleration is reshaping operational planning, command structures, and force employment concepts across the world.



Space as the Foundation of Deep Precision Operations

The transformation of warfare from industrial-age attrition to information-centric competition has elevated the importance of precision. Modern military success increasingly depends not on the volume of firepower applied, but on the ability to apply force accurately, rapidly, and at the most consequential point in time and space. Precision has become both an operational requirement and a strategic advantage.

Yet precision does not emerge from weapons alone. Precision-guided munitions, long-range missile systems, autonomous platforms, and advanced aircraft often receive considerable attention because they represent the visible instruments of military power. However, their effectiveness is fundamentally dependent on a less visible layer of infrastructure that enables forces to detect, identify, track, communicate, navigate, and engage targets with confidence. Increasingly, that infrastructure resides in space.

Modern precision warfare is built upon what may be described as a space-enabled operational architecture. This architecture combines intelligence, communications, navigation, and timing capabilities into a single ecosystem that supports every stage of military operations. Space systems do not merely support combat; they increasingly determine the quality, speed, and effectiveness of military action itself.

The Space Triad

At the heart of this architecture lies a combination of three mutually reinforcing capabilities: Intelligence, Surveillance and Reconnaissance (ISR); Positioning, Navigation and Timing (PNT); and Assured Communications. Together, these capabilities form the operational backbone of deep precision warfare.

ISR provides visibility across the battlespace. PNT provides precision and synchronisation. Communications provide connectivity and command. The absence of any one of these elements significantly degrades military effectiveness. Together, they create the information architecture that enables modern operations.

This triad has become increasingly important because contemporary warfare is no longer confined to geographically defined battlefields. Military forces operate across multiple domains simultaneously, often over vast distances and within highly dynamic operational environments. Maintaining awareness, coordination, and responsiveness under such conditions requires persistent access to information and assured connectivity.

ISR: The Eyes of Precision Warfare

The first component of the space triad is Intelligence, Surveillance and Reconnaissance.

Historically, military commanders relied on reconnaissance patrols, airborne observation, and human intelligence to understand the operational environment. Today, satellite constellations provide persistent surveillance across vast geographic areas, enabling the continuous monitoring of activities on land, at sea, and increasingly within the electromagnetic domain.

Advances in Earth observation technologies have significantly enhanced this capability. High-resolution optical imagery, synthetic aperture radar, hyperspectral sensing, and signals intelligence systems can now provide detailed situational awareness under a wide range of environmental conditions. More importantly, the growing availability of commercial satellite imagery has expanded access to information far beyond traditional military organisations.

Persistent ISR fundamentally alters military planning. The ability to observe activity continuously reduces uncertainty, improves targeting accuracy, and enables commanders to anticipate developments rather than merely react to them. In effect, ISR reduces the fog of war by transforming unknowns into observable variables.

The strategic significance of this capability extends beyond intelligence collection. Persistent surveillance increasingly shapes deterrence, operational planning, force protection, and strategic decision-making. The side capable of seeing more, seeing earlier, and seeing continuously enjoys a substantial advantage.

PNT and Assured Communications: Enabling Precision at Scale

While ISR provides awareness, awareness alone is insufficient to achieve operational effects. Military forces must also know where they are, where their targets are located, and how to coordinate activities across dispersed formations. This is where Positioning, Navigation and Timing and assured communications become indispensable.

PNT systems provide the precision necessary for modern military operations. Precision-guided munitions, missile systems, aircraft, naval platforms, autonomous vehicles, and command networks all rely upon accurate positioning and timing information. The ability to synchronise activities across multiple domains increasingly depends on trusted navigation and timing services.

Equally important are communications systems that connect sensors, commanders, and operational units. Modern military organisations generate enormous volumes of information. The value of that information depends on the ability to move it rapidly and securely across the force. Space-based communications provide the connectivity required to coordinate operations over large geographic areas, particularly in environments where terrestrial infrastructure may be unavailable, degraded, or contested.

Together, PNT and communications transform information into action. They ensure that intelligence can be shared, decisions can be communicated, and military effects can be coordinated with precision and speed.

The strategic importance of these capabilities becomes particularly evident in long-range precision operations. A target may be identified through satellite imagery, validated through multiple intelligence sources, tracked through persistent surveillance, and engaged by a platform operating hundreds or even thousands of kilometres away. Such operations are possible only when ISR, PNT, and communications function as part of an integrated architecture.



A2AD and the New Geometry of Conflict

Throughout much of military history, geography was one of the most important determinants of strategic advantage. Mountain ranges, rivers, oceans, deserts, and distance shaped military campaigns, influenced force deployment, and often determined the outcome of conflicts. The ability to project power across geographic barriers represented a major source of military strength, while natural obstacles frequently provided defensive advantages to those seeking to deny access to territory or strategic objectives.

The emergence of space-enabled military architectures is fundamentally altering this relationship between geography and warfare. Modern military competition is increasingly shaped not only by physical terrain, but also by the ability to control access, movement, information, and decision-making within contested operational environments. This shift is particularly evident in the evolution of Anti-Access and Area Denial (A2AD) strategies, which have emerged as one of the defining characteristics of contemporary military planning.

At its core, A2AD seeks to achieve a relatively simple objective: prevent an adversary from operating freely within a designated region. Anti-Access capabilities are designed to restrict the ability of opposing forces to enter a theatre of operations, while Area Denial capabilities seek to constrain their freedom of manoeuvre once they are present. Together, these approaches create operational environments in which movement becomes costly, uncertain, and increasingly risky.

What distinguishes contemporary A2AD architectures from earlier defensive strategies is the central role played by information. Modern denial strategies depend less on static defensive positions and more on the ability to detect, track, target, and engage adversary forces across large geographic areas.

The Rise of Denial Strategies

The growing prominence of A2AD reflects broader changes in the character of warfare. As precision strike capabilities have become more sophisticated, military forces have acquired the ability to influence events at increasingly greater distances. Long-range missile systems, precision-guided weapons, unmanned platforms, and advanced surveillance architectures now allow forces to identify and engage targets far beyond traditional front lines.

This development has created new opportunities for denial-based strategies. Rather than seeking to defeat adversaries through direct confrontation alone, states increasingly seek to shape the operational environment itself. The objective is not merely to destroy opposing forces, but to restrict their options, complicate their planning, and impose costs on their operations.

Space-Enabled A2AD Architectures

The effectiveness of A2AD depends upon the integration of multiple capabilities into a coherent operational system. Surveillance satellites provide persistent monitoring. Communications networks connect sensors with decision-makers. Navigation systems support precision engagement. Data fusion architectures transform observations into actionable intelligence. Long-range strike systems provide the means to generate military effects.

Individually, each capability contributes to operational effectiveness. Collectively, they create what is increasingly described as a kill web—a networked architecture capable of detecting, tracking, targeting, and engaging adversaries across multiple domains.

Space occupies a central position within this architecture because it enables persistent awareness at scale. Unlike terrestrial sensors constrained by geography or line-of-sight limitations, space-based systems can monitor vast regions continuously and provide information across national boundaries and operational theatres. This persistent visibility significantly enhances the effectiveness of denial strategies.

The growing integration of space-based sensing with missile forces, maritime systems, air defence networks, and electronic warfare capabilities is transforming how military power is projected and contested. Future conflicts are likely to involve highly interconnected operational environments where information flows continuously between sensors and effectors, reducing the time available for adversaries to respond.

This evolution is particularly evident in the Indo-Pacific region, where large geographic distances, maritime competition, and long-range precision strike capabilities are increasingly shaping strategic planning. Here, the ability to maintain awareness and deny operational freedom may prove as important as traditional measures of military strength.

The Battle for Freedom of Action

The strategic significance of A2AD lies in its impact on freedom of action. Military operations ultimately depend upon the ability to manoeuvre, communicate, sustain forces, and apply effects where and when required. Denial strategies seek to constrain these activities by increasing uncertainty and reducing operational flexibility.

In this sense, future conflicts may increasingly become contests over access rather than territory. The objective may not be to occupy physical space, but to control the conditions under which others can operate. Space-enabled architectures play a critical role in this process because they provide the information infrastructure necessary to monitor activity, coordinate responses, and sustain operational awareness.

This dynamic is changing the geometry of conflict. Traditional military planning often focused on front lines, territorial boundaries, and physical objectives. Contemporary operational environments are becoming increasingly multidimensional, spanning land, sea, air, cyber, electromagnetic, and space domains simultaneously. Actions occurring in one domain can rapidly influence outcomes in another, creating a highly interconnected battlespace in which information becomes the principal enabler of military power.

For India, these developments have important implications. The country's strategic environment includes contested borders, expansive maritime interests, and a rapidly evolving regional security landscape. Maintaining freedom of action across these environments will increasingly depend upon the ability to generate persistent awareness, integrate information



The Battle for Decision Advantage

Military history has often been interpreted through the lens of technology, geography, and firepower. Yet beneath every major military transformation lies a more fundamental reality: warfare is ultimately a contest of decisions. Commanders seek to understand the operational environment, anticipate adversary actions, allocate resources, and translate intent into action. Success frequently depends not on who possesses the greatest number of platforms or weapons, but on who can make better decisions, faster and with greater confidence.

In the emerging era of information-centric warfare, this principle is becoming more pronounced than ever before.

The increasing integration of space systems, artificial intelligence, advanced sensors, communications networks, and data analytics is transforming military competition into a contest for decision advantage. Modern warfare is increasingly characterised by an abundance of information rather than a scarcity of it. The challenge facing military organisations is no longer collecting data; it is converting vast quantities of data into operational understanding and actionable decisions before an adversary can do the same.

This transformation represents a profound shift in the nature of military power. Historically, military advantage was often measured through visible indicators such as force size, industrial capacity, and weapon inventories. While these factors remain important, they are increasingly influenced by a less visible variable: the speed and quality of decision-making.

From Information Superiority to Decision Superiority

The concept of information superiority emerged during the late twentieth century as military organisations recognised the growing importance of sensors, communications networks, and digital technologies. The objective was straightforward: acquire better information than an adversary and use it to improve operational effectiveness.

Today, however, information superiority alone is insufficient. Modern militaries often possess access to enormous volumes of information from satellites, UAVs, radar systems, electronic intelligence networks, cyber operations, commercial data sources, and open-source intelligence. Possessing information is no longer the primary challenge. Understanding it, prioritising it, and acting upon it rapidly have become the decisive factors.

This evolution has given rise to the concept of decision superiority. Decision superiority refers to the ability to observe, interpret, decide, and act more effectively than an adversary while operating under conditions of uncertainty



The concept of information superiority emerged during the late twentieth century as military organisations recognised the growing importance of sensors, communications networks, and digital technologies. The objective was straightforward: acquire better information than an adversary and use it to improve operational effectiveness.

Today, however, information superiority alone is insufficient. Modern militaries often possess access to enormous volumes of information from satellites, UAVs, radar systems, electronic intelligence networks, cyber operations, commercial data sources,

The Sensor-to-Shooter Revolution

One of the most visible manifestations of decision-centric warfare is the evolution of the sensor-to-shooter cycle. Traditionally, military operations involved a series of sequential processes. Information was collected, transmitted to headquarters, analysed by specialists, reviewed by commanders, and eventually translated into action. While effective in relatively stable environments, such processes often required significant time. Delays between detection and engagement could extend from hours to days, providing adversaries with opportunities to manoeuvre, conceal, or reposition forces.

Modern operational architectures seek to compress this cycle dramatically. Advances in space-based surveillance, data fusion, secure communications, and automation increasingly allow information to move directly from sensors to operational decision-makers. Targets can be identified, validated, and engaged far more rapidly than was previously possible. The objective is not simply to increase speed, but to reduce the gap between awareness and action.

This compression of time is reshaping military operations. Future conflicts are likely to be characterised by rapidly evolving situations in which delays of minutes or even seconds can influence outcomes. Forces capable of shortening their sensor-to-shooter cycles gain a significant advantage in generating operational effects and maintaining initiative.



Artificial Intelligence and the Compression of Decision Cycles

Artificial intelligence is accelerating this transformation. The volume of information generated by modern military systems increasingly exceeds the capacity of human analysts alone. Satellite constellations, surveillance networks, electronic intelligence systems, cyber monitoring tools, and autonomous platforms collectively produce enormous quantities of data. Extracting meaningful insight from this information requires increasingly sophisticated analytical tools.

AI offers the ability to identify patterns, detect anomalies, prioritise threats, automate routine analysis, and support decision-making at unprecedented speeds. Machine learning systems can process imagery, analyse behavioural indicators, correlate information from multiple sources, and assist commanders in understanding rapidly evolving operational environments.

The significance of AI lies not merely in automation, but in its ability to compress decision cycles. Tasks that once required large teams of analysts and extended periods of review can increasingly be performed in near real time. This acceleration allows military organisations to respond more rapidly to emerging threats and opportunities.

At the same time, the growing reliance on AI introduces new challenges. Trust, transparency, data integrity, and algorithmic resilience become critical considerations when decisions carry strategic consequences. Future military organisations will therefore need to balance automation with human judgement, ensuring that technological speed does not come at the expense of strategic understanding.



The Future Contest: Advantage versus Paralysis

The ultimate objective of modern military competition is increasingly becoming the creation of decision advantage while imposing decision paralysis on an adversary. Decision advantage enables military organisations to maintain initiative, exploit opportunities, and shape the operational environment. Decision paralysis, by contrast, creates uncertainty, confusion, delay, and reduced freedom of action. A force that cannot understand what is happening, cannot trust the information it receives, or cannot respond in time becomes progressively less effective regardless of the quality of its platforms or weapons.

This reality is reshaping military strategy. Adversaries increasingly seek to disrupt communications, manipulate information, interfere with sensors, contest spectrum, and degrade situational awareness. Such actions are not necessarily intended to destroy military capability outright. Rather, they seek to slow decision-making, create uncertainty, and undermine confidence within command structures. In this sense, future warfare may increasingly become a contest between competing decision architectures. One side seeks to accelerate understanding, improve coordination, and shorten response times. The other seeks to create delay, confusion, and disruption.

For India, the implications are profound. As military operations become increasingly data-driven and networked, the ability to generate decision advantage will become a critical component of deterrence and operational effectiveness. Investments in satellites, ISR systems, communications networks, artificial intelligence, and resilient command architectures should therefore be viewed not as isolated capabilities, but as elements of a broader decision ecosystem.

Ultimately, the future battlefield may be defined less by who possesses the most platforms and more by who can convert information into action most effectively. In an environment characterised by persistent surveillance, compressed timelines, and multi-domain operations, the ability to make better decisions faster than an adversary may become the most important military advantage of all.

The challenge for India is therefore not simply to acquire advanced space capabilities, but to integrate them into a coherent strategic framework. Capability creates potential. Doctrine transforms potential into power. As space becomes increasingly central to military effectiveness, the successful implementation and institutionalisation of India's military space doctrine becomes essential.



From Doctrine to Military Space Power

For much of its space journey, India has approached space primarily as a domain of technological achievement, national development, and strategic capability building. The country's space programme has delivered remarkable successes across communications, Earth observation, navigation, launch systems, disaster management, and scientific exploration. These achievements have contributed significantly to economic development, governance, and national prestige while also providing important support to defence and security requirements.

However, the strategic environment in which these capabilities operate is changing rapidly. The growing militarisation of space, the emergence of counterspace capabilities, the increasing dependence of modern warfare on space-enabled systems, and the rise of information-centric military competition are creating challenges that extend beyond technology. The central question is no longer whether India possesses space capabilities. The more important question is how those capabilities should be employed, protected, integrated, and leveraged to support national security objectives in an increasingly contested environment.

This distinction is important because capability and doctrine are not the same thing.Capabilities provide tools. Doctrine provides purpose. Capabilities determine what a nation can do. Doctrine determines how, when, and why those capabilities should be employed.

Throughout military history, technological superiority alone has rarely guaranteed strategic success. The decisive advantage has often belonged to those capable of integrating technology within coherent operational concepts and strategic frameworks. Aircraft existed before air power doctrine. Tanks existed before armoured warfare doctrine. Cyber capabilities existed before cyber strategy. In each case, the transformative impact emerged not from the technology itself, but from the development of concepts that connected capability with purpose.

India's expanding space capabilities now face a similar inflection point.

Beyond Capability Accumulation

Much of the current discussion surrounding military space power focuses on assets. Attention is often directed toward the number of satellites launched, the sophistication of sensors deployed, the availability of communications systems, or the range of navigation capabilities available. These are important indicators of national capability, but they do not in themselves constitute military space power.

Military space power emerges when capabilities are integrated into a broader framework that supports deterrence, operational effectiveness, resilience, and strategic decision-making.
A nation may possess advanced satellites yet lack the institutional structures required to exploit their full potential during crisis or conflict. It may have sophisticated Earth observation systems but lack mechanisms for integrating that information into operational planning. It may possess communications infrastructure without fully incorporating it into joint military operations. In such cases, capability exists, but power remains under-realised.

As India's military modernisation accelerates and defence operations become increasingly joint and technology-enabled, the need for a doctrine-driven approach becomes more pronounced. Space can no longer be viewed as a specialised support function operating on the margins of military planning. It must increasingly be understood as a foundational enabler of military effectiveness.

The Challenge of Strategic Integration

One of the defining characteristics of future warfare will be the integration of multiple domains. Military operations will increasingly span land, sea, air, cyber, electromagnetic, and space environments simultaneously. Actions occurring in one domain will rapidly influence outcomes in another. The effectiveness of military forces will therefore depend upon their ability to operate within interconnected operational architectures rather than isolated service-specific structures.

This evolution creates new demands for strategic integration. Space-enabled ISR supports maritime awareness, air operations, land campaigns, missile defence, and strategic decision-making. Satellite communications connect dispersed formations across theatres. Navigation systems support precision engagement and operational synchronisation. Space-based services increasingly influence every level of military activity, from tactical operations to strategic planning.
Yet the value of these capabilities depends upon their integration into broader operational concepts. Without doctrine, individual capabilities risk developing in parallel rather than as part of a coherent system. The challenge is not simply to connect satellites to military operations. It is to integrate space into the very logic of military planning, force design, deterrence, and warfighting.

The emergence of integrated theatre commands further reinforces this requirement. Joint operations demand common situational awareness, interoperable communications, shared intelligence architectures, and coordinated decision-making. Space-enabled capabilities provide much of the infrastructure necessary to support these objectives. A military space doctrine can serve as the framework through which these capabilities are organised and employed.

A Doctrine for the Information Age

The ultimate purpose of a military space doctrine is not to prescribe the use of specific technologies. Technologies will evolve continuously. Satellites, sensors, artificial intelligence systems, communications architectures, and autonomous platforms will change over time. Doctrine must therefore operate at a higher level.

Its purpose is to define how a nation intends to generate strategic advantage within a changing security environment.

For India, that advantage will increasingly depend upon the ability to maintain awareness, preserve connectivity, protect critical information architectures, support precision operations, and sustain decision superiority under contested conditions. These objectives extend beyond any individual satellite programme or technological capability. They require a coherent vision linking space capabilities with national security strategy. The development of such a doctrine represents the next stage in India's evolution as a space power. The challenge is no longer merely to build space systems. It is to transform those systems into instruments of national power capable of supporting deterrence, resilience, and military effectiveness in an increasingly complex strategic environment.

The question, therefore, is no longer whether India requires a military space doctrine. The adoption of the Joint Doctrine for Military Space has already provided an important conceptual foundation. The challenge now is how its principles can be operationalised across force structure, capability development, theatre commands, space-domain awareness, commercial integration, and future multi-domain operations.

Conclusion: From Space Capability to Space Power

The evolution of military space capabilities is reshaping the foundations of national power and military effectiveness. What began as a domain primarily associated with communications, navigation, and reconnaissance has emerged as a central pillar of modern warfare, influencing everything fromintelligence collection and precision engagement to deterrence, operational planning, and strategic decision-making.

This transformation reflects a broader shift in the character of conflict. Contemporary warfare is no longer defined solely by the movement of forces across land, sea, and air. It is increasingly characterised by the movement of information across networks, sensors, command architectures, and decision ecosystems. Military advantage depends not only on the ability to generate combat power, but on the ability to perceive, understand, and respond faster than an adversary.
Space lies at the centre of this transformation. Persistent surveillance architectures are reducing the traditional advantages of geography and concealment. Space-enabled communications are connecting forces across vast operational theatres. Navigation and timing systems are enabling precision engagement at unprecedented ranges. Artificial intelligence, cloud computing, and data fusion are accelerating the conversion of information into operational action. Together, these developments are compressing decision cycles and creating new forms of military competition centred on information superiority and decision advantage.

At the same time, the strategic environment is becoming increasingly contested. Counterspace capabilities, electronic warfare systems, cyber operations, and denial architectures are transforming space from a supporting environment into a domain of strategic competition. The challenge is no longer simply to access space, but to operate effectively within an environment where access, awareness, and freedom of action may be continuously contested.

For India, this evolution presents both opportunity and responsibility. The country has made remarkable progress in building indigenous space capabilities and establishing itself as a major spacefaring nation. However, the next phase of growth will require a transition from capability development to strategic integration. The question is no longer whether India can build satellites, launch vehicles, and communications systems. The question is how these capabilities can be integrated into a coherent framework that supports deterrence, military effectiveness, resilience, and strategic autonomy.

This is ultimately the purpose of military space doctrine. Doctrine serves as the bridge between capability and strategy. It provides the principles that guide how capabilities are organised, protected, integrated, and employed in support of national objectives. As military operations become increasingly dependent on space-enabled architectures, the development of a coherent doctrinal framework becomes essential for ensuring that technological investments translate into operational and strategic advantage.

The future military balance will not be determined solely by who possesses the largest constellation, the most advanced sensors, or the greatest number of platforms. It will increasingly be shaped by who can integrate capabilities into resilient operational architectures, sustain information superiority, and generate decision advantage under contested conditions.

India's emergence as a space power will therefore be defined not only by what it builds in space, but by how effectively it integrates space into its broader vision of national security and military strategy. The transition from space capability to space power has already begun. The challenge for the coming decade is to ensure that it is guided by a clear strategic purpose and a coherent doctrinal foundation.



Strategic Priorities for the Next Decade

- **Understanding the Adversarial Space Environment**

India's future military planning must recognise that space is increasingly becoming a contested operational domain. Strategic competition, counterspace capabilities, and denial strategies are likely to shape the future security environment and must be incorporated into long-term planning assumptions.

- **From Space Support to Space Power**

Space can no longer be viewed solely as an enabling capability. It is increasingly becoming an integral component of military effectiveness, deterrence, and national power. Future approaches should reflect this shift from support functions to strategic integration.

- **Building Sovereign ISR Dominance**

Persistent awareness will become a prerequisite for military effectiveness. Investments in Earth observation, maritime surveillance, electronic intelligence, and space-based sensing must focus not only on collection but on creating comprehensive situational awareness across multiple domains.

- **Accelerating the Sensor-to-Shooter Cycle**

Future conflicts will reward speed. The ability to reduce the time between detection, decision, and engagement will become a critical determinant of operational success. Integrated architectures that connect sensors, decision-makers, and effectors will be increasingly important.

- **Preparing for a World Without Sanctuary**

Persistent surveillance and advanced sensing technologies are reducing the ability of military forces to conceal activity. Future concepts of operation must account for an environment in which movements, deployments, and preparations are increasingly observable.

- **Integrating Space into Joint Warfighting**

Space capabilities must become an integral part of joint operational planning rather than a specialised support function. The effectiveness of future theatre commands will depend upon seamless integration of space-enabled intelligence, communications, and navigation capabilities..

- **Building Resilient Military Space Architectures**

Operational effectiveness requires continuity under contested conditions. Resilience, redundancy, distributed architectures, and survivability must become foundational principles of future military space systems.

- **Harnessing Artificial Intelligence for Decision Advantage**

Artificial intelligence will increasingly shape how information is processed, prioritised, and acted upon. The integration of AI into military space architectures should focus on enhancing situational awareness, accelerating decision-making, and supporting operational agility.

The Decline of Strategic Sanctuary

Another consequence of the space age is the gradual erosion of what military strategists once described as strategic sanctuary. For centuries, states relied upon distance, terrain, concealment, and remoteness to protect critical assets and activities. Mountain ranges, deserts, forests, and vast oceanic spaces provided natural barriers that complicated observation and limited awareness.

Today, those barriers are becoming increasingly permeable. The proliferation of Earth observation satellites has created a world characterised by persistent surveillance. Commercial operators now deploy constellations capable of imaging the same location multiple times per day. Synthetic Aperture Radar (SAR) satellites can observe through clouds, smoke, and darkness. Artificial intelligence enables rapid analysis of enormous volumes of imagery and sensor data.

The result is a dramatic increase in global visibility. Military deployments, infrastructure construction, maritime activity, and even economic indicators are becoming progressively more observable. Activities that once occurred beyond public view can now be monitored by governments, private companies, research institutions, and independent analysts.

This shift is fundamentally altering strategic behaviour. The challenge for governments is no longer merely acquiring information. Increasingly, the challenge lies in operating effectively within an environment where others can acquire information as well. Strategic surprise becomes more difficult. Concealment becomes more complex. Decision cycles become shorter.

In many respects, the future security environment may be characterised not by information scarcity, but by information abundance.

Geography Is Evolving, Not Disappearing

It would be premature to conclude that geography no longer matters. The Indo-Pacific remains oneof the world's most strategically important regions because of its maritime routes, economic significance, and concentration of military power. The Arctic is gaining importance because of changing environmental conditions and emerging transportation corridors. Energy infrastructure, manufacturing hubs, ports, and population centres remain rooted in physical locations.

Geography continues to shape opportunity and vulnerability. What is changing is the way geography is understood and managed. Space has introduced a new layer of strategic infrastructure that sits above traditional geographic realities. Nations now compete not only for territory and resources, but also for access to information, communications, navigation, and awareness. These capabilities increasingly determine how effectively geography can be leveraged, protected, or overcome.
In this sense, geography is not disappearing. It is being supplemented by a new domain of strategic competition. The nations that succeed in the coming decades will not necessarily be those occupying the most advantageous geographic positions. They will increasingly be those capable of integrating terrestrial and orbital infrastructure into coherent systems of power and influence.

This marks the beginning of a broader transformation in international affairs. If the industrial age was defined by control over territory and resources, the space age is increasingly being defined by control over information and awareness. Geography may still shape the battlefield, but data is rapidly becoming the resource that determines who understands it first, who acts upon it fastest, and who ultimately gains advantage from it.

The strategic competition of the twenty-first century is therefore not simply about where nations are located. It is increasingly about what they can see, what they can know, and how quickly they can act upon that knowledge.



The New Currency of Power: Data, Awareness and Information Dominance

If geography shaped power during the industrial era, awareness is increasingly shaping power in the space age. The strategic value of space is often discussed in terms of launch vehicles, satellite constellations, communications systems, or navigation architectures. Yet these capabilities are merely the infrastructure layer. Their true value lies in the information they generate and the awareness they create. In an increasingly complex and interconnected world, the ability to observe developments, reduce uncertainty, anticipate change, and make informed decisions is becoming a defining source of national advantage.

This represents a significant shift in the nature of power. Historically, strategic advantage was often linked to physical assets—territory, military forces, industrial capacity, or natural resources. Today, advantage increasingly stems from the ability to generate actionable awareness across economic, environmental, technological, and security domains. Space systems have become indispensable because they provide persistent visibility at national, regional, and global scales.

The implications extend far beyond defence and security. Governments rely on space-derived information for disaster management, infrastructure planning, resource management, and climate monitoring. Businesses use geospatial intelligence to assess supply chains, monitor economic activity, and manage risk. Financial institutions increasingly incorporate Earth observation data into decision-making processes. In each case, the strategic value is not the satellite itself but the insight derived from the information it produces.

A second transformation is also underway. The competition is no longer centred on access to data alone. Information has become abundant. What increasingly matters is the ability to integrate multiple sources of information, extract meaningful insights, and translate those insights into decisions faster than competitors. The convergence of space systems, artificial intelligence, cloud computing, and advanced analytics is therefore creating a new hierarchy of advantage based on decision superiority rather than information ownership alone.

This shift is influencing how nations approach space capability development. The objective is no longer simply to place assets in orbit. It is to build integrated information architectures that connect satellites, communications networks, analytical platforms, and decision-making systems into coherent ecosystems.

Those ecosystems increasingly shape economic competitiveness, national resilience, and strategic influence.

For emerging space powers, this

evolution creates both opportunities and challenges. Access to space-derived information is becoming more democratised, lowering traditional barriers to participation. At the same time, competition is intensifying around the infrastructure, standards, and ecosystems through which information is generated and distributed. The result is a new form of strategic competition centred not merely on technology, but on awareness itself.

The growing importance of awareness is also reshaping international alignments. Nations are increasingly investing in sovereign capabilities, trusted partnerships, and interoperable architectures to ensure access to critical information during periods of uncertainty or crisis. As a result, the competition for influence is gradually expanding beyond satellites and launch systems to encompass the broader ecosystems that generate, process, and secure information.

This raises a larger geopolitical question. If awareness is becoming the new currency of power, who controls the infrastructures that generate it? The answer is increasingly found in the emergence of competing space ecosystems and strategic blocs that are reshaping the global balance of power.

The Great Space Blocs

The growing importance of space has introduced a new dimension to international competition. While earlier eras were characterised by contests over territory, resources, industrial capacity, and military power, the emerging space age is increasingly witnessing competition between strategic ecosystems. These ecosystems are not defined solely by satellites or launch vehicles. They comprise integrated architectures that combine communications, navigation, Earth observation, data infrastructure, industrial capabilities, regulatory frameworks, and international partnerships.

The significance of these architectures lies in their ability to generate influence. Nations that establish widely adopted technological systems often shape standards, dependencies, and patterns of cooperation far beyond their borders. In this respect, space infrastructure is becoming an instrument of geopolitical influence in much the same way that maritime trade routes, energy networks, and telecommunications systems shaped previous eras of international power.

A defining feature of the current landscape is the emergence of distinct approaches to space power. The United States continues to lead through a highly integrated ecosystem that combines government capabilities, private sector innovation, defence requirements, and global partnerships. This model has enabled the rapid expansion of launch capacity, communications networks, Earth observation capabilities, and emerging space services. More importantly, it has created an ecosystem that many partners and allies naturally integrate with, reinforcing its global reach and influence.

China has pursued a different path. Over the past two decades, Beijing has systematically developed an end-to-end space ecosystem encompassing launch systems, navigation services, communications architectures, Earth observation capabilities, and human spaceflight programmes.

The growing importance of space has introduced a new dimension to international competition. While earlier eras were characterised by contests over territory, resources, industrial capacity, and military power, the emerging space age is increasingly witnessing competition between strategic ecosystems. These ecosystems are not defined solely by satellites or launch vehicles. They comprise integrated architectures that combine communications, navigation, Earth observation, data infrastructure, industrial capabilities, regulatory frameworks, and international partnerships.

unications networks, Earth observation capabilitions architectures, Earth observation capabilities, and human spaceflight programmes.

The Rise of Infrastructure Diplomacy

A less visible but equally significant development is the growing role of infrastructure diplomacy. Historically, diplomatic influence was exercised through political agreements, economic assistance, trade relationships, and security arrangements. Today, influence is increasingly generated through the provision of technological infrastructure. Communications systems, navigation services, Earth observation capabilities, and digital platforms are becoming mechanisms through which nations build long-term relationships and strategic relevance.

S

pace plays a central role in this evolution because many emerging economies view space-enabled services as essential tools for development. Connectivity, disaster management, agricultural monitoring, climate resilience, maritime awareness, and infrastructure planning increasingly depend upon access to reliable space capabilities. Nations capable of providing such capabilities are therefore able to create enduring partnerships that extend beyond traditional diplomatic engagement.

This dynamic is particularly evident across the Global South, where demand for practical space applications is growing rapidly. For many countries, the value of space lies not in prestige or exploration, but in its ability to address developmental challenges and improve economic resilience. As a result, access to space-enabled infrastructure is becoming an increasingly important component of international cooperation.

Beyond Competition: The Search for Strategic Balance

The emergence of competing space ecosystems also presents a challenge for middle powers and emerging space nations. Few countries possess the resources required to replicate every element of a comprehensive space architecture. Most must therefore navigate a complex landscape of partnerships, dependencies, and strategic choices.

This reality is encouraging a search for balance. Nations increasingly seek diversified partnerships, interoperable systems, and trusted collaborations that reduce vulnerability while preserving flexibility. Strategic autonomy is no longer understood as complete self-sufficiency. Instead, it is increasingly viewed as the ability to participate in global ecosystems without becoming excessively dependent upon any single architecture.

This perspective is particularly relevant for countries such as India. As one of the world's leading spacefaring nations and an increasingly important actor within the global space economy, India occupies a unique position. It engages with advanced space powers, contributes to international initiatives, supports capacity-building across the Global South, and maintains a growing commercial ecosystem. This combination provides opportunities to shape partnerships that are not based on dependence, but on mutual capability enhancement and shared strategic interests.

The emerging space order is therefore not simply a story of competition between major powers. It is equally a story about how nations position themselves within a landscape of evolving architectures, partnerships, and technological ecosystems. The decisions taken today regarding infrastructure, standards, industrial collaboration, and strategic partnerships are likely to influence patterns of power and influence for decades to come.

The most visible manifestation of this competition is unfolding in the Indo-Pacific, where maritime security, economic connectivity, technological rivalry, and strategic influence increasingly intersect with space capabilities. It is here that many of the defining features of the emerging space order are becoming most apparent.



The Indo-Pacific Space Chessboard

Strategic Competition Above the Maritime Domain

The Indo-Pacific has emerged as the centre of gravity of twenty-first-century geopolitics. Home to more than half of the world's population, some of its fastest-growing economies, and the most critical maritime trade corridors, the region increasingly shapes global discussions on security, technology, economic resilience, and strategic influence. Yet beneath the visible competition unfolding across sea lanes, ports, supply chains, and military deployments lies another contest that receives far less attention. The future balance of power in the Indo-Pacific is increasingly being influenced by what happens above the Earth rather than solely upon it.

Space has become the invisible layer connecting the region's economic and security architecture. Navigation systems support the movement of commercial shipping and military platforms. Earth observation satellites provide visibility across vast maritime spaces. Satellite communications enable connectivity across remote islands, oceans, and regions where terrestrial infrastructure remains limited. Weather monitoring systems support disaster preparedness, while positioning and timing services underpin transportation networks, financial systems, and digital infrastructure. As a result, many of the activities that sustain the Indo-Pacific's economic vitality and security stability increasingly depend upon assets operating in orbit.

This dependence is particularly significant because of the geographic realities of the region. Unlike continental theatres where physical infrastructure can often provide continuity and redundancy, the Indo-Pacific is characterised by enormous distances, dispersed island chains, extensive coastlines, and vast maritime spaces. Monitoring, securing, and managing these environments requires persistent visibility that conventional terrestrial systems alone cannot provide. Space therefore serves as a strategic equaliser, allowing nations to extend awareness far beyond their immediate physical reach.

Maritime Power in the Age of Persistent Awareness

For centuries, maritime power was measured through the ability to control sea lanes, deploy naval assets, and protect commercial routes. While these capabilities remain important, the nature of maritime power is evolving. Increasingly, advantage derives from awareness rather than presence alone.

The ability to track vessel movements, monitor fishing activity, identify anomalous behaviour, assess infrastructure development, and detect emerging threats has become a critical component of regional security. Space-based systems provide the persistent awareness necessary to perform these functions at scale. In many respects, maritime competition is shifting from controlling oceans to understanding them.

This transformation is particularly relevant in an era marked by increasing congestion, contested maritime claims, grey-zone activities, illegal fishing, and growing competition for resources.Nations that possess superior awareness are often better positioned to protect their interests, respond to crises, and shape events before they escalate. The result is a gradual transition from platform-centric security to information-centric security, where the ability to see, understand, and anticipate developments becomes as important as the ability to respond militarily.

The Strategic Convergence of Space and Regional Security

The growing role of space in the Indo-Pacific is also altering how regional security is conceived. Traditional security arrangements focused largely on military capabilities, defence partnerships, and deterrence. While these remain essential, an increasing number of challenges confronting the region do not fit neatly within conventional security frameworks.

Climate-related disasters, disruptions to supply chains, humanitarian emergencies, maritime incidents, and threats to critical infrastructure all require rapid access to reliable information. They demand coordination across governments, agencies, and international partners. In each of these areas, space-enabled capabilities play a crucial role by providing a common operating picture that supports decision-making and collective action.

This has led to a subtle but important shift in strategic thinking. Security is no longer defined solely by the ability to defend territory. It increasingly encompasses the ability to maintain resilience, ensure continuity, and preserve awareness under conditions of uncertainty. Space has become central to these objectives because it provides the information infrastructure upon which resilience depends.

The Rise of Regional Space Architectures

One of the most notable developments in recent years has been the emergence of regional approaches to space cooperation. As nations recognise the shared nature of many regional challenges, there is growing interest in developing mechanisms that enable information exchange, interoperability, and collaborative use of space-derived capabilities.

These arrangements are not traditional alliances in the military sense. Rather, they represent practical architectures designed to improve awareness, strengthen resilience, and support collective problem-solving. They often focus on areas such as disaster management, maritime domain awareness, climate monitoring, and capacity building. Their significance lies not only in the capabilities they provide, but in the trust and familiarity they create among participating nations.

This trend reflects a broader evolution in international relations. In an increasingly interconnected environment, influence is generated not

merely through military strength or economic scale, but through the ability to create platforms for cooperation. Space is uniquely positioned to support such cooperation because many of its applications are inherently transnational. Weather systems, maritime activity, environmental changes, and disaster events do not respect political boundaries. Consequently, the value of space often increases when information is shared rather than retained.

India's Strategic Position in the Indo-Pacific

India occupies a distinctive position within this evolving landscape. Geographically situated at the heart of the Indian Ocean and possessing one of the world's most mature space programmes, India is uniquely placed to contribute to regional stability and resilience. Its capabilities in Earth observation, navigation, communications, disaster management, and launch services provide a strong foundation for supporting both national priorities and regional objectives.

More importantly, India's approach to space has historically emphasised practical applications, capacity building, and inclusive development. This perspective resonates strongly across the Indo-Pacific, where many countries view space not primarily as an arena of competition, but as a tool for addressing developmental challenges and strengthening resilience. By supporting access to space-enabled services, sharing expertise, and contributing to regional initiatives, India has an opportunity to play a role that extends beyond traditional notions of power projection.

The Indo-Pacific therefore offers a glimpse into the future of international affairs. It is a region where economic connectivity, strategic competition, technological ecosystems, and space infrastructure are becoming increasingly intertwined. It is also a region where the emerging logic of astro-politics is most visible. The ability to generate awareness, support resilience, and shape regional architectures may ultimately prove as important as the ability to deploy military assets or project economic influence.

As nations become more dependent on interconnected technological systems, however, a new challenge begins to emerge. Connectivity creates opportunity, but it can also create vulnerability. Dependence on external communications networks, navigation systems, digital infrastructure, or data architectures introduces risks that can be exploited during periods of tension or crisis. Understanding these vulnerabilities is essential because the next phase of strategic competition may not be defined by the ownership of infrastructure alone, but by the ability to influence those who depend upon it.



Strategic Dependencies: When Infrastructure Becomes Leverage

One of the defining characteristics of the modern world is the extent to which economies, governments, and societies depend upon interconnected technological systems. Communications networks, navigation services, digital platforms, cloud infrastructure, semiconductor supply chains, undersea cables, and satellite architectures collectively form the invisible operating system of contemporary civilisation. Their success lies precisely in their ubiquity. They are so deeply embedded within everyday activity that they are rarely noticed until they become unavailable.

Space infrastructure occupies a particularly important position within this ecosystem. Satellite communications support connectivity across remote regions and maritime spaces. Navigation systems underpin transportation networks, logistics operations, financial transactions, emergency services, and military platforms. Earth observation systems contribute to environmental management, infrastructure planning, disaster response, and strategic awareness. As societies become more digital and interconnected, dependence upon these capabilities continues to grow.

Historically, infrastructure was largely viewed as a source of economic efficiency and development. Today, it is increasingly viewed through a strategic lens. The growing reliance on interconnected systems has created a new form of vulnerability: dependence itself. Nations that rely heavily onexternal capabilities for critical functions may find that access, continuity, or reliability can become subject to geopolitical pressures, technological restrictions, or strategic competition.

This reality has become particularly evident in recent years. Global disruptions to semiconductor supply chains demonstrated how concentrated production capabilities can create vulnerabilities across entire industries. Debates surrounding telecommunications infrastructure highlighted concerns regarding technological dependence and strategic autonomy. Similar concerns are increasingly emerging within the space sector, where navigation systems, communications architectures, launch capabilities, and data ecosystems are becoming integral to national resilience.

The significance of these dependencies extends beyond economics. Modern military operations rely heavily upon positioning, navigation, timing, communications, and intelligence systems that are increasingly space-enabled. Critical infrastructure networks often depend upon satellite-derived timing signals. Financial systems require precise synchronisation to execute transactions. Logistics networks rely on continuous navigation services to manage the movement of goods and services. The disruption of such capabilities, whether through technical failure, cyberattack, political restrictions, or con-

One of the defining characteristics of the modern world is the extent to which economies, governments, and societies depend upon interconnected technological systems. Communications networks, navigation services, digital platforms, cloud infrastructure, semiconductor supply chains, undersea cables, and satellite architectures collectively form the invisible operating system of contemporary civilisation. Their success lies precisely in their ubiquity. They are so deeply embedded within everyday activity that they are rarely noticed until they become unavailable.

Space infrastructure occupies a particularly important position within this ecosystem. Satellite communications support connectivity across remote regions and maritime spaces. Navigation systems underpin transportation networks, logistics operations, financial transactions, emergency services, and military platforms. Earth observation systems contribute to environmental management, infrastructure planning, disaster response, and strategic awareness. As societies become more digital and interconnected, dependence upon these capabilities continues to grow.

Historically, infrastructure was largely viewed as a source of economic efficiency and development. Today, it is increasingly viewed through a strategic lens. The growing reliance on interconnected systems has created a new form of vulnerability: dependence itself. Nations that rely heavily onexternal capabilities for critical functions may find that access, continuity, or reliability can become subject to geopolitical pressures, technological restrictions, or strategic competition.

This reality has become particularly evident in recent years. Global disruptions to semiconductor supply chains demonstrated how concentrated production capabilities can create vulnerabilities across entire industries. Debates surrounding telecommunications infrastructure highlighted concerns regarding technological dependence and strategic autonomy. Similar concerns are increasingly emerging within the space sector, where navigation systems, communications architectures, launch capabilities, and data ecosystems are becoming integral to national resilience.

The significance of these dependencies extends beyond economics. Modern military operations rely heavily upon positioning, navigation, timing, communications, and intelligence systems that are increasingly space-enabled. Critical infrastructure networks often depend upon satellite-derived timing signals. Financial systems require precise synchronisation to execute transactions. Logistics networks rely on continuous navigation services to manage the movement of goods and services. The disruption of such capabilities, whether through technical failure, cyberattack, political restrictions, or conflict, can produce consequences that extend far beyond the immediate sector involved.

This has led to a broader reassessment of resilience. The traditional approach focused primarily on protecting infrastructure from physical threats. The emerging challenge is ensuring continuity of function when access to critical systems may be uncertain. Resilience therefore increasingly depends on redundancy, diversification, interoperability, and trusted partnerships. The objective is not complete self-sufficiency, which is often unrealistic in an interconnected world, but the ability to avoid excessive dependence on any single provider, technology, or ecosystem.

For many countries, this shift is driving renewed interest in sovereign capabilities. Navigation systems, secure communications networks, Earth observation architectures, launch infrastructure, and domestic industrial capacity are increasingly viewed as strategic assets rather than purely technical capabilities. The objective is not isolation from global ecosystems but the preservation of strategic choice. Nations seek the ability to participate in international networks while retaining sufficient capability to protect their interests under adverse circumstances.



Strategic Network Blocs: The Rise of Technology-Centred Alignments

The twentieth century was defined by military alliances. NATO, the Warsaw Pact, and a range of bilateral and multilateral security arrangements shaped the geopolitical landscape through defence commitments, strategic deterrence, and collective security. While such alliances continue to play an important role in international affairs, the emerging geopolitical environment is giving rise to a different form of alignment—one that is increasingly organised around technology, infrastructure, standards, and interconnected ecosystems.

The defining feature of the twenty-first century may not be the emergence of new military blocs, but the emergence of strategic network blocs. These blocs are not necessarily established through formal treaties or security guarantees. Instead, they evolve through the adoption of common technologies, participation in shared industrial ecosystems, integration with digital infrastructure, alignment of regulatory frameworks, and dependence on interconnected architectures. Navigation systems, communications networks, cloud infrastructure, semiconductor supply chains, digital public infrastructure, Earth observation services, and increasingly space-based capabilities are becoming the foundations upon which long-term strategic relationships are built.

This transformation reflects a broader shift in the nature of influence. Historically, power was projected through military presence and economic reach. Today, influence increasingly derives from the ability to shape ecosystems. Nations that provide trusted infrastructure, establish widely adopted standards, and occupy central positions within technology networks often acquire strategic relevance that extends far beyond their geographic boundaries.

Space is becoming an important element of this transformation because it sits at the intersection of multiple strategic systems. Satellite communications support digital connectivity. Navigation systems underpin transportation, logistics, and economic activity. Earth observation capabilities support agriculture, environmental management, maritime awareness, and national security. As countries adopt and integrate these capabilities, they become connected to larger ecosystems that influence how information is generated, shared, and utilised.

From Security Partnerships to Ecosystem Partnerships

One of the most significant geopolitical developments of recent years has been the growing recognition that resilience cannot be achieved solely through military cooperation. Increasingly, resilience depends upon access to trusted technologies, diversified supply chains, interoperable systems, and reliable infrastructure.

This has expanded the scope of strategic partnerships. Relationships that were once focused primarily on defence cooperation are now increasingly encompassing industrial collaboration, technology development, digital infrastructure, innovation ecosystems, and space capabilities. The objective is not simply to enhance military preparedness but to strengthen the broader foundations upon which economic competitiveness and national resilience depend.

The evolution of Europe's approach to technological sovereignty reflects this trend. Concerns regarding excessive dependence in critical sectors have encouraged greater emphasis on indigenous capability development, industrial resilience, and trusted partnerships. Similar discussions are occurring across the Indo-Pacific, where governments are seeking to balance openness and cooperation with the need to preserve strategic flexibility.

The result is a new model of partnership in which technology ecosystems play a role traditionally associated with security arrangements. Countries are increasingly assessing not only who their allies are, but also which infrastructures they depend upon, which standards they adopt, and which ecosystems they integrate with.

The Competition for Standards and Architectures

An important but often overlooked dimension of strategic competition concerns standards. Throughout history, standards have shaped markets, influenced industrial development, and created spheres of influence. Railway gauges, telecommunications protocols, internet architectures, and financial systems all demonstrate how technical standards can generate long-term strategic effects. The space sector is increasingly entering a similar phase.

Navigation systems, satellite communications architectures, data-sharing frameworks, cybersecurity protocols, space traffic management practices, and emerging lunar governance mechanisms are all becoming subjects of international engagement. The countries and institutions that help shape these frameworks often influence the direction of markets, investment flows, industrial partnerships, and technological development.

This is particularly significant because the next phase of space growth is expected to be increasingly international and commercial. As more countries and private actors participate in the space economy, questions relating to interoperability, standards, governance, and trusted architectures will become increasingly important. Strategic influence will therefore depend not only on capability, but also on the ability to shape the rules and frameworks through which capabilities interact.t



Europe's Strategic Dilemma

The rapid evolution of the global space economy is creating opportunities for unprecedented collaboration. International partnerships are expanding, commercial actors are transforming innovation cycles, and technological ecosystems are becoming increasingly interconnected. Yet this growing interdependence has also exposed a fundamental strategic question confronting governments across the world: how can nations remain open to cooperation while preserving their ability to act independently when required?

This challenge is particularly visible in Europe, where the pursuit of strategic autonomy has emerged as a central policy objective over the past decade. While the concept extends across defence, technology, energy, and industrial policy, it has acquired particular significance within the space sector. European policymakers increasingly recognise that access to independent navigation systems, Earth observation capabilities, secure communications networks, and launch infrastructure is not merely a matter of technological capability; it is a matter of strategic freedom.

At its core, the debate is not about self-sufficiency. Complete technological independence is neither realistic nor desirable in an interconnected world. Modern innovation depends upon global collaboration, international markets, and cross-border partnerships. The challenge instead is preserving freedom of action in an environment where critical systems are becoming increasingly interconnected and dependencies are becoming increasingly complex.

The Pursuit of Strategic Sovereignty

The European experience illustrates how technological capability and geopolitical influence have become closely intertwined. Navigation systems, communications architectures, Earth observation programmes, and secure digital infrastructure are no longer viewed solely as economic assets. They are increasingly regarded as strategic enablers that support resilience, decision-making, and long-term competitiveness.

This perspective has gained prominence as geopolitical competition has intensified and technological dependencies have become more visible. The question facing policymakers is no longer whether global cooperation should continue, but how to ensure that cooperation does not result in excessive vulnerability. The answer has increasingly been sought through investments in sovereign capabilities, diversified partnerships, and trusted industrial ecosystems.What makes this development particularly significant is that it reflects a broader shift in strategic thinking. For much of the post-Cold War period, efficiency was often prioritised over resilience. Globalisation encouraged specialisation, integration, and optimisation. Today, resilience has emerged as an equally important objective.

From Strategic Autonomy to Strategic Partnerships

An interesting paradox has emerged from this pursuit of sovereignty. The more nations seek strategic autonomy, the more they often recognise the importance of trusted partnerships.
The objective is not isolation. Rather, it is the creation of relationships that enhance resilience while preserving flexibility. This distinction is important because it challenges the traditional assumption that sovereignty and cooperation are competing objectives. In reality, the most effective forms of sovereignty increasingly depend upon the quality of partnerships that nations are able to cultivate.

This is particularly evident in the evolving relationship between Europe and India. Both are major democratic actors, both are investing in advanced technological capabilities, and both share an interest in maintaining open, secure, and rules-based access to critical domains. Their cooperation increasingly extends beyond traditional commercial engagement into areas such as industrial collaboration, emerging technologies, supply-chain resilience, secure communications, Earth observation applications, and innovation ecosystems.

The significance of such partnerships lies not only in the capabilities they generate but also in the strategic options they create. In a world characterised by competing technological ecosystems and growing geopolitical uncertainty, trusted partnerships provide diversification, reduce concentration risks, and strengthen resilience.

Lessons for an Emerging Space Order

The European experience offers a broader lesson for the international space community. The future of space development is unlikely to be defined by a simple choice between globalisation and self-reliance. Instead, it will be shaped by the ability to balance openness with resilience, collaboration with autonomy, and innovation with security.

This balance is becoming increasingly important as space transitions from a specialised domain into a foundational layer of economic and strategic activity. Countries are no longer evaluating space programmes solely in terms of scientific achievement or national prestige. They are increasingly assessing how space capabilities contribute to economic competitiveness, industrial development, technological leadership, and national resilience.

For emerging space powers, the challenge is therefore not simply to build capabilities. It is to build ecosystems. The countries that succeed will be those capable of combining domestic strengths with international partnerships, creating networks that are both globally connected and strategically resilient.

In many respects, Europe's experience represents an early example of a challenge that is likely to confront an increasing number of nations in the years ahead. As competition intensifies around technology, infrastructure, and information architectures, strategic sovereignty will become less about independence from others and more about the ability to engage with others from a position of strength.

For India, this transition presents a particularly significant opportunity. Positioned at the intersection of major geopolitical, economic, and technological networks, India is uniquely placed to shape the next phase of international space cooperation. The question is no longer whether India will participate in the emerging space order, but what role it will play in defining it.



India and the Architecture of the Next Space Order

Throughout much of the space age, the international space ecosystem was shaped by a relatively small number of major powers. The strategic contest revolved around access to technology, launch capability, satellite infrastructure, and scientific achievement. Most countries participated as users of space-enabled services rather than architects of the systems that produced them. The coming decades, however, may witness a different reality.

As space becomes embedded within economic systems, digital infrastructure, national security architectures, climate resilience frameworks, and industrial development strategies, the question facing many nations is no longer how to access space. The more important question is who will shape the rules, institutions, partnerships, and operating principles of the emerging space economy.

This distinction is important because history demonstrates that influence is rarely determined solely by technological capability. Nations that shape standards, establish frameworks, create institutions, and build ecosystems often exert influence disproportionate to their material power. The most enduring forms of leadership are frequently exercised not through dominance, but through the ability to organise cooperation around shared interests and common objectives. The international space sector is approaching precisely such a moment. Over the next two decades, hundreds of billions of dollars are expected to flow into space-enabled services, commercial infrastructure, communications systems, Earth observation applications, in-space operations, navigation architectures, and emerging lunar activities. At the same time, an increasing number of countries are entering the space domain. Many of these nations are not seeking prestige-driven programmes. They are seeking practical solutions for connectivity, disaster management, agriculture, climate resilience, urban planning, maritime governance, and economic development.

This creates an important governance challenge. The institutions, standards, and cooperation mechanisms that shaped the early space age were designed for a relatively small group of advanced spacefaring nations. The emerging space economy is far more diverse, commercially driven, and globally distributed. It requires new approaches to collaboration, capacity building, technology sharing, and market development.

This is where India occupies a uniquely advantageous position. Unlike many established space powers, India's space journey has been deeply connected to developmental objectives. Communications, remote sensing, weather forecasting,

disaster management, education, healthcare delivery, and rural connectivity have long formed central pillars of India's space programme. As a result, India possesses practical experience in applying space technologies to large-scale societal and developmental challenges. This perspective aligns closely with the priorities of many emerging economies that increasingly view space as an enabler of development rather than solely a domain of strategic competition.

At the same time, India possesses characteristics that allow it to engage simultaneously with multiple geopolitical and economic groupings. It maintains strong relationships with advanced space powers, plays an influential role within the Indo-Pacific, participates actively in multilateral institutions, and enjoys considerable credibility across the Global South. Few countries are positioned at the intersection of so many strategic networks.

The significance of this position extends beyond diplomacy. The future space economy will require trusted intermediaries capable of connecting industrial ecosystems, facilitating technology partnerships, supporting capacity-building efforts, and enabling broader participation in space-enabled development. Countries that can perform these functions will play an important role in shaping how the benefits of space are distributed and how future governance frameworks evolve.

The opportunity for India, therefore, is not merely to become a larger space power. Many nations are pursuing that objective. The more significant opportunity lies in helping shape the architecture of the next space order itself. This architecture will not be defined solely by launch capacity, satellite numbers, or defence capabilities. It will increasingly be shaped by standards, interoperability frameworks, industrial partnerships, digital ecosystems, talent networks, regulatory models, and cooperative platforms. Nations capable of influencing these foundational layers will help determine how future space markets operate and how international collaboration evolves.

Perhaps the most important strategic question is whether the future space order becomes fragmented into competing technological spheres or evolves into a more interconnected ecosystem characterised by interoperability and shared benefit. The answer will influence not only commercial opportunities, but also the accessibility of space-enabled services for billions of people. India is one of the few countries capable of contributing meaningfully to that outcome. Its experience as both a major spacefaring nation and a development-oriented space actor provides a perspective that is increasingly relevant in a world where the benefits of space must extend beyond traditional power centres.

The next phase of space leadership may therefore look very different from the last. It may be defined less by competition for dominance and more by the ability to shape institutions, connect ecosystems, and expand participation. In such an environment, influence will derive not only from what a nation builds for itself, but from the systems it helps others access and the opportunities it enables for the broader international community.

India's greatest opportunity in the coming decades may therefore not be to emerge as another major power within the existing space order. It may be to help define what the next space order looks like.



Conclusion: The Coming Age of Astro-Politics

The international system is entering a period of transition in which space is no longer a supporting domain of national power but an increasingly central determinant of it. The significance of this shift lies not merely in the growing number of satellites in orbit or the expansion of commercial space activity. Its deeper importance stems from the fact that space now underpins many of the systems upon which modern economies, security architectures, and societies depend.

This transformation is reshaping traditional assumptions about power. Geography remains important, but awareness increasingly shapes outcomes. Infrastructure remains important, but the ability to influence the networks that connect infrastructure is becoming equally significant. Capability remains important, but resilience increasingly depends upon access to trusted ecosystems rather than isolated national assets.

The result is the emergence of a more complex strategic environment in which influence flows through interconnected architectures of communications, navigation, Earth observation, digital infrastructure, and industrial ecosystems. The countries that occupy central positions within these architectures are likely to possess advantages that extendbeyond conventional measures of military or economic strength.
The Indo-Pacific provides an early glimpse of this future. It is a region where maritime competition, technological rivalry, economic interdependence, and space-enabled capabilities increasingly intersect. It demonstrates that strategic competition is no longer confined to land, sea, air, or even space as individual domains. Instead, competition increasingly occurs across integrated systems that connect multiple domains simultaneously.

At the same time, the pursuit of technological sovereignty by major actors illustrates another defining characteristic of the emerging era. Nations are seeking resilience not through isolation, but through acareful balance of domestic capability, trusted partnerships, and diversified ecosystems. Strategic autonomy is increasingly becoming a function of choice rather than self-sufficiency.

Within this evolving landscape, the future international order may be shaped less by traditional alliance structures and more by the networks that support connectivity, information exchange, innovation, and economic activity. Space occupies a unique position within these networks because it serves as an enabling layer for many of the critical functions that sustain modern societies. Astro-politics is therefore not a future possibility. It is an emerging reality. Understanding its dynamics will be essential to understanding the international order of the decades ahead.

Strategic Priorities for the Next Decade

- **Building Influence Through Ecosystems**

The next phase of competition in space is unlikely to be determined solely by individual missions, satellite deployments, or launch capabilities. Influence will increasingly flow through ecosystems that connect industry, technology, infrastructure, talent, and international partnerships. Nations that successfully create and participate in such ecosystems will be better positioned to shape standards, attract investment, and influence the direction of future space markets. The strategic challenge is therefore not only to build capabilities, but to build enduring networks of collaboration and innovation.

- **Strengthening Strategic Resilience**

As economies become more dependent on space-enabled services, resilience will emerge as a defining strategic requirement. Navigation systems, communications networks, Earth observation capabilities, and digital infrastructure are becoming critical enablers of economic activity and national security. The coming decade will require greater emphasis on redundancy, interoperability, supply-chain security, and trusted partnerships to ensure continuity in an increasingly uncertain geopolitical environment.

- **Shaping the Rules of the Emerging Space Economy**

The future space economy will be influenced as much by governance frameworks and standards as by technology itself. Questions relating to interoperability, data governance, space traffic management, spectrum coordination, lunar activities, and commercial participation are likely to become increasingly important. Countries that contribute to the development of these frameworks will possess an opportunity to shape the operating environment of the next generation of space activity.

- **Expanding Space as an Instrument of Development**

For much of the world, the significance of space lies not in prestige but in practical impact. Connectivity, climate resilience, disaster management, agriculture, maritime governance, and infrastructure planning will continue to drive demand for space-enabled services. Expanding access to these applications will remain essential to ensuring that the benefits of the space economy extend beyond traditional spacefaring nations and contribute to broader developmental objectives.

- **Advancing Trusted International Partnerships**

The future international space ecosystem will be characterised by a complex balance between competition and cooperation. Strategic autonomy and international collaboration are no longer opposing concepts; increasingly, they reinforce one another. Trusted partnerships will play an important role in supporting innovation, reducing vulnerabilities, diversifying supply chains, and strengthening resilience. The countries that successfully combine sovereign capability with international engagement will be best positioned to navigate the evolving geopolitical landscape.

- **Positioning India as a System-Shaping Space Power**

India enters the next decade with a unique combination of capabilities, partnerships, and strategic relationships. Its growing industrial base, expanding commercial ecosystem, developmental approach to space applications, and increasing global engagement create opportunities that extend beyond capability development alone. The more significant opportunity lies in helping shape the institutions, partnerships, and frameworks that will define the next phase of the global space economy. India's long-term influence may ultimately be measured not only by what it builds, but by the role it plays in shaping the architecture of the emerging space order.



BUILDING INDIA'S DEFENCE SPACE INDUSTRIAL ECOSYSTEM

Introduction: The Industrial Foundations of Space Power

The global space sector is undergoing one of the most profound transformations since the dawn of the Space Age. For much of the twentieth century, space capability was viewed primarily through the lens of national programmes, technological milestones, and strategic achievements. Success was measured by launch vehicles, satellites, planetary missions, and scientific breakthroughs. Governments were the principal architects, operators, and consumers of space capability, while industry largely functioned as a supporting partner within state-led programmes.

That model is rapidly evolving. Space is no longer confined to a specialised sector of scientific or strategic activity. It has become an enabling layer for economic growth, digital infrastructure, national security, disaster management, communications, navigation, and global commerce. As dependence on space-enabled services expands, the determinants of space power are also changing.

The ability to launch a satellite or develop a mission remains important, but these capabilities alone no longer define leadership. Increasingly, space power is determined by the capacity to innovate continuously, manufacture at scale, mobilise capital, secure supply chains, integrate commercial capabilities, and sustain technological advantage over long periods of strategic competition.

This shift reflects a broader transformation in the nature of national power itself. Modern military effectiveness, economic competitiveness, and technological leadership increasingly depend on ecosystems rather than institutions. The world's leading space powers are no longer building isolated programmes; they are cultivating integrated industrial architectures that combine government demand, commercial innovation, private capital, advanced manufacturing, software capabilities, academia, and defence requirements into a unified capability framework.

Recent global developments have reinforced this reality. The emergence of large-scale commercial satellite constellations, responsive launch systems, dual-use technologies, and data-driven business models has fundamentally altered the economics of space. At the same time, contemporary conflicts have demonstrated that industrial responsiveness, supply-chain resilience, and the ability to replenish capability can be as important as the capability itself.

capability can be as important as the capability itself. Space resilience is no longer simply an operational challenge; it is increasingly an industrial challenge.

For India, this transformation arrives at a pivotal moment. Over the past decades, the country has built one of the world's most respected space programmes, developed sovereign launch and satellite capabilities, established critical national infrastructure in orbit, and emerged as an increasingly important participant in the global space economy. Yet the demands of the next decade will be fundamentally different from those of the last.

F

uture space power will not be measured solely by missions completed or satellites launched. It will increasingly be measured by the strength of the ecosystem that supports them. The ability to convert research into products, innovation into deployment, startups into enterprises, and industrial capacity into strategic capability will determine whether India can transition from being a successful spacefaring nation to becoming a sustained space power.

The central challenge is therefore no longer capability creation alone. It is capacity creation. It is the ability to build an ecosystem capable of continuously generating, deploying, scaling, and sustaining space capability at national scale. This chapter examines the emergence of that ecosystem and explores how India can build the industrial foundations required to support its long-term defence and space ambitions.



Beyond the State-Centric Space Model

ThThe traditional model of space development was built around a relatively simple structure. Governments funded programmes, national agencies developed technologies, defence establishments defined requirements, and industry executed contracts. This approach proved highly effective during the early decades of the space age when missions were expensive, technologically complex, and largely restricted to a handful of advanced nations.

The contemporary space sector operates under fundamentally different conditions. Technological barriers are falling, commercial participation is expanding, software is becoming as important as hardware, and innovation cycles are accelerating. The result is a transition from programme-centric space development to ecosystem-centric space development.

The world's most successful space powers increasingly rely on a model that integrates government institutions, defence organisations, private industry, startups, academia, investors, digital infrastructure providers, and advanced manufacturing networks into a single capability ecosystem. Competitive advantage emerges not from any individual participant but from the strength of the interactions between them.

This trend is particularly visible in the United States, where government demand, defence requirements, commercial innovation, and private investment have combined to create one of the most dynamic space ecosystems in history. Commercial companies now play a central role in launch services, communications infrastructure, Earth observation, space-based intelligence, and national security architectures. The distinction between commercial capability and strategic capability is becoming progressively blurred.

A similar lesson is emerging from contemporary conflict environments. Modern military operations increasingly depend upon commercial communications networks, satellite imagery, cloud computing, geospatial analytics, and dual-use technologies developed outside traditional defence procurement systems. The implication is significant: future military capability will increasingly originate from broader industrial ecosystems rather than defence establishments alone.

For India, this represents both an opportunity and a strategic necessity. The scale and complexity of future space architectures make it increasingly difficult for any single institution to independently develop, manufacture, operate, and sustain all required capabilities. Constellations comprising hundreds of satellites, space-based intelligence networks, secure communications architectures, autonomous systems, artificial intelligence-enabled analytics, and resilient supply chains require

participation from a far wider ecosystem than traditional government programmes were designed to support.

The emergence of India's private space sector, the creation of IN-SPACe, growing venture investment, expanding startup activity, and increasing defence-space collaboration collectively signal the beginning of this transition. However, the objective should not simply be the creation of more companies or the expansion of commercial activity. The larger objective is the creation of a Military–Industrial–Space Ecosystem capable of supporting national requirements across the full spectrum of competition, crisis, and conflict.

Such an ecosystem must perform several functions simultaneously. It must generate innovation through research and entrepreneurship. It must convert innovation into deployable capability through manufacturing and engineering. It must provide resilience through diversified supply chains and industrial depth. Most importantly, it must possess the capacity to scale rapidly when strategic conditions demand it.

This distinction is critical. Industrial capability is often measured by what can be built during peacetime. Strategic capacity is measured by what can be sustained during periods of disruption, competition, and conflict. As space becomes increasingly integrated into national security architectures, this capacity will become a defining measure of national power.

The future of India's defence-space ambitions will therefore depend not only on what is launched into orbit, but on the ecosystem that exists on the ground to design, build, replenish, upgrade, and sustain those capabilities. The transition from a state-centric model to an ecosystem-centric model is not merely an industrial evolution. It is a strategic imperative.

From Research to Readiness: The Triple Helix of Innovation

One of the most persistent misconceptions in discussions surrounding India's defence and space sectors is the belief that the country's primary challenge is innovation. In reality, India possesses no shortage of scientific talent, engineering capability, research institutions, or entrepreneurial ambition. The country produces one of the world's largest pools of STEM graduates, hosts globally competitive technology companies, and has demonstrated the ability to execute complex missions across space, defence, nuclear energy, and digital infrastructure. The challenge lies elsewhere. It lies in the transition from innovation to deployment.

Across the world, technological leadership is increasingly determined not by the number of ideas generated, but by the ability to transform those ideas into products, platforms, and operational capabilities. The gap between laboratory success and market adoption remains one of the most difficult challenges in technology ecosystems. In the defence-space sector, where development cycles are long, certification requirements are demanding, and customers are limited, this challenge becomes even more pronounced.

Historically, India's innovation architecture evolved in silos. Universities generated research. National laboratories developed technologies. Industry focused on manufacturing and services. Defence users operated largely at the end of the chain. While each component contributed independently, the interaction between them remained limited. As a result, promising technologies often struggled to cross what innovation economists describe as the "valley of death"—the stage between prototype development and operational deployment where many innovations fail despite their technical merit.

The countries that have successfully addressed this challenge have generally adopted a different model. Instead of treating academia, industry, and government as separate entities, they have created highly integrated innovation ecosystems in which all three operate as interconnected partners. This framework is often described as the Triple Helix Model, where universities generate knowledge, industry commercializes innovation, and government acts as both enabler and strategic customer.

The United States provides perhaps the most mature example of this approach. Many of the technologies that define modern military and commercial space capability—including satellite navigation, reusable launch systems, advanced materials, autonomous systems, and artificial intelligence—emerged through decades of collaboration between universities, government-funded research institutions, defence agencies, and private industry. Organizations such as DARPA became effective not because they funded research alone, but because they connected researchers, manufacturers, investors, and end users within a common innovation ecosystem.

China has adopted a different but equally integrated approach. Through its Military-Civil Fusion strategy, technological advances in commercial sectors are systematically leveraged for national strategic objectives. Universities, research institutions, private firms, and state-owned enterprises operate within a framework designed to accelerate the transition of technology from research to deployment. The result is a development cycle that increasingly emphasizes scale, speed, and industrialization rather than isolated technological breakthroughs.

For India, the implications are significant. The country's future competitiveness will depend less on its ability to generate research and more on its ability to institutionalize pathways that convert research into capability. The emergence of IN-SPACe, technology transfer initiatives, industry access to testing facilities, startup-focused programmes, and collaborative innovation mechanisms represent important steps in this direction. These initiatives recognize that infrastructure, expertise, and institutional support are often as important as funding itself.

From Infrastructure Access to Innovation Access

A critical lesson emerging from successful space ecosystems worldwide is that innovation rarely occurs in isolation. Startups and emerging enterprises often fail not because they lack technical competence, but because they lack access—to laboratories, testing facilities, manufacturing infrastructure, customers, data, mentors, and capital.

In the space sector, access barriers can be particularly severe. Satellite testing facilities, environmental qualification infrastructure, launch opportunities, advanced manufacturing systems, and mission validation environments require substantial investment. No startup ecosystem can independently replicate such capabilities at scale. Consequently, the countries that have accelerated innovation most effectively are those that have democratized access to national infrastructure.

India's ongoing efforts to open testing facilities, expand industry participation, and facilitate greater interaction between government institutions and private enterprises should therefore be viewed not merely as administrative reforms, but as strategic interventions. They reduce barriers to entry, lower development costs, shorten innovation cycles, and allow a broader range of participants to contribute to national capability development.



Demand as Industrial Policy: Fixing the Innovation-to-Induction Gap

For decades, discussions on defence industrial development have focused primarily on supply-side interventions. Governments have funded research programmes, established laboratories, created incubators, supported startups, opened testing facilities, and launched innovation initiatives. While these measures remain essential, they address only one side of the equation. Innovation ecosystems do not flourish solely because technologies are created. They flourish because markets exist to absorb them.

This distinction is particularly important in the defence-space sector, where governments often serve as the primary customer. Unlike consumer technology markets, where products can be validated through commercial demand, defence technologies frequently require a strategic buyer willing to assume risk during the early stages of development. The absence of such demand creates a structural challenge. Startups can develop prototypes, researchers can generate breakthroughs, and companies can demonstrate capability, but without a credible pathway to adoption, innovation struggles to transition into sustainable industrial activity.

This phenomenon is often described as the innovation-to-induction gap. It represents the space between technological feasibility and operational deployment—a stage where many promising technologies stagnate despite their potential value. In India's defence-space ecosystem, this gap remains one of the most significant barriers to industrial scale.

The challenge is particularly acute because space and defence technologies are inherently capital-intensive. Developing satellite subsystems, communications architectures, advanced sensors, propulsion technologies, autonomous systems, or space-based analytics platforms often requires years of investment before meaningful revenue is generated. Traditional venture capital models are not always aligned with such timelines. Investors typically seek predictable pathways to growth, whereas defence-space ventures often face lengthy procurement cycles, uncertain acquisition outcomes, and limited customer bases.

Consequently, the most valuable support that governments can provide is not always financial assistance. In many cases, the most powerful signal is demand.

Procurement as a Strategic Instrument

Historically, major technological ecosystems have often been built around anchor customers. The early development of the internet, satellite navigation systems, advanced semiconductors, commercial aviation, and numerous dual-use technologies was supported by governments acting as first adopters. Public procurement created markets, reduced uncertainty, and enabled private capital to participate with greater confidence.

The same principle applies to the defence-space sector.

When governments provide clear acquisition pathways, phased procurement commitments, or long-term capability roadmaps, they create confidence throughout the ecosystem. Investors gain visibility. Manufacturers can plan production. Supply chains become more willing to invest. Entrepreneurs gain confidence that successful development efforts will lead to meaningful market opportunities.

This is one of the most underappreciated dimensions of industrial policy. Demand itself becomes
a strategic tool for ecosystem development.

The significance of this principle can be observed in several global examples. Many of today's leading aerospace and technology firms were not initially built through subsidies alone. They were built because governments created reliable demand for emerging capabilities. Early procurement commitments enabled companies to attract capital, scale operations, and invest in long-term innovation. The result was the creation of industries that ultimately became globally competitive.

From Compliance to Capability

Traditional procurement systems were designed for a different era. Their primary objective was to acquire proven capabilities while minimizing risk. Such systems are well suited for purchasing mature platforms, but they often struggle to accommodate emerging technologies whose value may not yet be fully demonstrated.

This creates a paradox. The technologies most likely to deliver future strategic advantages are often the least compatible with conventional procurement approaches.

Startups and emerging enterprises frequently encounter requirements relating to financial history, production experience, qualification standards, and performance guarantees that were originally designed for established suppliers. While such requirements serve important purposes, they can inadvertently create barriers for precisely the type of innovators that governments seek to encourage.

The challenge is therefore not simply procedural. It is conceptual.Future acquisition systems must increasingly balance compliance with capability. They must preserve accountability and transparency while creating pathways through which innovative technologies can be evaluated, demonstrated, and adopted. This requires greater experimentation, phased acquisition models, rapid prototyping mechanisms, challenge-based procurement, and outcome-oriented contracting approaches.

The objective should not be to lower standards. It should be to create mechanisms that allow emerging capabilities to prove themselves.

The Strategic Importance of Predictability

Perhaps the most important requirement for ecosystem development is predictability. Industrial ecosystems thrive when participants can make long-term decisions with confidence. Manufacturing investments, workforce development, infrastructure creation, technology maturation, and supply-chain expansion all depend upon expectations regarding future demand. Uncertainty discourages investment. Predictability attracts it.

For India's defence-space sector, this suggests the importance of moving beyond project-by-project engagement toward longer-term capability roadmaps. Clear signals regarding future requirements, technology priorities, and procurement pathways can have effects far beyond the immediate acquisition itself. They influence investment decisions, shape industrial strategy, and encourage ecosystem participants to align resources toward national objectives.

In this context, procurement should be viewed not merely as a purchasing function, but as a strategic capability-development instrument.-tive.

The future success of India's defence-space ecosystem will depend not only on its ability to generate innovation, but on its ability to create demand structures capable of absorbing that innovation. Research creates possibilities. Procurement determines whether those possibilities become operational realities.

The next challenge, however, emerges once demand begins to materialize. Even with strong procurement frameworks and growing adoption, industrial ecosystems must still overcome a more fundamental constraint: scale. Technologies can be developed and procured, but without sufficient capital, manufacturing depth, and supply-chain resilience, they struggle to evolve into enduring national capabilities. Understanding the economics of strategic capacity therefore becomes the next critical step in building a sustainable defence-space industrial ecosystem.



Financing and Scaling Strategic Capacity: The Economics of Defence Space

One of the most significant misconceptions surrounding the space economy is the assumption that technological capability automatically translates into industrial capability. In reality, the two are fundamentally different. A country may possess talented engineers, successful startups, advanced research institutions, and even proven technologies, yet still struggle to build a globally competitive space industry. The missing ingredient is often capital—not merely funding for innovation, but financing for scale.

Historically, space was primarily a government-funded enterprise. National agencies financed research, developed infrastructure, procured systems, and absorbed much of the technological risk. The emergence of commercial space has fundamentally altered this model. Today's space economy increasingly depends upon private investment, venture capital, institutional financing, advanced manufacturing, and long-term industrial investment. As a result, access to capital is becoming as important as access to technology.

This reality is particularly relevant for defence-space capabilities. Unlike software ventures that can achieve rapid growth with relatively modest capital requirements, space and defence technologies are inherently capital-intensive. Satellite manufacturing facilities, advanced electronics production lines, propulsion systems, testing infrastructure, launch integration capabilities, and secure communications architectures require substantial upfront investment. Development timelines are often measured in years rather than months, while returns may only materialize after lengthy qualification and procurement cycles.

The consequence is what may be described as a financing mismatch. Defence-space ventures often require patient capital, but much of the private investment ecosystem is optimized for rapid growth and shorter investment horizons. Venture investors typically seek scalable opportunities capable of generating significant returns within predictable timeframes. Defence-space companies, however, frequently operate in environments characterized by long development cycles, regulatory complexity, limited customer bases, and uncertain procurement outcomes. The result is a structural gap between the type of capital available and the type of capital required.This challenge is not unique to India. Across the world, governments are increasingly recognizing that strategic industries cannot rely exclusively on traditional market mechanisms. The United States has expanded support for dual-use technology ecosystems through defence innovation programmes, strategic contracting mechanisms, and public-private investment models. Europe has launched major initiatives aimed at strengthening industrial resilience and reducing technological dependencies.

Manufacturing Depth as Strategic Capacity

Financing challenges become even more significant when viewed through the lens of manufacturing. Much of the global discussion surrounding space innovation focuses on startups, software platforms, and emerging technologies. Yet future strategic advantage will depend equally on manufacturing depth.

The history of industrial competition demonstrates that nations rarely achieve technological leadership without corresponding production capability. During the Second World War, industrial output became a decisive determinant of military success. During the Cold War, manufacturing capacity enabled sustained technological competition. In the emerging space age, the ability to produce satellites, sensors, electronics, propulsion systems, and advanced materials at scale may prove equally important.

The economics of this challenge are becoming increasingly evident. Traditional space programmes were designed around a small number of highly sophisticated assets. The emerging space economy is moving toward distributed architectures comprising hundreds or even thousands of satellites. Such architectures require entirely different industrial models. Success increasingly depends on production efficiency, supply-chain integration, automation, and manufacturing scalability.

This transformation has profound implications for India. The country's long-term competitiveness will depend not only on its ability to design advanced systems but also on its ability to produce them repeatedly, affordably, and at scale. The challenge therefore extends beyond innovation policy into industrial policy. Supply chains, component manufacturing, electronics ecosystems, materials capability, and advanced production infrastructure all become critical elements of national space power.

The Rise of Strategic Capital

A second shift is also becoming visible globally. Increasingly, capital itself is being viewed as strategic infrastructure. Nations are beginning to recognize that critical technologies often require financing mechanisms different from those used in conventional commercial sectors. Sovereign funds, defence innovation funds, strategic investment vehicles, and public-private financing models are emerging as important tools for capability development. Their purpose is not simply to provide capital but to bridge the gap between technological potential and industrial scale.

For India, this issue is likely to become increasingly important over the coming decade. The country possesses a rapidly growing space ecosystem, expanding defence requirements, and a vibrant entrepreneurial base. However, sustaining growth across these sectors will require financing mechanisms capable of supporting long-term industrial development. The challenge is not merely to fund startups; it is to finance the creation of enduring industrial capacity.

This distinction matters because strategic competition is increasingly becoming a competition between ecosystems rather than individual firms. The countries that succeed will not necessarily be those producing the highest number of startups or prototypes. They will be those capable of creating self-reinforcing cycles of innovation, investment, manufacturing, and deployment.

Ultimately, space power is not built solely through technology. It is built through the institutions, industries, supply chains, and financial systems that enable technology to scale. Innovation may create a breakthrough, but capital determines whether that breakthrough remains a prototype or becomes a national capability. As India seeks to strengthen its defence-space ecosystem, the challenge therefore extends beyond funding innovation. It involves building the economic foundations capable of sustaining strategic capacity over decades rather than years.



Industrial Capacity as Strategic Deterrence

For much of modern military history, deterrence has been associated with visible instruments of power. Armies, naval fleets, air forces, missile arsenals, and strategic weapons systems traditionally served as the principal indicators of national strength. Military planning focused on platforms, force structures, and inventories. The underlying assumption was straightforward: the side possessing superior capabilities would possess greater strategic advantage.

The character of conflict is changing. The emerging space age is introducing a different logic of competition—one in which the ability to sustain, replenish, adapt, and regenerate capability may become as important as the capability itself. In this environment, industrial capacity evolves from an economic asset into a strategic asset.

This shift is already visible in contemporary conflicts. The Russia–Ukraine war has highlighted the extent to which industrial production, supply-chain resilience, logistics networks, and technological adaptation influence battlefield outcomes. Military effectiveness has increasingly depended not only on the quality of equipment deployed at the outset of conflict but on the ability to replace losses, expand production, integrate emerging technologies, and sustain operations over time. The lesson is clear: modern wars are not won solely by inventories accumulated before conflict; they are won by the capacity to generate capability during conflict.

The implications for the space domain are profound. For decades, military space planning focused primarily on protecting a limited number of high-value assets. Satellites were expensive, scarce, and difficult to replace. Consequently, resilience was often viewed through the lens of protection. The objective was to prevent disruption.

The emerging architecture of space power is fundamentally different. Large satellite constellations, distributed networks, proliferated systems, software-defined payloads, and commercial space services are reshaping the economics of resilience. Future military effectiveness may depend less on protecting every asset and more on maintaining the ability to rapidly replace, reconstitute, and upgrade capabilities when disruption occurs.

This represents a transition from asset-centric resilience to industrial resilience.



The Era of Capability Regeneration

A defining feature of future conflicts may be the contest between attrition and regeneration. Historically, industrial mobilization occurred over months or years. Modern space architectures may require regeneration cycles measured in weeks or even days. Satellites may need to be replenished rapidly. Communications capacity may need to be restored almost immediately. Space-based intelligence networks may require continuous augmentation to compensate for evolving threats and operational requirements.

The countries capable of responding to these demands will possess a significant strategic advantage.This requires a fundamentally different approach to industrial planning. Manufacturing systems must become more agile. Supply chains must become more resilient. Production processes must become more automated. Launch systems must become more responsive. Software architectures must support continuous upgrades rather than periodic modernization cycles.

The challenge is not merely technological. It is organizational. National ecosystems must be capable of operating at a tempo that traditional defence-industrial models were never designed to support.

From Platforms to Production Capacity

One of the most important strategic lessons of the coming decade may be that production capacity itself becomes a measure of power.

The traditional metrics of space capabilitysatellites launched, missions completed, or infrastruc ture deployed—remain important. However, they provide only a snapshot of capability at a specific moment in time. Strategic competition increasingly rewards adaptability rather than static advantage.

A nation possessing a hundred satellites but limited replacement capacity may ultimately be less resilient than a nation capable of manufacturing and deploying dozens of satellites every month. Similarly, a country that relies on fragile supply chains may possess impressive capabilities in peacetime but face significant vulnerabilities during crises.

This is why industrial depth matters. Supply chains, component manufacturing, electronics ecosystems, testing infrastructure, launch capability, software development, and workforce readiness collectively determine the ability to sustain strategic capability under stress. These factors are rarely visible, yet they often determine long-term outcomes.

The Strategic Logic for India

For India, the significance of industrial capacity extends beyond military preparedness. The country is entering a period in which space capabilities will increasingly support economic activity, digital infrastructure, communications networks, disaster response, national security, and geopolitical influence. As dependence on space-enabled services grows, resilience becomes a national requirement rather than a sectoral concern.

This reality places new responsibilities on the defence-space industrial ecosystem. Success can no longer be measured solely through technological achievements or individual missions. The more important question is whether the ecosystem can sustain capability under conditions of prolonged competition and uncertainty.

Can critical components be produced domestically at scale?

Can satellite manufacturing be accelerated when required?

Can launch capacity respond rapidly to operational needs?

Can commercial and military capabilities be integrated into resilient architectures?

Can innovation cycles operate faster than evolving threats?

The future space economy will undoubtedly generate new technologies, new business models, and new forms of competition. Yet the ultimate foundation of space power will remain industrial. Nations that can consistently transform innovation into production, production into capability, and capability into resilience will possess enduring advantages.

The next phase of strategic competition may therefore be defined less by who launches first and more by who can recover fastest, scale quickest, and adapt most effectively. In such an environment, industrial capacity is not merely a contributor to deterrence—it becomes deterrence itself.

Conclusion: From Capability Creation to Capacity Sustenance

The evolution of the global space sector is redefining the foundations of national power. Space capability is no longer measured solely by technological achievement, scientific accomplishment, or strategic assets in orbit. Increasingly, it is measured by the strength of the ecosystem capable of creating, sustaining, and continuously renewing those capabilities over time.

India's achievements in space have established a strong foundation for future growth. The country's success in launch systems, satellite technologies, navigation capabilities, planetary exploration, and applications-driven innovation has demonstrated both technological competence and institutional excellence. Yet the demands of the coming decade will require a broader transformation. The challenge is no longer simply to build capability. It is to build the industrial, financial, technological, and institutional capacity necessary to sustain capability at scale.

The central argument of this chapter is that enduring space power is ultimately an ecosystem outcome. Innovation must connect with industry. Research must connect with deployment. Capital must connect with manufacturing. Procurement must connect with capability development. National institutions, private enterprises, academia, investors, and end users must operate not as isolated actors but as components of a larger strategic system. The strength of this system will increasingly determine India's ability to compete, adapt, and lead in an increasingly dynamic space environment.

This transition carries significance far beyond the space sector itself. As communications, navigation, intelligence, disaster response, digital infrastructure, and military operations become increasingly dependent upon space-enabled capabilities, the resilience of the broader national ecosystem becomes a matter of strategic importance. The ability to innovate continuously, manufacture at scale, secure supply chains, attract capital, and regenerate capability under pressure will become defining attributes of national competitiveness.

The next phase of India's space journey will therefore be shaped not only by what is launched into orbit, but by what is built on the ground. The countries that emerge as enduring space powers will not necessarily be those that achieve the most spectacular technological milestones. They will be those that create the institutions, industries, partnerships, and ecosystems capable of sustaining progress across decades of technological change and geopolitical competition.

India has already demonstrated its ability to create capability. The defining challenge of the next decade is to transform that capability into sustained capacity. Achieving this transition will not only strengthen India's strategic autonomy and economic competitiveness, but also position the country as one of the principal architects of the next era of global space development.

Strategic Priorities for the Next Decade

- **Building a National Space Production Base**

The next phase of India's space journey will require a transition from project-based execution to industrial-scale production. Future military and commercial architectures will depend on satellite constellations, advanced electronics, secure communications systems, space-based intelligence platforms, and responsive launch capabilities operating at a scale far beyond traditional programmes. Building a national production base capable of manufacturing, integrating, testing, and deploying these systems rapidly and repeatedly will be essential. The strategic objective should not simply be technological self-reliance, but the ability to sustain capability generation at scale.

- **Accelerating the Innovation-to-Deployment Cycle**

India's growing innovation ecosystem has demonstrated significant technological potential across space, defence, digital technologies, and advanced manufacturing. The next challenge lies in shortening the journey from research to operational capability. Greater integration between academia, startups, industry, defence users, and national institutions will be required to ensure that promising technologies are rapidly tested, validated, adopted, and scaled. Future competitiveness will increasingly depend on the speed at which ideas are translated into deployable capability.

- **Strengthening Sovereign Supply Chains**

As geopolitical competition intensifies and technology ecosystems become increasingly fragmented, resilient supply chains will emerge as a critical component of national security. Semiconductors, advanced materials, sensors, propulsion systems, electronics, and strategic components will form the backbone of future space architectures. Developing trusted and diversified supply chains, while reducing vulnerabilities in critical areas, will be central to sustaining long-term industrial resilience.space activity.

- **Expanding Strategic Capital for Defence Space**

The growth of India's defence-space ecosystem will require financing mechanisms aligned with the long development cycles and capital intensity of strategic technologies. Traditional venture capital models alone are unlikely to support the scale of investment required for advanced manufacturing, infrastructure development, deep technology innovation, and capability maturation. The coming decade will require a broader ecosystem of patient capital, institutional investment, strategic funding mechanisms, and public-private financing models capable of supporting long-term industrial growth.

- **Institutionalizing Civil–Military–Commercial Integration**

The distinction between civilian, commercial, and military space capabilities is becoming increasingly blurred. Communications networks, Earth observation systems, launch services, geospatial analytics, and digital infrastructure are now supporting both economic and security objectives simultaneously. Future resilience will depend on the ability to integrate these domains within a common ecosystem. Strengthening collaboration among government agencies, defence establishments, industry, academia, and commercial operators will be essential to building a responsive and adaptive space architecture.

- **Preparing for Responsive and Resilient Space Operations**

The future strategic environment will place greater emphasis on resilience, adaptability, and capability regeneration. Space architectures will need to withstand disruption, recover rapidly, and evolve continuously in response to emerging threats and technological change.



PERSISTENT SPACE CAPABILITY, LAUNCH AGILITY AND MISSION SUSTAINMENT

Introduction: From Access to Persistence

For much of the Space Age, national prestige and strategic relevance were measured by access to space. The ability to launch satellites, place payloads into orbit, and demonstrate technological competence defined a country's position within the global space hierarchy. Space programmes were evaluated through missions completed, launch vehicles developed, and scientific milestones achieved. Access was the primary objective because access itself was scarce.

That era is rapidly coming to an end. The contemporary strategic environment is characterized not by scarcity of access, but by the proliferation of capability. More countries, companies, and institutions now possess the ability to operate in space than at any point in history. Thousands of satellites are being deployed across multiple orbital regimes. Commercial constellations are transforming communications and Earth observation. Military organizations increasingly depend upon space-based services for intelligence, surveillance, targeting, navigation, communications, and operational planning. As space becomes embedded within the foundations of modern economic and security architectures, a new strategic question is emerging.

The challenge is no longer how to reach space. The challenge is how to remain effective in space.

This distinction is more significant than it appears. Space systems were traditionally designed around periodic observations, limited coverage, and relatively static operating concepts. Modern military operations, however, require continuous awareness, real-time information, rapid decision-making, and uninterrupted access to critical services. The shift from episodic support to persistent support is fundamentally transforming how space architectures are designed, operated, and sustained.

At the same time, the space domain itself is becoming increasingly contested. The proliferation of satellites, the emergence of counter-space capabilities, growing dependence on orbital infrastructure, and the integration of space into military operations have collectively elevated the importance of resilience. Space systems must now be designed not only for performance but also for survivability, redundancy, adaptability, and rapid recovery.



The Quest for Persistent Space Awareness: From Episodic ISR to Continuous Battlespace Visibility

The history of military space operations has largely been a history of intermittent observation. Traditional intelligence, surveillance, and reconnaissance (ISR) architectures were designed around periodic coverage, where satellites passed over areas of interest at predetermined intervals and collected information that was subsequently processed, analysed, and disseminated. While such systems provided valuable strategic intelligence, they were often constrained by revisit rates, data latency, and the inability to maintain continuous visibility over dynamic operational environments.

Modern warfare is increasingly exposing the limitations of this approach.Military operations now unfold across compressed timelines and multiple domains simultaneously. Force mobilizations, missile launches, electronic emissions, maritime movements, drone operations, and logistical activities can evolve within minutes rather than days. The value of intelligence is therefore determined not only by accuracy, but by timeliness. Information that arrives after an event has occurred may be useful for analysis, but it is often less useful for decision-making.

This reality is driving a fundamental shift from episodic ISR to persistent battlespace awareness. Persistent awareness seeks to create a continuously updated understanding of operational environments by integrating multiple sensors, orbital layers, and data sources into a single intelligence architecture. Rather than relying on isolated observations, the objective is to maintain an uninterrupted picture of activities across land, maritime, air, cyber, and space domains. The goal is not merely surveillance; it is decision superiority.

The End of Platform-Centric ISR

For decades, ISR capability was often associated with individual platforms. A satellite collected imagery. A radar tracked movement. A signals intelligence payload intercepted communications. Each platform contributed a specific layer of information.

The future architecture is fundamentally different.Increasingly, intelligence will be generated through constellations rather than individual satellites. Hundreds of sensors operating across multiple orbital regimes will function as an integrated network capable of continuously observing, correlating, and analysing activity. Information will no longer be derived from a single source but from the fusion of multiple sources operating simultaneously.

This transition mirrors developments occurring in other military domains. Modern combat systems increasingly rely on networks rather than platforms, ecosystems

systems increasingly rely on networks rather than platforms, ecosystems rather than assets, and information superiority rather than numerical superiority. Space architectures are evolving along the same trajectory.

Multi-Orbit Architectures and Continuous Coverage

No single orbital regime can independently provide the persistence, resolution, survivability, and responsiveness required by modern military operations. Low Earth Orbit offers high-resolution observations and rapid revisit rates but limited dwell time. Geostationary systems provide continuous coverage over broad areas but lack the resolution required for tactical applications. Medium Earth Orbit and highly elliptical orbits offer additional advantages that complement these capabilities.

The future therefore lies in multi-orbit architectures. Such architectures combine the strengths of different orbital layers to create a persistent intelligence ecosystem. Low Earth Orbit constellations provide detailed tactical awareness. Medium Earth Orbit systems support broader surveillance and data fusion. Geostationary platforms contribute strategic monitoring, communications, and early warning capabilities. Together, these layers form a resilient and interconnected architecture capable of supporting operations across multiple levels of warfare.

The significance of this approach extends beyond surveillance. Multi-orbit integration enables continuity. If one layer is degraded, disrupted, or unavailable, others can compensate. Persistence is achieved not through a single asset, but through the collective resilience of the architecture.

Analytics as the New Centre of Gravity

The expansion of sensing capabilities is generating an unprecedented volume of data. Modern constellations can collect imagery, signals, telemetry, weather information, and environmental observations at a scale far beyond the capacity of traditional analytical methods. The challenge is no longer data collection. The challenge is extracting meaning from data quickly enough to influence decisions.

Consequently, the centre of gravity in future ISR architectures is shifting from sensors to analytics. Advanced analytics systems are increasingly capable of identifying patterns, detecting anomalies, tracking behavioural changes, and correlating information across multiple sources. Instead of simply observing events, they help explain what those events mean and what they may indicate about future activity.

This transformation is particularly important for military applications. Heat signatures may reveal force mobilization. Signals intelligence may indicate changes in operational posture. Repeated movement patterns may suggest preparation for specific actions. The ability to connect these indicators into coherent assessments significantly enhances situational awareness.

AI and the Compression of Decision Cycles

Artificial intelligence is accelerating this transformation further. Emerging AI systems are beginning to fuse optical imagery, synthetic aperture radar data, signals intelligence, geospatial information, and operational doctrine into integrated analytical frameworks. Such systems can identify targets, monitor activity, detect changes, and generate assessments at speeds impossible through manual analysis alone.

The strategic significance of this capability lies in its impact on decision cycles. Future conflicts are likely to be characterized by intense competition between sensing, analysis, decision-making, and action. The side capable of moving through this cycle faster gains a significant operational advantage. AI-enabled analytics therefore become more than an efficiency tool; they become a force multiplier.

Persistent awareness is ultimately about reducing uncertainty. It seeks to transform fragmented observations into continuous understanding and convert information into actionable insight. In an era where military effectiveness increasingly depends on speed, precision, and awareness, the ability to maintain persistent visibility across the battlespace may prove as decisive as traditional measures of military strength.

The challenge, however, is that awareness alone does not guarantee resilience. Even the most sophisticated intelligence architecture remains vulnerable if it cannot withstand disruption, degradation, or loss. The next stage in the evolution of space capability therefore involves building systems designed not only to observe continuously, but to endure continuously.

The Rise of Autonomous Space Operations

Analytics, Edge Computing and Machine-Speed Decision Making

The value of persistent awareness ultimately depends on the ability to transform information into action. Modern space architectures are generating unprecedented volumes of data through optical sensors, synthetic aperture radar systems, electronic intelligence payloads, weather satellites, navigation networks, and communications constellations. Yet the strategic advantage does not lie in the possession of data itself. It lies in the ability to interpret, prioritize, and act upon that data before an adversary can do the same.

This reality is driving a fundamental shift in the nature of space operations. The traditional model relied heavily on human analysts processing information after collection, often through multiple layers of review and dissemination. Such approaches were effective when data volumes were manageable and operational timelines were measured in hours or days. Future operational environments, however, will be defined by decision cycles measured in minutes or seconds. Human-centric analytical models are increasingly unable to keep pace with the scale and speed of modern information flows.

The consequence is the emergence of autonomous space operations, where artificial intelligence, machine learning, edge computing, and advanced analytics become integral components of operational architectures rather than supplementary tools.

From Data Collection to Decision Intelligence

Historically, ISR systems were designed to answer the question: What is happening?
The next generation of systems must answer a more complex set of questions:

- Why is it happening?
- What is likely to happen next?
- What actions should be considered in response?

This evolution marks the transition from information gathering to decision intelligence.
Modern analytical architectures are increasingly capable of integrating multiple data streams simultaneously. Optical imagery can be fused with radar observations, electronic emissions, weather patterns, terrain data, maritime traffic information, and historical behavioural models. The resulting intelligence picture is significantly richer than what any individual sensor can provide.

The strategic advantage of such integration is not simply improved awareness. It is the ability to identify weak signals, detect emerging patterns, and generate predictive insights before events fully materialize. In many cases, the greatest value of intelligence lies not in describing events after they occur but in anticipating them before they unfold.

Foundation Models and the Future of Space Analytics

The emergence of large-scale AI models is creating new possibilities for space operations. Just as foundation models have transformed language processing and computer vision, similar approaches are beginning to influence geospatial intelligence and space analytics.

Future analytical systems may be capable of ingesting enormous volumes of multi-source data and creating continuously evolving representations of operational environments. These systems will not simply identify objects or classify imagery. They will develop contextual understanding of activities, relationships, behaviours, and anomalies across entire theatres of operation.

A maritime surveillance system, for example, may no longer focus solely on identifying vessels. Instead, it may analyse behavioural patterns, shipping routes, communication activity, weather conditions, and historical movement data to identify suspicious behaviour automatically. Similarly, border monitoring systems may correlate imagery, terrain analysis, infrastructure development, transportation activity, and electronic emissions to generate assessments regarding evolving operational conditions.

The implications extend far beyond surveillance. As analytical models become increasingly sophisticated, they will support planning, resource allocation, threat assessment, and mission management functions across multiple domains simultaneously.

Edge Computing and Distributed Intelligence

A second transformation involves where analysis occurs.Traditional architectures often required raw data to be transmitted to centralized processing facilities before analysis could begin. While effective for many applications, this approach introduces latency and increases dependence on communications infrastructure. Future architectures are increasingly moving intelligence closer to the sensor itself.

The strategic implications are substantial. In contested environments where communications may be disrupted or degraded, distributed intelligence architectures provide greater resilience. Satellites become more than sensing platforms; they become intelligent nodes within a larger operational network.



The Compression of Decision Cycles

Throughout military history, competitive advantage has often been linked to the speed of decision-making. The ability to observe, orient, decide, and act faster than an adversary has repeatedly proven decisive in conflict.

Space-enabled intelligence is now becoming a central component of this dynamic.
Artificial intelligence, predictive analytics, and autonomous systems are dramatically reducing the time required to move from observation to action. Activities that once required teams of analysts working over extended periods can increasingly be performed in near real time. This compression of decision cycles enhances responsiveness, improves situational awareness, and enables more effective operational planning.

The strategic significance of this trend extends beyond efficiency. Faster decision cycles create opportunities to shape events rather than simply react to them. They allow military and civilian decision-makers to operate proactively rather than defensively.

However, speed alone does not guarantee success. The ability to process information rapidly must be accompanied by architectures capable of surviving disruption and maintaining continuity under stress. As dependence on space-enabled services grows, resilience becomes as important as intelligence itself. The future of space operations will therefore depend not only on awareness and analytics, but also on the ability to sustain those capabilities in contested and uncertain environments.

Mission Resilience Through Layered Architectures

- ### Constellations, Redundancy and Reconstitution

The history of space systems has traditionally been defined by scarcity. Satellites were expensive, technologically complex, and limited in number. Individual assets often performed critical functions, creating architectures heavily dependent on a relatively small number of platforms. While these systems delivered impressive capabilities, they also created vulnerabilities. The loss or degradation of a single satellite could have significant operational consequences.

The emerging space environment is driving a fundamental rethinking of this model. As military operations, economic systems, and critical infrastructure become increasingly dependent upon space-enabled services, resilience is becoming a central design requirement. The challenge is no longer simply how to deploy capability into orbit. The challenge is how to ensure that capability remains available despite technical failures, environmental hazards, operational disruptions,



The Compression of Decision Cycles

Throughout military history, competitive advantage has often been linked to the speed of decision-making. The ability to observe, orient, decide, and act faster than an adversary has repeatedly proven decisive in conflict.

Space-enabled intelligence is now becoming a central component of this dynamic.
Artificial intelligence, predictive analytics, and autonomous systems are dramatically reducing the time required to move from observation to action. Activities that once required teams of analysts working over extended periods can increasingly be performed in near real time. This compression of decision cycles enhances responsiveness, improves situational awareness, and enables more effective operational planning.

The strategic significance of this trend extends beyond efficiency. Faster decision cycles create opportunities to shape events rather than simply react to them. They allow military and civilian decision-makers to operate proactively rather than defensively.

However, speed alone does not guarantee success. The ability to process information rapidly must be accompanied by architectures capable of surviving disruption and maintaining continuity under stress. As dependence on space-enabled services grows, resilience becomes as important as intelligence itself. The future of space operations will therefore depend not only on awareness and analytics, but also on the ability to sustain those capabilities in contested and uncertain environments.

Mission Resilience Through Layered Architectures

- ### Constellations, Redundancy and Reconstitution

The history of space systems has traditionally been defined by scarcity. Satellites were expensive, technologically complex, and limited in number. Individual assets often performed critical functions, creating architectures heavily dependent on a relatively small number of platforms. While these systems delivered impressive capabilities, they also created vulnerabilities. The loss or degradation of a single satellite could have significant operational consequences.

The emerging space environment is driving a fundamental rethinking of this model. As military operations, economic systems, and critical infrastructure become increasingly dependent upon space-enabled services, resilience is becoming a central design requirement. The challenge is no longer simply how to deploy capability into orbit. The challenge is how to ensure that capability remains available despite technical failures, environmental hazards, operational disruptions, or deliberate interference.

Reconstitution as a Strategic Capability

Traditional resilience strategies focused primarily on protection. The objective was to prevent failure. The emerging environment demands a different approach. No system can be guaranteed complete protection against technical failure, orbital congestion, cyber intrusion, or evolving threats. Consequently, resilience increasingly depends upon the ability to restore capability rapidly when disruption occurs.

This introduces the concept of reconstitution. Reconstitution refers to the ability to replace, augment, or regenerate space capability within operationally relevant timelines. It transforms resilience from a passive concept into an active capability. The focus shifts from preventing all disruption to ensuring rapid recovery after disruption.

For military planners, this distinction is critical. Future conflicts may involve efforts to degrade communications networks, surveillance architectures, navigation systems, or data infrastructure.

Designing for Continuity

Mission sustainment begins long before a satellite is launched. It begins during architecture design. Future systems must be designed with continuity as a foundational requirement rather than an afterthought. Redundancy, interoperability, modularity, distributed operations, and flexible deployment models must be embedded into system architectures from the outset.

This represents a departure from traditional thinking. Instead of optimizing solely for performance, future architectures must optimize for endurance. They must be capable of operating through uncertainty, adapting to changing circumstances, and recovering from disruption without catastrophic loss of functionality.

For India, this principle carries growing importance. As national dependence on space-enabled capabilities expands across defence, communications, maritime awareness, disaster management, and digital infrastructure, the consequences of disruption become increasingly significant. Building resilient architectures is therefore not merely a technical challenge; it is a strategic necessity.

The future of space power will depend not only on the sophistication of individual systems but on the resilience of the broader architecture that supports them. Awareness creates understanding. Analytics enable decisions. Resilience ensures continuity.

The next challenge is restoring and expanding capability at operational speed. This requires a new approach to access itself—one based not on periodic launches, but on the ability to place capabilities into orbit whenever strategic conditions demand. Responsive launch therefore becomes the next critical pillar of mission readiness and sustainment.

Launch Agility and Responsive Space

- **Rebuilding Capability at Operational Speed**

For most of the Space Age, launch was viewed as a discrete event. Satellites were developed over many years, launch campaigns were planned months in advance, and missions were designed around long development cycles. This approach reflected a strategic environment in which space systems were relatively scarce, operational requirements evolved slowly, and the primary objective was achieving reliable access to orbit.

The demands of the emerging strategic environment are fundamentally different. Modern military operations increasingly require flexibility, adaptability, and responsiveness. Space architectures are becoming larger, more distributed, and more deeply integrated into operational planning.



The In-Space Logistics Revolution

- **Servicing, Refuelling and Orbital Sustainment**

The first six decades of the Space Age were largely defined by a simple operational model. Satellites were launched, performed their intended missions, and eventually ceased operations when fuel was exhausted, systems degraded, or mission requirements changed. Once deployed, space assets were generally treated as fixed and finite resources. Their lifespan was determined largely by design limitations rather than operational choices.

That model is beginning to change. A new generation of technologies is transforming how nations think about spacecraft operations, asset management, and mission sustainment. Orbital servicing, refuelling, inspection, repair, relocation, and autonomous proximity operations are creating the foundations of what may eventually become a fully developed in-space logistics ecosystem. The implications of this transition are comparable to the emergence of logistics networks in aviation, maritime trade, and terrestrial transportation. Space is gradually evolving from an environment where assets are deployed and abandoned into an environment where assets can be maintained, upgraded, and sustained.

The Emergence of Orbital Logistics

Every mature transportation system relies upon logistics.
Ships require ports. Aircraft require maintenance facilities. Military forces require supply chains. Space systems have historically operated without equivalent support structures. As a result, satellites were often designed with significant redundancy and conservative operational assumptions because intervention after launch was largely impossible.Orbital servicing changes this equation.

The ability to inspect, repair, reposition, or refuel satellites introduces flexibility that has rarely existed in space operations. Assets can remain operational longer. Failures can potentially be mitigated. Mission profiles can evolve after deployment. The operational life of critical infrastructure can be extended significantly.

The strategic significance of these capabilities extends far beyond cost savings. They introduce an entirely new layer of resilience into space architectures.

Docking as a Foundational Capability

At the centre of this transformation lies one of the most important technological developments in future space operations: docking.
The ability of spacecraft to approach, rendezvous, and physically connect with one another creates the foundation upon which many future capabilities will depend. Refuelling, servicing, assembly, repair, transportation, and orbital mobility all require reliable docking technologies.

Historically, docking was associated primarily with human spaceflight and space stations. Future applications are likely to be far broader. Commercial satellites, military platforms, servicing vehicles, orbital depots, and future infrastructure nodes may all rely upon docking capabilities as a routine operational function.
As the number of satellites in orbit continues to grow, docking may become one of the foundational technologies that enables sustainable long-term operations in space.

Beyond Refuelling: The Future of Satellite Life Extension

Public discussions often associate orbital servicing with refuelling. While fuel replenishment remains important, the future scope of in-space servicing is considerably broader.
Emerging concepts include component replacement, software updates, sensor upgrades, debris inspection, orbit adjustments, and life-extension services that allow satellites to remain operational long after their original design life. In effect, satellites may increasingly evolve from disposable assets into maintainable infrastructure.

This shift has significant implications for both commercial and military operators. Critical systems can be sustained longer. Investments can be protected. Operational flexibility can be enhanced. Most importantly, mission continuity can be preserved without requiring immediate replacement.

The Strategic Importance of Orbital Mobility

A second dimension of orbital sustainment involves mobility.

Future space architectures are unlikely to remain static. Satellites may need to change positions, support evolving missions, respond to operational requirements, or integrate with new systems. Orbital mobility enables such flexibility by allowing spacecraft to manoeuvre more efficiently and adapt to changing circumstances.

In strategic terms, mobility enhances resilience. Assets that can be repositioned are often more difficult to predict, target, or constrain. Mobility also supports the development of distributed architectures in which capabilities can be reconfigured dynamically rather than remaining fixed throughout their operational life.

Conclusion: Persistence as the New Measure of Space Power

The first era of the Space Age was defined by access. The strategic challenge was reaching orbit. Nations competed to develop launch vehicles, deploy satellites, and demonstrate technological capability. Success was measured by pres ence in space.

The second era focused on capability. Communications networks, navigation systems, Earth observation constellations, and military space assets became essential components of national power. The objective was no longer merely access, but the effective utilization of space for economic, scientific, and strategic purposes.
A third era is now emerging.

As space becomes increasingly integrated into military operations, critical infrastructure, economic activity, and geopolitical competition, the defining challenge is shifting once again. Future success will depend not simply on access or capability, but on persistence. Nations must be able to maintain awareness, sustain operations, absorb disruption, restore capability, and adapt continuously within a dynamic and contested environment.

This transformation is reshaping every aspect of space architecture. Intelligence systems are evolving from periodic observation to continuous awareness. Analytics are moving from human-centred processing to machine-assisted decision-making. Space resilience is shifting from platform protection to architectural redundancy and rapid reconstitution. Launch systems are transitioning from scheduled operations to responsive capability deployment. Satellites themselves are evolving from finite assets into maintainable infrastructure supported by orbital servicing and logistics.

Taken together, these developments point toward a fundamental conclusion: space power is increasingly becoming a function of continuity.

The nations that emerge as leaders in the coming decades will not necessarily be those possessing the largest number of satellites or the most ambitious individual missions. They will be those capable of sustaining operational effectiveness despite uncertainty, competition, disruption, and technological change. Their advantage will derive from the ability to remain continuously present, continuously aware, and continuously capable.

For India, the significance of this transition is profound. As the country expands its role in the global space economy and deepens its dependence on space-enabled capabilities, persistence will become an essential requirement for both national security and economic resilience. Building such persistence will require investments not only in technology, but also in architecture, institutions, industrial capacity, analytics, launch readiness, and sustainment mechanisms.

Ultimately, the future of space power will be determined not by who reaches orbit first, but by who can remain effective there the longest. In the emerging era of continuous competition, persistence becomes more than an operational objective—it becomes the defining measure of strategic success.

Strategic Priorities for the Next Decade

- **Building a National Persistent ISR Architecture**

India's future space capability must evolve beyond individual satellites toward integrated, multi-layered intelligence architectures capable of delivering continuous awareness across terrestrial, maritime, air, cyber, and space domains. The objective should be the creation of a persistent national sensing ecosystem that combines optical, radar, electronic intelligence, navigation, and communications capabilities across multiple orbital regimes. Such architectures will increasingly underpin military decision-making, border management, maritime domain awareness, disaster response, and strategic deterrence.

- **Developing Sovereign Space Analytics and Artificial IntelligenceInstitutionalizing Civil–Military–Commercial Integration**

The strategic value of future space systems will increasingly reside in analytics rather than collection alone. As data volumes continue to expand exponentially, the ability to fuse information, generate predictive insights, identify anomalies, and support decision-making at operational speed will become a critical national capability. Investments in artificial intelligence, foundation models, geospatial intelligence platforms, edge computing, and autonomous analytics architectures should therefore be viewed as strategic infra structure rather than merely technological enhancements.

- **Creating Multi-Orbit Resilient Space Architectures**

Future resilience will depend upon diversity, redundancy, and architectural depth. India should progressively transition toward integrated multi-orbit architectures that combine Low Earth Orbit, Medium Earth Orbit, and Geostationary systems into a coherent operational framework. Such architectures will enhance continuity of operations, improve survivability, and reduce vulnerabilities associated with dependence on isolated platforms or orbital layers.

- **Establishing Responsive Launch Infrastructure**

The ability to launch rapidly in response to operational requirements will become a defining characteristic of future space powers. Responsive launch capability should therefore be treated as a component of national readiness rather than solely as a commercial service. Developing rapid integration mechanisms, distributed launch infrastructure, flexible mission architectures, and operational launch readiness will significantly strengthen India's ability to regenerate capability during periods of crisis or disruption.

- **Investing in Orbital Sustainment and Space Logistics**

Orbital servicing, satellite life extension, autonomous rendezvous operations, refuelling technologies, and in-space logistics are likely to become foundational elements of future space architectures. Early investments in these capabilities can position India at the forefront of an emerging domain that will shape both commercial and strategic space operations over the coming decades. The transition from deploy-and-replace models to maintain-and-sustain models will become increasingly important as orbital infrastructure grows in scale and complexity.

- **Institutionalising Mission Reconstitution Planning**

Historically, space planning focused primarily on capability deployment. Future planning must place equal emphasis on capability regeneration. Reconstitution strategies, reserve capacity, contingency architectures, launch readiness frameworks, and industrial support mechanisms should become integral components of national space planning. The ability to restore capability rapidly may ultimately prove as important as the capability itself.



SPACE FOR HOMELAND SECURITY, CIVIL DEFENCE AND INTERNAL SECURITY

Introduction: Expanding Space from Warfighting to National Resilience

The strategic discourse surrounding space is often dominated by military competition, deterrence, counter-space systems, and great-power rivalry. Yet for most nations, the largest and most immediate impact of space technology is not on the battlefield—it is within national borders.

Every year, governments face a growing spectrum of non-traditional security challenges: floods, wildfires, cyclones, landslides, industrial accidents, terrorism, narcotics trafficking, illegal migration, infrastructure failures, pandemics, urban crowd disasters, and climate-induced emergencies. These threats may not resemble conventional warfare, but their consequences can be equally devastating. They can disrupt economies, overwhelm institutions, damage critical infrastructure, displace populations, and undermine public confidence in the state.

The scale of these risks is increasing rapidly. According to the UN Office for Disaster Risk Reduction, the world now experiences nearly 400 major disasters annually, almost double the number recorded two decades ago. Climate-linked disasters alone have caused more than US$3.6 trillion in economic losses since 2000. India is among the world's most disaster-exposed nations, facing cyclones, floods, landslides, droughts, earthquakes, heatwaves, glacial lake outburst floods, and urban flooding simultaneously.

At the same time, internal security challenges are becoming increasingly complex. India's 15,000 km land borders, 7,500 km coastline, vast maritime zones, critical infrastructure networks, and rapidly urbanising population create a security environment that cannot be managed solely through manpower-intensive approaches. Traditional surveillance models designed for the twentieth century are struggling to cope with twenty-first century challenges.

This reality is driving a fundamental shift in homeland security thinking worldwide. The future of internal security will increasingly depend on persistent visibility, predictive intelligence, and real-time situational awareness. Space systems are uniquely positioned to provide all three.

The distinction between external security and internal security is becoming increasingly blurred. A major flood can disrupt critical infrastructure with consequences comparable to a conventional attack. A prolonged communications outage can affect emergency services, financial systems, and

The strategic discourse surrounding space is often dominated by military competition, deterrence, counter-space systems, and great-power rivalry. Yet for most nations, the largest and most immediate impact of space technology is not on the battlefield—it is within national borders.

Every year, governments face a growing spectrum of non-traditional security challenges: floods, wildfires, cyclones, landslides, industrial accidents, terrorism, narcotics trafficking, illegal migration, infrastructure failures, pandemics, urban crowd disasters, and climate-induced emergencies. These threats may not resemble conventional warfare, but their consequences can be equally devastating. They can disrupt economies, overwhelm institutions, damage critical infrastructure, displace populations, and undermine public confidence in the state.

The scale of these risks is increasing rapidly. According to the UN Office for Disaster Risk Reduction, the world now experiences nearly 400 major disasters annually, almost double the number recorded two decades ago. Climate-linked disasters alone have caused more than US$3.6 trillion in economic losses since 2000. India is among the world's most disaster-exposed nations, facing cyclones, floods, landslides, droughts, earthquakes, heatwaves, glacial lake outburst floods, and urban flooding simultaneously.

At the same time, internal security challenges are becoming increasingly complex. India's 15,000 km land borders, 7,500 km coastline, vast maritime zones, critical infrastructure networks, and rapidly urbanising population create a security environment that cannot be managed solely through manpower-intensive approaches. Traditional surveillance models designed for the twentieth century are struggling to cope with twenty-first century challenges.

This reality is driving a fundamental shift in homeland security thinking worldwide. The future of internal security will increasingly depend on persistent visibility, predictive intelligence, and real-time situational awareness. Space systems are uniquely positioned to provide all three.

The distinction between external security and internal security is becoming increasingly blurred. A major flood can disrupt critical infrastructure with consequences comparable to a conventional attack. A prolonged communications outage can affect emergency services, financial systems, and governance functions simultaneously.

A breakdown in situational awareness during a disaster can have consequences measured not only in economic losses but also in human lives. Security is therefore increasingly linked to resilience—the ability of a nation to anticipate risks, absorb shocks, and recover rapidly from disruption.

Space systems are emerging as one of the most powerful enablers of this resilience. Modern satellites can monitor environmental conditions across vast geographic areas, provide early warning of emerging hazards, support emergency communications when terrestrial networks fail, enable real-time situational awareness, track infrastructure performance, and generate actionable intelligence for decision-makers. Combined with advances in artificial intelligence, cloud computing, geospatial analytics, and digital governance platforms, these capabilities are creating entirely new approaches to public safety and homeland security.

The global trend is unmistakable. Countries are increasingly integrating space technologies into disaster management, border security, law enforcement, emergency communications, critical infrastructure protection, environmental monitoring, and urban governance. Homeland security is no longer viewed solely as a function of manpower and physical infrastructure. It is increasingly becoming a data-driven enterprise supported by persistent visibility and predictive intelligence.

For India, the significance of this transformation

From Static Geography to Dynamic Territory

Most governance systems remain rooted in static geography. Administrative maps identify boundaries, ownership records establish legal control, and infrastructure databases describe assets at a particular point in time. Yet the physical world changes continuously. Rivers alter their course. Urban areas expand. New construction emerges. Informal settlements develop. Infrastructure deteriorates. Environmental conditions evolve. Risk accumulates gradually until it becomes visible through a crisis.

The challenge is that administrative systems often struggle to keep pace with these changes. Digital twins offer an alternative model. Instead of describing territory periodically, they monitor territory continuously. High-resolution satellite imagery, synthetic aperture radar systems, climate sensors, utility networks, traffic systems, and geospatial databases are integrated into a living representation of the physical world. Decision-makers can therefore observe not only what exists today but also how conditions are changing over time.

The strategic implications are significant. Governments gain the ability to identify vulnerabilities before they become failures, monitor development patterns before they create risks, and detect anomalies before they escalate into emergencies. The emphasis shifts from observation to anticipation.

The Rise of Predictive Governance

One of the most important developments emerging from geospatial intelligence is the transition from descriptive governance to predictive governance. Historically, governments have focused on understanding current conditions. Increasingly, they seek to understand future conditions.

Advances in artificial intelligence and predictive modelling are making this possible. Satellite imagery can now be combined with hydrological models, climate projections, infrastructure databases, demographic information, and economic indicators to simulate future scenarios. Governments can evaluate how floods may propagate through urban areas, how heat stress may affect public infrastructure, how traffic disruptions may impact emergency response, or how population growth may alter service requirements.

Several advanced economies are already moving in this direction. Singapore's national digital twin programme has demonstrated how geospatial intelligence can support urban planning, emergency management, transportation optimization, and infrastructure resilience. Similar initiatives are emerging across Europe, the Gulf region, and East Asia. What began as a planning tool is increasingly becoming a national decision-support capability.

The strategic value lies not in visualization, but in foresight. The ability to identify risks before they materialize fundamentally changes how governments allocate resources, prioritize investments, and prepare for disruption.

Hyperlocal Intelligence in an Age of Systemic Risk

The next frontier of homeland security is not national-scale awareness. It is hyperlocal awareness. Many of the most damaging events in recent years have occurred at highly localized scales. Urban floods affecting specific neighbourhoods, landslides triggered on individual slopes, cloudbursts impacting isolated valleys, industrial accidents concentrated within limited geographic areas, and infrastructure failures affecting critical nodes have all demonstrated that risk is increasingly granular.

National-level monitoring often fails to capture such complexity. Future resilience will therefore depend upon the ability to understand territory at much higher levels of resolution. Which bridge faces the highest flood risk? Which power

substation is most vulnerable to extreme heat? Which transportation corridor becomes inaccessible first during a disaster? Which neighbourhood is likely to experience cascading infrastructure failures?

These are not questions that can be answered through conventional administrative reporting. They require integrated geospatial intelligence supported by continuous monitoring and predictive analytics.

The future of homeland security will increasingly depend upon such capabilities because the most consequential risks are no longer broad and visible. They are localized, interconnected, and often hidden until a crisis emerges.

The State as a Real-Time Decision System

Perhaps the most important implication of the digital twin concept is that it transforms the state itself. For much of modern history, governments functioned through periodic decision cycles. Reports were submitted monthly. Reviews occurred quarterly. Surveys were conducted annually. Strategic planning was based on information that was often months old by the time decisions were made.

Space-enabled geospatial intelligence is beginning to change this model. For the first time, governments are acquiring the ability to observe territory continuously. Infrastructure performance, environmental conditions, mobility patterns, public safety indicators, and emerging risks can increasingly be monitored in near real time. Decision-making becomes faster, more informed, and more adaptive.

This may ultimately prove to be one of the most important governance transformations of the twenty-first century. Just as digital networks transformed communications and the internet transformed information access, geospatial intelligence is transforming territorial awareness. Nations that successfully integrate these capabilities into governance systems will possess a significant advantage in managing complexity, reducing vulnerability, and strengthening resilience.
In this emerging environment, satellites are no longer simply tools for observation. They are becoming the foundation of a new operating system for the modern state. The future of homeland security will depend not merely on protecting territory, but on understanding territory with a level of precision, continuity, and predictive insight that was previously impossible.

Climate Security as Homeland Security: The New Geography of Risk

For much of modern history, climate and security were treated as separate policy domains. Climate was viewed primarily as an environmental concern, while security was associated with military threats, law enforcement challenges, and geopolitical competition. Government institutions reflected this separation. Environmental agencies monitored weather and natural resources, while security agencies focused on territorial integrity, public safety, and national defence.

That distinction is becoming increasingly difficult to sustain. Across the world, climate change is emerging not simply as an environmental challenge but as a force multiplier capable of amplifying existing vulnerabilities across infrastructure systems, economic networks, population centres, and governance institutions. The consequences are no longer confined to environmental degradation. They increasingly manifest as disruptions to public services, displacement of populations, resource competition, infrastructure failures, and pressures on state capacity.

In this sense, climate change is evolving into one of the most consequential homeland security challenges of the twenty-first century. The strategic significance of this transformation lies in the fact that climate impacts are rarely isolated events. They interact with transportation networks, power systems, communications infra-

substation is most vulnerable to extreme heat? Which transportation corridor becomes inaccessible first during a disaster? Which neighbourhood is likely to experience cascading infrastructure failures?

These are not questions that can be answered through conventional administrative reporting. They require integrated geospatial intelligence supported by continuous monitoring and predictive analytics.

The future of homeland security will increasingly depend upon such capabilities because the most consequential risks are no longer broad and visible. They are localized, interconnected, and often hidden until a crisis emerges.

The State as a Real-Time Decision System

Perhaps the most important implication of the digital twin concept is that it transforms the state itself. For much of modern history, governments functioned through periodic decision cycles. Reports were submitted monthly. Reviews occurred quarterly. Surveys were conducted annually. Strategic planning was based on information that was often months old by the time decisions were made.

Space-enabled geospatial intelligence is beginning to change this model. For the first time, governments are acquiring the ability to observe territory continuously. Infrastructure performance, environmental conditions, mobility patterns, public safety indicators, and emerging risks can increasingly be monitored in near real time. Decision-making becomes faster, more informed, and more adaptive.

This may ultimately prove to be one of the most important governance transformations of the twenty-first century. Just as digital networks transformed communications and the internet transformed information access, geospatial intelligence is transforming territorial awareness. Nations that successfully integrate these capabilities into governance systems will possess a significant advantage in managing complexity, reducing vulnerability, and strengthening resilience.
In this emerging environment, satellites are no longer simply tools for observation. They are becoming the foundation of a new operating system for the modern state. The future of homeland security will depend not merely on protecting territory, but on understanding territory with a level of precision, continuity, and predictive insight that was previously impossible.

Climate Security as Homeland Security: The New Geography of Risk

For much of modern history, climate and security were treated as separate policy domains. Climate was viewed primarily as an environmental concern, while security was associated with military threats, law enforcement challenges, and geopolitical competition. Government institutions reflected this separation. Environmental agencies monitored weather and natural resources, while security agencies focused on territorial integrity, public safety, and national defence.

That distinction is becoming increasingly difficult to sustain. Across the world, climate change is emerging not simply as an environmental challenge but as a force multiplier capable of amplifying existing vulnerabilities across infrastructure systems, economic networks, population centres, and governance institutions. The consequences are no longer confined to environmental degradation. They increasingly manifest as disruptions to public services, displacement of populations, resource competition, infrastructure failures, and pressures on state capacity.

In this sense, climate change is evolving into one of the most consequential homeland security challenges of the twenty-first century. The strategic significance of this transformation lies in the fact that climate impacts are rarely isolated events. They interact with transportation networks, power systems, communications infra-

Coastal Resilience and the Expanding Security Perimeter

While the Himalayas represent one frontier of climate risk, India's coastlines represent another. More than 250 million people live within coastal districts, while a substantial proportion of economic activity, industrial infrastructure, ports, logistics networks, and energy assets are concentrated near the coast. Rising sea levels, intensifying cyclones, coastal erosion, and changing marine conditions are therefore creating a new category of security challenge.

Traditionally, coastlines were viewed primarily through the lens of maritime security. Increasingly, they must also be viewed through the lens of climate resilience. Future disruptions may not originate from hostile actors. They may originate from storm surges damaging critical infrastructure, flooding affecting transportation networks, or environmental changes impacting coastal livelihoods. These developments can create secondary effects that influence migration, economic stability, and public services.

Space-based monitoring systems are becoming central to managing these risks. Satellite observations support cyclone forecasting, coastal erosion assessment, maritime domain awareness, infrastructure planning, and environmental monitoring. More importantly, they provide decision-makers with a long-term understanding of how coastlines themselves are changing.

The traditional approach to climate adaptation often focused on projects. Build a flood barrier.

Strengthen a road.

Upgrade a drainage system.

Such measures remain important, but they are increasingly insufficient on their own. The scale and complexity of emerging climate risks require something broader: climate intelligence.
Climate intelligence refers to the continuous integration of environmental monitoring, predictive analytics, geospatial intelligence, infrastructure data, and risk modelling into decision-making processes. It enables governments to identify vulnerabilities, evaluate future scenarios, and prioritize investments based on evolving risk landscapes rather than historical assumptions.

In many respects, climate intelligence is becoming as important to homeland security as traditional intelligence is to national security. The countries that manage climate risk most effectively over the coming decades will not necessarily be those that spend the most on recovery. They will be those that understand risk earliest, anticipate change most accurately, and adapt most intelligently.

For India, this represents one of the most important strategic opportunities of the coming decade. The integration of space technologies into climate resilience planning offers the possibility of moving beyond reactive disaster management toward a model of anticipatory governance. In an era where environmental change is increasingly shaping economic and social outcomes, such capabilities may prove indispensable to national resilience.

Yet even the most sophisticated intelligence systems become ineffective if communication breaks down during a crisis. Understanding risk is essential, but acting on that understanding requires connectivity. The next pillar of homeland security therefore lies in ensuring that communication survives when everything else fails.



The Last Network Standing: Space Communications and Continuity of Governance

Most discussions on emergency communications focus on connectivity. They examine bandwidth, coverage, terminals, networks, and technologies that enable communication during disasters. While these considerations are important, they often overlook a more fundamental reality.

Every major crisis is ultimately a governance crisis. Natural disasters, civil disturbances, infrastructure failures, terrorist incidents, cyber attacks, and humanitarian emergencies rarely become catastrophic because governments lack information. They become catastrophic when governments lose the ability to communicate, coordinate, and direct response efforts across multiple institutions simultaneously.

The ability of the state to function during disruption depends upon the ability of decision-makers, emergency responders, military units, police forces, district administrations, infrastructure operators, and public service providers to remain connected. Once communication collapses, situational awareness deteriorates, coordination slows, resource allocation becomes inefficient, and public confidence begins to erode. The strategic value of space communications therefore extends far beyond connectivity. It lies in preserving continuity of governance under conditions where conventional systems fail.

The Fragility of Terrestrial Networks

Modern societies have become deeply dependent upon terrestrial communications infrastructure. Mobile towers, fibre-optic networks, data centres, power systems, and internet exchanges collectively form the backbone of contemporary governance and economic activity. Yet these systems are far more fragile than commonly assumed.

Recent crises across the world have repeatedly demonstrated this vulnerability. During major earthquakes, communication towers are damaged or lose power. Floods disrupt fibre-optic infrastructure. Wildfires destroy transmission corridors. Landslides sever connectivity across entire regions. Civil unrest can overwhelm networks or render them inaccessible. Even relatively localized disruptions can create information blackouts affecting large populations.

The challenge is not merely technological. Modern governance increasingly relies on digital connectivity for almost every function. Emergency response coordination, disaster management platforms, health systems, transportation networks, law enforcement databases, financial services, and public communication mechanisms all depend upon uninterrupted information flows.

Communication as Strategic Resilience

Historically, governments viewed communications infrastructure primarily as a utility. The emerging security environment suggests a different perspective.Communications increasingly function as strategic resilience infrastructure.

The distinction is important. A road can be damaged and repaired. A bridge can be rebuilt. Power systems can often be restored progressively. Communication failures, however, have immediate system-wide consequences because they impair decision-making itself. Without communication, authorities cannot effectively assess conditions, deploy resources, coordinate agencies, or communicate with affected populations.

Future homeland security architectures must therefore prioritize communication continuity with the same seriousness traditionally reserved for physical infrastructure protection. This principle is increasingly reflected in advanced national resilience strategies worldwide. Governments are moving away from viewing satellite communications as backup systems and toward treating them as integral components of national continuity architectures.

The question is no longer whether satellites should support emergency communications. The question is whether emergency communications should be designed around space-enabled resilience from the outset.

The Emergence of Multi-Orbit Resilience

One of the most important developments in satellite communications is the emergence of multi-orbitarchitectures. Traditionally, emergency communications relied primarily on geostationary satellites. These systems provided reliable coverage but often involved trade-offs relating to latency, mobility, and operational flexibility.
The contemporary environment is increasingly characterized by integration. Low Earth Orbit constellations provide low-latency connectivity and rapid deployment. Medium Earth Orbit systems contribute broader regional coverage and resilience. Geostationary satellites continue to provide wide-area communications and strategic continuity. Together, these architectures create a layered communications ecosystem capable of maintaining connectivity under a wide range of operating conditions.

The significance of this shift extends beyond technical performance. Multi-orbit systems reduce dependence on any single network architecture. They create redundancy, improve survivability, and enhance operational flexibility during crises. More importantly, they enable governments to maintain communications even when portions of the broader network environment become degraded or unavailable.
109

In resilience planning, redundancy is often viewed as a cost. In homeland security, redundancy is increasingly becoming a necessity.

The Future of Mobile Governance

A second transformation is equally significant. Historically, emergency operations were organized around fixed command centres. Coordination occurred from dedicated facilities connected to established infrastructure. This model worked reasonably well when crises were geographically contained and infrastructure remained largely intact.

Future emergencies are likely to be different. Extreme weather events, climate-induced disasters, and complex emergencies increasingly affect large geographic areas simultaneously. Critical infrastructure may be damaged. Access routes may become inaccessible. Populations may be displaced rapidly. Under such conditions, command and control systems must become far

more mobile.

This is driving the emergence of deployable communications architectures. Portable satellite terminals, vehicle-mounted command systems, rapidly deployable connectivity platforms, and mobile operations centres are enabling authorities to establish communications networks wherever they are needed. The objective is not merely restoring connectivity. It is enabling governance to move with the crisis.

This represents a subtle but important shift. Traditionally, governments brought affected populations back into functioning administrative systems. Future resilience models increasingly bring administrative capability directly to affected populations.

Continuity of Governance as a Strategic Capability

The deeper lesson emerging from recent disasters, conflicts, and crises is that resilience depends less on preventing disruption and more on maintaining functionality despite disruption.

No society can eliminate risk entirely.

Disasters will occur.

Infrastructure will fail.

Unexpected events will emerge.

The true measure of resilience lies in whether institutions can continue functioning when such disruptions occur. Space communications play a unique role in this context because they operate independently of many vulnerabilities affecting terrestrial networks. They provide continuity when conventional systems are damaged, degraded, or unavailable. More importantly, they enable governments to maintain situational awareness, preserve command structures, coordinate responses, and communicate with citizens under the most challenging conditions.

In an era where information has become as important as physical infrastructure, communications resilience is increasingly becoming governance resilience. The future of homeland security will therefore depend not only on the ability to manage crises, but on the ability to remain connected throughout them. Nations that preserve connectivity preserve decision-making. Nations that preserve decision-making preserve governance itself.

The next challenge extends beyond communication. Even when governments can see risks and remain connected, they must still confront a growing category of threats that operate across vast geographies, exploit administrative blind spots, and often remain invisible until significant damage has already occurred. Addressing such challenges requires persistent observation at national scale a capability that is redefining the future of internal security.

Invisible Threats in Visible Territory: Persistent Monitoring of Internal Security Risks

Traditional security thinking is heavily influenced by the concept of borders. Threats are often imagined as originating outside national territory and moving inward. Military planning, border management, and conventional security architectures have therefore focused on detecting, deterring, and responding to external actors.

The internal security environment of the twenty-first century is fundamentally different. Many of the most consequential threats confronting modern states do not originate beyond borders. They emerge within borders. They exploit geography, governance gaps, infrastructure corridors, environmental vulnerabilities, and the sheer complexity of national territory. They rarely appear as singular events. Instead, they manifest as networks operating across multiple locations simultaneously, often remaining undetected until their cumulative impact becomes significant.

The Rise of Networked Threats

One of the defining characteristics of contemporary internal security challenges is their networked nature. Unlike conventional threats, which often possess clear geographic origins and identifiable actors, modern illicit activities operate through distributed ecosystems. Logistics chains, financial transactions, transportation networks, communications systems, and geographic mobility are integrated into sophisticated operational structures capable of adapting rapidly to enforcement actions.

Narcotics trafficking provides a powerful example. International assessments indicate that maritime routes have become one of the primary channels for large-scale narcotics movement globally. The Indian Ocean region is increasingly emerging as a critical transit zone connecting production centres, trafficking networks, and consumer markets. These routes often extend across multiple jurisdictions, involve legitimate commercial activity as cover, and exploit the vastness of maritime spaces to avoid detection.

The challenge is not simply tracking individual shipments. It is identifying recurring patterns across thousands of seemingly unrelated activities. Space-based monitoring is uniquely suited to this task because it provides continuity. Unlike traditional patrol-based systems, satellites observe the same areas repeatedly over extended periods, allowing analysts to identify anomalies, behavioural changes, and recurring trends that would otherwise remain invisible.

The Geography of Illicit Economies

A second challenge lies in understanding how geography itself shapes criminal activity. Illegal mining, timber smuggling, environmental crime, unauthorized construction, resource theft, and land encroachment often occur in remote regions where state presence is limited. These activities are frequently treated as isolated enforcement issues. In reality, many form part of broader economic ecosystems that generate substantial financial flows while degrading environmental and institutional resilience.

The global scale of environmental crime illustrates the significance of this challenge. International organizations estimate that environmental crime now ranks among the world's largest illicit economies, generating hundreds of billions of dollars annually through activities such as illegal logging, mining, wildlife trafficking, and resource exploitation.

For India, the implications extend beyond environmental protection. Illegal extraction activities affect infrastructure projects, transportation corridors, watershed systems, forest ecosystems, and local governance structures. They often intersect with organized criminal networks and exploit precisely those geographic areas where monitoring remains difficult.

This is where space-based monitoring provides a strategic advantage. Changes in land use, vegetation cover, excavation patterns, transportation activity, and infrastructure development can be detected over time. Rather than focusing solely on individual violations, authorities gain the ability to understand how entire illicit ecosystems evolve geographically.

The Low-Altitude Security Challenge

The rapid proliferation of unmanned systems is introducing another dimension to internal security. Historically, national surveillance architectures focused primarily on the ground, the sea, and higher-altitude airspace. The emergence of affordable drones is creating an entirely new operating environment.

Drones are increasingly being used for smuggling, reconnaissance, contraband delivery, illegal surveillance, infrastructure monitoring, and a growing range of illicit activities. Their low cost, accessibility, and operational flexibility make them attractive tools for both criminal and non-state actors.

The challenge is not simply detecting individual drones. It is understanding the broader activity patterns associated with their use.

Space-enabled monitoring, combined with terrestrial sensors, geospatial analytics, and AI-driven pattern recognition, can contribute to identifying launch locations, recurring routes, operational hotspots, and supporting infrastructure. This shifts the focus from intercepting individual incidents to disrupting entire networks.

Persistent Visibility as a Security Multiplier

The traditional model of internal security relied heavily on patrols, checkpoints, inspections, and localized enforcement activities. These approaches remain essential, but they face growing limitations in environments characterized by scale, complexity, and rapidly evolving threats.

The future model increasingly revolves around persistent visibility. Persistent visibility refers to the ability to observe territory continuously rather than intermittently. It enables authorities to move beyond incident reporting and toward pattern recognition. The objective is not simply to know what happened. It is to understand what is changing.

This capability is particularly valuable because most internal security threats develop gradually. Smuggling routes become established over time. Illegal settlements expand incrementally. Resource theft follows predictable patterns. Environmental degradation accumulates progressively. Early indicators often exist long before enforcement agencies become aware of the problem. Space systems provide the continuity necessary to identify these indicators.

From Monitoring to Anticipation

The deeper significance of these developments lies in their impact on decision-making. Historically, security agencies have been judged by how effectively they respond to incidents. Increasingly, success may be measured by the ability to prevent incidents altogether.

This requires moving beyond surveillance toward anticipation. The integration of Earth observation, geospatial intelligence, artificial intelligence, and predictive analytics is creating conditions in which authorities can identify emerging risks before they fully materialize. Instead of reacting to illegal activities after they have become established, governments can intervene during their formative stages.

The strategic advantage is substantial. States that understand territorial patterns earlier can allocate resources more effectively, target enforcement more precisely, and reduce the costs associated with prolonged intervention. Internal security becomes less about managing consequences and more about shaping outcomes.

The future of homeland security will therefore depend not only on the ability to monitor territory, but on the ability to interpret the hidden patterns operating within it. In an increasingly complex security environment, the greatest threats may not be those that are difficult to see. They may be those that are visible every day but remain insufficiently understood.

The next frontier extends even further. Beyond security and risk management lies a more profound transformation—the use of space-enabled intelligence not merely to protect society, but to govern it more effectively. This evolution is beginning to reshape how states manage land, infrastructure, public assets, cities, and citizens themselves.



The Geography of Governance: Space as Public Infrastructure

For most of modern history, governments have relied upon administrative systems designed for an analogue world. Land records were maintained through physical surveys. Infrastructure inventories were updated periodically. Urban planning depended on manual inspections. Public assets were managed through fragmented databases. Decision-making was often constrained by incomplete information, delayed reporting cycles, and limited visibility across large geographic areas.

These systems were sufficient when economies moved slowly and infrastructure developed incrementally. The twenty-first century presents a fundamentally different challenge.

Governments today are responsible for managing increasingly complex physical systems: expanding cities, transportation corridors, energy networks, water infrastructure, industrial zones, logistics chains, digital infrastructure, environmental assets, and public services that operate continuously across vast territories. The scale, speed, and interconnectedness of these systems are exposing the limitations of traditional governance models. The result is a growing realization that space is no longer simply a strategic capability. It is becoming governance infrastructure. Just as roads enabled mobility, electricity enabled industrialization, and telecommunications enabled connectivity, geospatial intelligence is increasingly enabling effective governance.

The Future of Land Intelligence

Few governance challenges illustrate this transformation more clearly than land management. Land remains one of the most valuable and contested resources in any society. Infrastructure development, industrial expansion, urban growth, environmental protection, agricultural productivity, taxation systems, and property rights all depend upon accurate understanding of land.

Yet land administration systems across much of the world continue to suffer from fragmentation, outdated records, overlapping claims, encroachments, and limited visibility into changing ground realities.

I

ndia is no exception. Land-related disputes account for a substantial proportion of civil litigation and frequently delay infrastructure projects, industrial investments, and public works. The economic impact extends far beyond the legal system. Delays in land acquisition, disputes over ownership, and uncertainty regarding boundaries often increase project costs and slow national development.

Space-based geospatial intelligence is beginning to change this equation. High-resolution imagery, change detection analytics,

digital cadastral integration, and geospatial verification systems can create continuously updated records of physical territory. Instead of relying exclusively on periodic surveys, governments can increasingly monitor land-use changes, encroachments, unauthorized development, and environmental degradation in near real time.
The strategic significance is not merely administrative efficiency. It is the creation of a trusted territorial baseline upon which economic growth, infrastructure development, and public policy can operate.

Managing Public Assets at National Scale

- Modern governments oversee millions of physical assets.
- Roads.
- Railways.
- Power transmission networks.
- Water systems.
- Government buildings.
- Ports.
- Airports.
- Schools.
- Hospitals.
- Telecommunications infrastructure.

Historically, these assets have been managed through sector-specific systems that often operate independently of one another. The result is fragmented visibility and uneven situational awareness.

The emergence of geospatial governance offers a different model. By integrating infrastructure datasets with Earth observation systems, governments can create dynamic asset-management architectures capable of monitoring conditions continuously. Infrastructure health, maintenance requirements, environmental exposure, operational performance, and emerging vulnerabilities can be assessed through a common geographic framework.

The implications for resilience are significant. Instead of responding to failures after they occur, governments gain the ability to identify vulnerabilities before disruption takes place. Maintenance becomes predictive rather than reactive. Resource allocation becomes data-driven rather than assumption-driven. The state moves from managing assets to managing asset intelligence.

Urban Governance in an Era of Complexity

The world's population crossed a historic threshold in 2007 when more people began living in cities than in rural areas. By 2050, nearly 70 percent of humanity is expected to reside in urban areas.

India is experiencing this transformation at enormous scale. Urban centres are becoming engines of economic growth, innovation, and investment. At the same time, they are becoming increasingly complex environments characterized by congestion, infrastructure stress, environmental pressures, and rising service demands.

Traditional urban governance struggles to cope with this complexity because cities change faster than administrative systems can often track.

- Informal settlements emerge rapidly.
- Transportation patterns evolve continuously.
- Construction activity transforms neighbourhoods.
- Utility demand fluctuates dynamically.
- Environmental conditions shift seasonally.
- Space-enabled intelligence offers governments the ability to observe these changes continuously.

Future smart cities will likely rely less on isolated sensors and more on integrated geospatial operating systems capable of combining mobility data, infrastructure information, environmental monitoring, demographic trends, and service delivery metrics into a unified urban intelligence platform. The objective is not simply efficiency. It is creating cities capable of adapting to change in real time.

Conclusion: From Response to Resilience

For much of modern history, homeland security was built around response. Governments focused on managing disasters, restoring services, and recovering from disruptions after they occurred. The emerging risk environment demands a different approach.

Climate change, infrastructure stress, urban complexity, environmental degradation, transnational crime, and evolving public safety challenges are creating risks that are increasingly interconnected and difficult to manage through reactive systems alone. The strategic advantage of the future will lie not in responding faster, but in anticipating earlier.

S

pace technologies are central to this transition. They provide governments with the ability to observe territory continuously, identify emerging vulnerabilities, maintain connectivity during crises, and make decisions based on real-time intelligence rather than delayed information. In doing so, they are transforming homeland security from an operational function into a predictive capability.

More importantly, space is evolving beyond a specialised technology domain to become a foundational layer of governance. Disaster management, infrastructure resilience, public safety, environmental monitoring, emergency communications, and territorial administration are all becoming increasingly dependent on space-enabled intelligence and connectivity.

For India, the opportunity is clear. The integration of space, geospatial intelligence, digital infrastructure, and governance systems can create a new model of national resilience—one that is proactive rather than reactive, predictive rather than responsive, and capable of managing complexity at national scale.

Ultimately, the future of homeland security will not be determined solely by the ability to protect territory. It will be determined by the ability to understand territory continuously, anticipate risks intelligently, and sustain governance through disruption. In that future, space will not simply support resilience—it will help define it.

Strategic Priorities for the Next Decade

- **Building India's National Resilience Architecture**

The coming decade will witness a fundamental shift in how nations approach homeland security, civil defence, and public resilience. The most effective governments will not necessarily be those that possess the largest response forces or the highest disaster-relief budgets. They will be those capable of anticipating risk earlier, maintaining situational awareness longer, coordinating action faster, and restoring normalcy more rapidly. Space-enabled capabilities will increasingly form the backbone of this transformation.

- **Establishing a National Digital Twin of Critical Infrastructure**

India's infrastructure footprint is expanding at an unprecedented scale through highways, railways, logistics corridors, ports, airports, power networks, industrial zones, and digital infrastructure. Managing these assets through fragmented databases and periodic inspections will become increasingly difficult. A long-term strategic priority should be the creation of a continuously updated national geospatial infrastructure layer that provides decision-makers with real-time visibility into the condition, utilization, and vulnerability of critical national assets. Such a capability would strengthen planning, maintenance, resilience, and crisis response simultaneously.

- **Creating a Climate Security Intelligence Framework**

Climate risks are becoming increasingly intertwined with national resilience. Floods, heatwaves, glacial instability, coastal erosion, water stress, and extreme weather events are no longer isolated environmental concerns but factors influencing economic activity, infrastructure performance, public safety, and regional stability. India should progressively integrate satellite observations, climate models, hydrological intelligence, and infrastructure risk assessments into a unified climate-security architecture capable of supporting long-term strategic planning.

- **Ensuring Universal Emergency Connectivity**

Recent crises around the world have demonstrated that communication failures often become force multipliers during emergencies. A resilient homeland security architecture requires communications systems that remain operational even when terrestrial infrastructure is damaged or unavailable. Developing a nationwide framework for emergency satellite communications, deployable connectivity systems, and multi-orbit communications resilience should become a central pillar of civil defence planning

- **Institutionalising Persistent National Monitoring**

Many internal security challenges develop gradually before becoming visible to authorities. Illegal mining, environmental crime, coastal infiltration, encroachment, trafficking networks, infrastructure degradation, and emerging vulnerabilities often exhibit detectable patterns long before they become major problems. Future homeland security frameworks should increasingly emphasize persistent monitoring and predictive intelligence rather than episodic observation and reactive intervention.

- **Institutionalising Persistent National Monitoring**

Many internal security challenges develop gradually before becoming visible to authorities. Illegal mining, environmental crime, coastal infiltration, encroachment, trafficking networks, infrastructure degradation, and emerging vulnerabilities often exhibit detectable patterns long before they become major problems. Future homeland

security frameworks should increasingly emphasize persistent monitoring and predictive intelligence rather than episodic observation and reactive intervention.

- **Integrating Space into Governance Platforms**

Space-enabled intelligence should not remain confined to specialist agencies. Its greatest value emerges when integrated into governance systems used by administrators, emergency responders, infrastructure operators, urban planners, and public safety institutions. The next decade should focus on embedding geospatial intelligence into routine governance processes so that it becomes part of everyday decision-making rather than an exceptional capability used only during crises.

- **Building a National Geospatial Workforce**

Technology alone cannot create resilience. The effective use of geospatial intelligence requires skilled personnel capable of interpreting data, integrating information, and translating insights into operational decisions. India will require a much larger cadre of geospatial analysts, climate-risk specialists, emergency management professionals, infrastructure intelligence experts, and public-sector decision-makers trained to operate within increasingly data-driven governance environments.

- **Positioning Space as Critical National Infrastructure**

Perhaps the most important strategic shift will be conceptual rather than technological. Space systems should increasingly be viewed not as isolated assets serving specific missions, but as foundational infrastructure supporting governance, public safety, economic resilience, and national security. Just as electricity, transportation networks, and telecommunications became indispensable components of modern states, space-enabled intelligence and connectivity are becoming essential elements of national resilience architecture.

This transition will define the next phase of India's homeland security evolution. The objective is no longer merely to respond effectively when crises occur. It is to build a nation capable of anticipating disruption, maintaining continuity, and adapting to an increasingly complex risk environment.



GEOSPATIAL INTELLIGENCE, AI AND DECISION SUPERIORITY

Introduction: From Information Dominance to Decision Dominance

For much of the Information Age, military modernization was driven by a single objective: information superiority. The assumption was straightforward. The side possessing more sensors, more intelligence sources, more surveillance platforms, and greater access to information would enjoy a decisive battlefield advantage. This assumption shaped military investments for over three decades, driving the proliferation of satellites, airborne surveillance systems, unmanned platforms, electronic intelligence capabilities, and network-centric warfare architectures.

The results have been extraordinary. Modern militaries today possess access to more information than at any point in human history. Hundreds of Earth observation satellites continuously image the planet. Unmanned systems generate persistent streams of video and telemetry. Ground sensors monitor vast areas in real time. Communications networks connect forces across multiple domains. Open-source intelligence, social media activity, commercial imagery, cyber intelligence, and electronic emissions contribute additional layers of information. The battlespace has become saturated with sensors.

Yet paradoxically, information abundance has created a new problem. The challenge confronting modern militaries is no longer information scarcity. It is information overload.

Recent conflicts have demonstrated that commanders are increasingly overwhelmed by the volume of data available to them. Intelligence organizations routinely collect more information than they can process, analyse, or exploit. During the DEFSAT discussion, one example highlighted that intelligence organizations often leave a substantial proportion of collected imagery and sensor data unanalysed simply because human analysts cannot keep pace with collection rates. The consequence is a growing gap between information collection and decision-making.

This gap is becoming strategically significant. Modern warfare is increasingly defined by speed. The side capable of detecting, understanding, and responding faster gains a disproportionate advantage. The OODA Loop—Observe, Orient, Decide, Act—remains relevant, but advances in artificial intelligence, automation, and geospatial intelligence are fundamentally compressing each stage of the cycle. Future conflicts

will not necessarily be won by those possessing the most information. They will increasingly be won by those capable of converting information into decisions faster than their adversaries.

This is where geospatial intelligence and artificial intelligence are emerging as transformative technologies. Historically, geospatial intelligence was viewed primarily as a support function. Maps, imagery interpretation, terrain analysis, and reconnaissance products helped commanders understand the physical battlespace. Today, geospatial intelligence is evolving into something far more consequential. It is becoming the integration layer through which information from satellites, drones, sensors, communications systems, cyber platforms, and intelligence networks can be fused into a coherent operational picture. In many respects, geospatial platforms are becoming the operating systems of modern warfare.

Artificial intelligence is accelerating this transformation. AI is increasingly being used to detect objects, identify patterns, update maps, prioritize intelligence, generate alerts, recommend courses of action, and support operational planning. While human judgement remains indispensable, AI is rapidly becoming a force multiplier that enables military organizations to process information at machine speed while preserving human control over critical decisions.

For India, these developments carry profound strategic implications. Future conflicts are likely to involve contested electromagnetic environments, degraded communications, autonomous systems, distributed operations, and unprecedented volumes of multi-domain data. Success will depend not only on acquiring advanced platforms but also on developing the ability to integrate sensors, fuse intelligence, generate trust in data, and support decision-making across the entire force structure.

The future battlespace will therefore be shaped by a new form of competition. Not competition for information. Competition for decision superiority.

The End of the Kill Chain: Why Mosaic Warfare is Reshaping Military Operations

For more than a century, military organizations have largely been built around platforms. Aircraft carriers projected naval power. Fighter aircraft dominated air operations. Tanks shaped land warfare. Strategic bombers, missile systems, radar networks, and surveillance platforms each performed specialized functions within relatively structured force architectures. These platforms became increasingly capable, increasingly sophisticated, and increasingly expensive.

The logic behind this approach was understandable. Superior platforms generated superior military capability. However, the strategic environment is changing in ways that challenge this assumption.

The emergence of precision-guided weapons, long-range surveillance systems, commercial satellite imagery, autonomous systems, and ubiquitous connectivity has dramatically increased the vulnerability of large military assets. Platforms that once operated with relative freedom can now be detected, tracked, targeted, and engaged with increasing precision. At the same time, the cost of building and sustaining these platforms continues to rise, creating concerns about affordability, survivability, and operational flexibility.

It was against this backdrop that DARPA introduced the concept of Mosaic Warfare around 2017–2019, a framework that featured prominently in the DEFSAT discussion. The central idea was deceptively simple: rather than relying on a small number of highly capable and highly vulnerable platforms, future military capability could be generated through large numbers of smaller, distributed, interconnected systems that could be assembled dynamically according to operational requirements.

From Kill Chains to Kill Webs

One of the most significant implications of Mosaic Warfare is the transition from kill chains to kill webs. Traditional military operations are often structured around linear processes. A target is detected, identified, tracked, engaged, and assessed through a sequence of interconnected actions. These processes form what is commonly known as a kill chain.

While effective, kill chains possess an inherent vulnerability. If a critical link is disrupted, the chain can fail. Communications may be interrupted. A sensor may be destroyed. Targeting data may become unavailable. A command node may be degraded. The effectiveness of the entire
system can be compromised.

Mosaic Warfare seeks to overcome this limitation by replacing linear architectures with networked architectures. Instead of a single path connecting sensors, decision-makers, and shooters, multiple pathways exist simultaneously. Sensors can support multiple weapon systems. Communications can be routed through alternative nodes. Intelligence can be generated from multiple sources. Decision-making can occur across distributed networks.

The result is a kill web rather than a kill chain. In such architectures, the loss of individual nodes reduces efficiency but does not necessarily result in mission failure. The network adapts, reroutes, and continues functioning despite disruption.
The significance of this shift cannot be overstated. Future warfare is increasingly becoming a contest between resilient networks rather than individual platforms.

Lessons from Contemporary Conflict

Recent conflicts have accelerated interest in distributed operational concepts. The conflict in Ukraine has demonstrated the power of integrating commercial satellite imagery, drones, electronic warfare systems, mobile communications, open-source intelligence, and precision strike capabilities into highly adaptive operational networks. Small, inexpensive systems have repeatedly generated effects disproportionate to their cost. Tactical units have gained access to intelligence capabilities previously reserved for strategic headquarters. Commercial technologies have increasingly become components of military kill webs.

A similar trend is visible across maritime and Indo-Pacific theatres. The proliferation of autonomous surface vessels, unmanned aerial systems, distributed sensor networks, and proliferated satellite constellations is reducing dependence on a limited number of high-value assets. Military planners increasingly recognize that survivability may depend less on protecting individual platforms and more on ensuring that the overall network remains functional.

This has significant implications for force development. The future military advantage may not belong exclusively to the force possessing the most advanced platforms. It may belong to the force possessing the most adaptable architecture.

The Strategic Role of Geospatial Intelligence

The challenge, however, lies in making such architectures function. A distributed force generates enormous volumes of information. Satellites produce imagery. Drones generate video feeds. Ground sensors report activity. Electronic intelligence systems collect emissions. Human intelligence contributes observations. Communications networks transmit status information continuously.

Without integration, these data streams become



Swimming in Sensors, Drowning in Data: The Intelligence Bottleneck of Modern Warfare

The defining challenge of modern military intelligence is no longer collection. It is comprehension. For decades, military organizations invested heavily in overcoming information scarcity. Satellites were launched to expand surveillance coverage. Airborne ISR platforms were deployed to observe hostile activity. Electronic intelligence systems monitored adversary communications. Unmanned systems extended reconnaissance capabilities deep into contested environments. The objective was simple: collect more information than the adversary.

Today, that objective has largely been achieved. The contemporary battlefield is saturated with sensors. Military satellites generate terabytes of imagery every day. Synthetic Aperture Radar constellations can observe targets regardless of weather or daylight conditions. UAVs provide persistent video feeds across operational theatres. Ground sensors monitor movement, emissions, and environmental conditions. Naval platforms generate maritime awareness data continuously. Open-source intelligence, social media activity, cyber intelligence, and commercial satellite imagery contribute additional layers of information.
The result is unprecedented visibility. Paradoxically, it is also creating unprecedented blindness. The fundamental problem is that collection capabilities are growing faster than analytical capabilities. Modern militaries increasingly possess the ability to collect enormous quantities of data but often struggle to convert that data into actionable intelligence within operationally relevant timelines. Intelligence organizations are finding themselves overwhelmed not by the absence of information, but by its abundance. This is rapidly emerging as one of the most important strategic challenges in defence planning.

The Collection-Analysis Gap

Historically, intelligence operations were constrained by limited collection opportunities. Analysts competed for scarce imagery, limited reconnaissance assets, and restricted surveillance windows. The challenge was obtaining information.

Today, the challenge is determining which information actually matters. A modern operational theatre may generate millions of observations every day. Vehicles move across road networks. Ships alter course. Aircraft change flight profiles. Communications systems emit signals. Infrastructure evolves. Personnel movements occur continuously. Satellites, drones, and sensors capture these activities at extraordinary scale.

Yet only a fraction of these observations possess operational significance. The strategic challenge lies in distinguishing signal from noise. This challenge is becoming increasingly acute as proliferated



constellations expand. A decade ago, military planners were concerned about insufficient observation. Today, they are increasingly concerned about excessive observation. Every additional sensor improves visibility while simultaneously increasing analytical burden.

The result is what many intelligence professionals describe as the collection-analysis gap: the widening disconnect between the volume of information collected and the volume that can be meaningfully exploited.

The Age of Persistent Surveillance

The emergence of persistent surveillance architectures is accelerating this trend. Traditional ISR missions operated through periodic collection. Satellites revisited targets at intervals. Reconnaissance aircraft flew scheduled missions. Intelligence updates occurred in defined cycles. Analysts had time to process information before the next collection event.

Persistent surveillance changes this dynamic entirely. Modern constellations provide continuous monitoring across vast areas. Drone swarms generate uninterrupted video streams. Maritime tracking systems monitor vessel activity in near real time. Electronic intelligence platforms continuously collect emissions data. Information no longer arrives in batches. It arrives continuously.

The implication is profound. Military organizations are transitioning from episodic intelligence environments to perpetual intelligence environments. In such conditions, traditional analytical workflows become increasingly unsustainable. Human analysts simply cannot review every image, monitor every sensor feed, or assess every anomaly manually. The volume of information exceeds human capacity.

The future therefore requires a different approach

AI as an Intelligence Filter

Artificial intelligence is often described as an intelligence generator. Its more immediate role may be far more practical. AI is becoming an intelligence filter. The primary value of AI lies not in producing intelligence independently but in helping analysts determine where to focus their attention. Automated systems can identify changes in imagery, detect unusual movement patterns, recognize objects, classify activity, prioritize alerts, and highlight anomalies requiring human review.

This dramatically alters the intelligence workflow. Instead of searching for information manually, analysts increasingly evaluate information pre-selected by intelligent systems. The role of the human shifts from collector to interpreter.

The Race Against Latency

Military discussions often focus on accuracy. Future conflicts may be equally influenced by latency. An intelligence product that arrives six hours late may be perfectly accurate and strategically irrelevant. A target may have moved. Conditions may have changed. Opportunities may have disappeared.

The challenge is therefore not simply generating intelligence. It is generating intelligence before decisions must be made. This places enormous pressure on intelligence architectures.

Every stage introduces delay:

- Collection.
- Transmission.
- Processing.
- Analysis.
- Validation.
- Dissemination.
- Decision-making.

Future military effectiveness will increasingly depend on compressing this timeline. The side capable of transforming raw observations into actionable understanding fastest gains a disproportionate operational advantage. This is where geospatial intelligence and artificial intelligence become inseparable. GEOINT provides the common operational picture. AI accelerates the transformation of data into insight. Together, they create the foundation for decision superiority.

Yet even perfect intelligence remains ineffective if it exists in isolation. Information must be integrated across platforms, services, sensors, and domains. The future challenge is therefore not merely analysing information faster, but creating a common framework through which information itself can be understood.

The Geospatial Operating System: Building a Single Source of Truth for the Battlefield

Military organizations have traditionally operated through specialized information systems.

- Air forces maintained air pictures.
- Navies maintained maritime pictures.
- Armies maintained ground intelligence.
- Intelligence agencies developed separate databases.
- Satellite operators managed independent imagery repositories.
- Each system was optimized for its specific mission.

While effective in an earlier era, such structures are becoming increasingly incompatible with modern warfare. Contemporary military operations unfold simultaneously across land, sea, air, cyber, electromagnetic, and space domains. Decisions made in one domain often produce immediate consequences in another. A satellite identifies a target. A drone confirms activity. An electronic intelligence system detects emissions.

A cyber operation disrupts communications. A precision weapon engages the objective.

The challenge is not collecting information from these domains. The challenge is integrating them.Future warfare demands a common understanding of the battlespace.



The Problem of Fragmented Intelligence

Different organizations often collect valuable intelligence but store, process, and analyse it within separate systems. The result is fragmented awareness rather than integrated understanding.

This fragmentation creates operational inefficiencies. A satellite operator may observe activity without access to electronic intelligence confirming its significance. A drone operator may identify movement without access to historical geospatial patterns. A commander may receive multiple intelligence reports without a clear mechanism for reconciling conflicting information.

The problem is rarely a lack of data. The problem is a lack of integration. Modern conflicts increasingly demonstrate that information superiority is not determined by who owns the most sensors. It is determined by who can combine information from those sensors most effectively.

GIS Beyond Mapping

\

Many discussions still associate GIS primarily with mapping. That characterization is increasingly outdated. The future military GIS platform is evolving into something far more ambitious: a geospatial operating system.

Just as a smartphone operating system integrates applications, communications, sensors, and user interactions into a unified environment, future military geospatial platforms will integrate intelligence sources, operational data, planning tools, command systems, and decision-support capabilities into a single operational framework.

The commander no longer needs separate screens for:

- satellite imagery,
- drone feeds,
- radar tracks,
- electronic intelligence,
- logistics information,
- operational planning

Instead, all information becomes visible through a common geospatial layer. The map evolves into a decision environment

Building the Battlefield Digital Twin

The next evolution of military geospatial intelligence is the concept of the battlefield digital twin. In civilian applications, digital twins create virtual representations of cities, infrastructure networks, industrial facilities, and transportation systems. Similar concepts are increasingly being applied to military operations.

A battlefield digital twin integrates terrain data, infrastructure information, force dispositions, logistics networks, sensor feeds, environmental conditions, and intelligence assessments into a continuously updated representation of the operational environment.

This offers several advantages.

- Commanders gain greater situational awareness.
- Operational planning becomes more dynamic.
- Potential courses of action can be modelled before execution.
- Emerging risks can be identified earlier.

The battlespace becomes something that can be analysed continuously rather than simply observed periodically. The significance of this capability grows as operations become increasingly distributed and data intensive.

Creating a Single Source of Truth

Perhaps the most important objective of future geospatial architectures is the creation of what technology communities often describe as a single source of truth. Modern warfare frequently suffers from competing versions of reality.

- Different sensors produce different observations.
- Different agencies generate different assessments.
- Different commanders operate using different assumptions.

These inconsistencies create friction, delay, and uncertainty. The purpose of a geospatial operating system is not merely to display information. It is to create shared understanding.

Every participant should operate from the same operational picture, the same data environment, and the same geospatial foundation. This significantly improves coordination across services and domains. More importantly, it reduces decision friction. The future battlefield will reward organizations capable of achieving common understanding faster than their adversaries.

From Information Systems to Decision Systems

The ultimate significance of the geospatial operating system lies in its evolution beyond information management. Historically, military information systems stored data. Future systems will increasingly support decisions. Artificial intelligence, sensor fusion, predictive analytics, and geospatial intelligence are converging to create platforms capable of recommending priorities, identifying opportunities, highlighting risks, and supporting operational planning in near real time.

The role of GIS is therefore changing fundamentally. It is no longer a support tool for military operations. It is becoming the environment within which military operations are understood, coordinated, and directed. This transformation represents one of the most important developments in contemporary defence technology. The future battlefield will not be defined solely by platforms or weapons. It will be defined by the architectures that connect them.

And at the centre of those architectures sits a new actor—artificial intelligence—whose role is increasingly shifting from analytical support to operational decision assistance.

The Battle for Defence AI Sovereignty

The history of military power has often been defined by control over strategic technologies. In different eras, nations competed for access to steel production, shipbuilding capacity, aviation technology, nuclear expertise, microelectronics, and precision manufacturing. Each technological revolution altered the distribution of power by creating new dependencies and new forms of strategic advantage. The ongoing revolution in artificial intelligence and geospatial intelligence is no different. However, unlike previous eras where physical platforms dominated military capability, the decisive assets of the future may increasingly be software architectures, data ecosystems, algorithms, and decision-support systems.



This shift carries profound implications for national security. Modern military operations are becoming increasingly dependent on digital architectures that collect, process, analyse, and disseminate information across multiple domains. Satellite imagery, UAV feeds, electronic intelligence, logistics systems, operational planning tools, and command-and-control networks are all converging into integrated decision environments. As these systems become more intelligent and autonomous, the question facing militaries is no longer simply whether they possess advanced platforms. The more important question is whether they possess sovereign control over the software and data architectures that govern those platforms.

Historically, strategic autonomy was often measured through ownership of hardware. Nations sought to manufacture aircraft, ships, missiles, and sensors domestically to reduce dependence on external suppliers. While these concerns remain valid, the centre of gravity is shifting. Future military effectiveness will depend increasingly on who controls the operating systems, artificial intelligence models, geospatial platforms, cloud architectures, and analytical frameworks that transform data into operational decisions. Dependence in these domains can create vulnerabilities that are far less visible than traditional supply-chain dependencies but potentially far more consequential.

The global strategic environment is already reflecting this reality. The United States, China, Europe, and several Indo-Pacific nations are investing heavily in sovereign artificial intelligence ecosystems, secure cloud infrastructures, military data platforms, and indigenous software stacks. These investments are driven by a recognition that future military competition will be shaped not only by physical capabilities but also by control over digital decision architectures. The nation that owns the data architecture increasingly owns the decision architecture, and the nation that owns the decision architecture possesses a significant operational advantage.

For India, this challenge is particularly important because the country's future defence modernization will generate enormous volumes of geospatial and operational data.

The expansion of indigenous satellite constellations, UAV fleets, sensor networks, secure communications systems, and digital battlefield architectures will create one of the largest military data environments in the region. The strategic value of these investments will ultimately depend on India's ability to integrate, analyse, and exploit this information within sovereign frameworks. Reliance on externally controlled software ecosystems or opaque algorithms introduces risks that extend beyond procurement. It affects trust, security, operational flexibility, and long-term strategic independence.

The challenge becomes even more significant in the context of artificial intelligence. Modern AI systems learn from data, improve through use, and increasingly influence operational decisions. Yet many advanced AI models operate as black boxes whose internal logic is not always transparent. In commercial applications, this may be inconvenient. In military operations, it can become a strategic vulnerability. Commanders must understand not only the recommendations generated by AI systems but also the assumptions, data sources, confidence levels, and analytical processes underlying those recommendations. Explainability, transparency, and auditability are therefore becoming critical requirements for defence AI architectures.

The importance of trusted military data will continue to grow as future conflicts become increasingly contested in the information domain. Adversaries may attempt to manipulate datasets, corrupt training environments, spoof sensor inputs, or introduce false information into decision systems. The ability to verify, authenticate, and secure data will become as important as the ability to collect it. Consequently, sovereign AI architectures must be built not only around performance but also around trust. Secure data governance, indigenous algorithm development, cyber resilience, and multi-layer validation mechanisms will become essential components of future military capability.

The evolution of geospatial intelligence further reinforces this trend. GIS platforms are no longer simply repositories for maps and imagery. They are becoming operational environments where intelligence is fused, targets are identified, missions are planned, and commanders develop situational awareness. In effect, they are evolving into digital battle management systems. Control over these systems therefore carries strategic significance comparable to control over communications networks or surveillance infrastructure. The future battlefield will increasingly be managed through software-defined architectures, making ownership of those architectures a matter of national security.

Ultimately, defence AI sovereignty is not a technology issue alone. It is a strategic autonomy issue. Nations that fail to develop trusted, secure, and indigenous decision architectures risk becoming dependent on external systems for some of the most critical functions of military operations. Conversely, nations that successfully build sovereign geospatial intelligence ecosystems, indigenous AI capabilities, and secure military data infrastructures will possess far greater freedom of action in future conflicts.

As warfare becomes increasingly data-centric, sovereignty itself is being redefined. In the industrial age, sovereignty was linked to control over territory. In the information age, it became linked to control over networks. In the emerging era of artificial intelligence, sovereignty may increasingly depend on control over data, algorithms, and decision systems. The battle for defence AI sovereignty is therefore not a future challenge. It is already underway, and its outcome will shape the military balance of the coming decades.

The challenge becomes even more significant in the context of artificial intelligence. Modern AI systems learn from data, improve through use, and increasingly influence operational decisions. Yet many advanced AI models operate as black boxes whose internal logic is not always transparent. In commercial applications, this may be inconvenient. In military operations, it can become a strategic vulnerability. Commanders must understand not only the recommendations generated by AI systems but also the assumptions, data sources, confidence levels, and analytical processes underlying those recommendations. Explainability, transparency, and auditability are therefore becoming critical requirements for defence AI architectures.

The importance of trusted military data will continue to grow as future conflicts become increasingly contested in the information domain. Adversaries may attempt to manipulate datasets, corrupt training environments, spoof sensor inputs, or introduce false information into decision systems. The ability to verify, authenticate, and secure data will become as important as the ability to collect it. Consequently, sovereign AI architectures must be built not only around performance but also around trust. Secure data governance, indigenous algorithm development, cyber resilience, and multi-layer validation mechanisms will become essential components of future military capability.

The evolution of geospatial intelligence further reinforces this trend. GIS platforms are no longer simply repositories for maps and imagery. They are becoming operational environments where intelligence is fused, targets are identified, missions are planned, and commanders develop situational awareness. In effect, they are evolving into digital battle management systems. Control over these systems therefore carries strategic significance comparable to control over communications networks or surveillance infrastructure. The future battlefield will increasingly be managed through software-defined architectures, making ownership of those architectures a matter of national security.

Ultimately, defence AI sovereignty is not a technology issue alone. It is a strategic autonomy issue. Nations that fail to develop trusted, secure, and indigenous decision architectures risk becoming dependent on external systems for some of the most critical functions of military operations. Conversely, nations that successfully build sovereign geospatial intelligence ecosystems, indigenous AI capabilities, and secure military data infrastructures will possess far greater freedom of action in future conflicts.

As warfare becomes increasingly data-centric, sovereignty itself is being redefined. In the industrial age, sovereignty was linked to control over territory. In the information age, it became linked to control over networks. In the emerging era of artificial intelligence, sovereignty may increasingly depend on control over data, algorithms, and decision systems. The battle for defence AI sovereignty is therefore not a future challenge. It is already underway, and its outcome will shape the military balance of the coming decades.

Conclusion: Decision Superiority as the New High Ground

For much of military history, success was determined by mass. Nations with larger armies, greater industrial capacity, and superior firepower often possessed decisive advantages. The Information Age shifted this paradigm by making information a critical source of military power. Intelligence, surveillance, reconnaissance, and networked communications became central to operational effectiveness.

information scarcity. Modern militaries already possess access to unprecedented volumes of data generated by satellites, sensors, drones, communications networks, cyber systems, and intelligence platforms. The advantage increasingly lies not in collecting more information, but in transforming information into understanding and understanding into action faster than an adversary.

This is the essence of decision superiority. Geospatial intelligence and artificial intelligence sit at the centre of this transformation. Together, they are enabling militaries to fuse data across domains, create integrated operational pictures, identify patterns invisible to human analysts, compress decision cycles, and support commanders operating in increasingly complex and contested environments. The battlefield is evolving from a platform-centric construct into a data-centric ecosystem where speed of comprehension may matter as much as speed of manoeuvre.

At the same time, the chapter highlights that technology alone will not determine success. Future military advantage will depend equally on trusted data, resilient architectures, sovereign AI capabilities, interoperable systems, and effective human-machine collaboration. The objective is not to replace commanders with algorithms, but to empower commanders with better information, greater context, and faster decision support. For India, this transition represents both a challenge and an opportunity. The convergence of indigenous space capabilities, expanding geospatial infrastructure, growing AI expertise, and defence modernization initiatives provides the foundation for building a truly integrated decision-centric warfare architecture. Achieving this vision will require sustained investment not only in sensors and platforms, but also in software, data frameworks, analytics, and institutional integration.

Ultimately, every era of warfare has been defined by a strategic high ground. In previous centuries, that high ground was terrain. In the industrial age, it was production capacity. In the information age, it became access to information. In the emerging era of intelligent warfare, the new high ground is decision superiority.

The side that can sense faster, fuse better, understand earlier, and decide sooner will possess the decisive advantage. In that contest, geospatial intelligence and artificial intelligence are no

Strategic Priorities for the Next Decade

- **Building India's Decision-Centric Warfare Architecture**

The coming decade will witness a profound shift in military competition. The central challenge will no longer be acquiring additional sensors, collecting larger volumes of data, or deploying more platforms. Most modern militaries are already entering an era of information abundance. The decisive advantage will increasingly belong to those capable of transforming information into decisions faster, more accurately, and more consistently than their adversaries. For India, this transition requires a deliberate effort to build a decision-centric warfare architecture that integrates geospatial intelligence, artificial intelligence, secure communications, and operational command systems into a coherent national capability.

- **Establishing a National Defence GEOINT Cloud**

India's future military effectiveness will depend upon its ability to integrate information generated across satellites, UAVs, airborne sensors, naval platforms, ground forces, cyber systems, and intelligence agencies. These datasets currently exist across multiple organizations and operational environments. A national defence GEOINT cloud capable of securely aggregating, processing, and distributing geospatial intelligence would provide the foundation for real-time situational awareness across all services. Such an architecture would significantly reduce information silos and enable commanders to operate from a common operational picture.

- **Building a Multi-Sensor Fusion Architecture**

Future battlefields will increasingly be characterized by data saturation. The challenge will not be the absence of information but the ability to combine information from diverse sources into actionable intelligence. India should prioritize the development of multi-sensor fusion frameworks capable of integrating satellite imagery, synthetic aperture radar, UAV feeds, electronic intelligence, open-source intelligence, and battlefield sensors into unified intelligence products. The objective should be to move from platform-centric intelligence to network-centric understanding.

- **Developing Battlefield Digital Twins**

One of the most promising applications of geospatial intelligence is the creation of dynamic digital representations of operational environments. Battlefield digital twins can integrate terrain, infrastructure, force deployments, logistics networks, weather conditions, and intelligence assessments into continuously updated operational models. Such capabilities will support mission planning, course-of-action evaluation, logistics optimization, and operational simulation. Over time, digital twins are likely to become an essential component of military decision-support systems.

- **Accelerating Human-Machine Teaming**

Artificial intelligence should be viewed as an augmentation capability rather than a replacement for human decision-makers. Future command systems must be designed around human-machine teaming, where AI performs tasks involving pattern recognition, anomaly detection, intelligence prioritization, and predictive analysis, while commanders retain responsibility for judgement, context, and operational decisions. Building trust between operators and AI systems will be as important as improving algorithmic performance.

- **Creating Trusted Military Data Frameworks**

As military organizations become increasingly dependent on AI-enabled systems, data integrity will become a strategic requirement. India should establish robust frameworks for data validation, provenance tracking, confidence scoring, and multi-source verification. Future conflicts are likely to involve information manipulation, spoofing, deception, and data poisoning. Trusted data architectures will therefore become a critical component of operational resilience.

Roadmap for Building India's Future Space Security Architecture

STRATEGIC PILLAR	PRIORITY AREA	KEY ACTIONS	LEAD STAKEHOLDERS	STRATEGIC OUTCOME
1. National Strategy & Governance	National Space Power Strategy	• Develop an integrated framework aligning defence, civil, and commercial objectives.	PMO, NSCS, DoS, MoD	Whole-of-government space strategy
2. Space Security & Resilience	Critical Space Infrastructure Protection	• Implement national space cybersecurity standards, SSA integration, and resilience planning.	CERT-In, DSA, ISRO, IN-SPACe	Protected and resilient space architecture
3. Military Space Capability	Integrated Military Space Operations	• Strengthen military space governance, planning, integration of ISR, SATCOM, PNT, and decision support architectures.	MoD, IDS, DSA, Armed Forces	Enhanced operational effectiveness and deterrence
4. Persistent Space Presence	Multi-Orbit Constellations	• Build distributed LEO-MEO-GEO architectures with redundancy and mission assurance.	ISRO, Industry, DSA	Continuous operational capability
5. Launch Agility	Responsive Launch Capability	• Establish rapid launch and reconstitution frameworks for national security missions.	ISRO, IN-SPACe, Industry	Faster recovery and mission continuity
6. On-Orbit Sustainment	Servicing & Life Extension	• Develop indigenous capabilities for inspection, servicing, refuelling, refurbishing, and debris mitigation.	ISRO, Start-ups, Industry	Improved mission longevity and resilience
7. GEOINT & AI	Decision Superiority Ecosystem	• Build AI-enabled geospatial intelligence and AI-assisted decision-support systems.	MoD, ISRO, Industry, Academia	Faster and better decision-making
8. Innovation Ecosystem	Defence-Space Industrial Base	• Expand indigenous manufacturing, support start-ups, strategic supply chains, and dual-use technology development.	IN-SPACe, Industry, DPIIT	Strategic autonomy and industrial depth
9. Procurement Reform	Service-Based Acquisition Models	• Shift from hardware procurement to capability and service procurement models.	MoD, Services, Industry	Faster adoption of innovation

ENABLER	EMERGING FOCUS AREA	KEY ACTIONS	LEAD STAKEHOLDERS	STRATEGIC OUTCOME
Innovation & Start-ups	Emerging Technology Acceleration	• Scale AI, quantum, advanced materials, robotics, and autonomous systems to create specialized solutions.	Start-ups, Academia, Industry	Future-ready technology ecosystem
Talent & Workforce	National Space Talent Mission	• Create specialized programs in GEOINT, AI, SSA, cyber, launch operations, and space policy.	Academia, ISRO, MoD	Skilled workforce pipeline
Homeland Security	Space for National Resilience	• Integrate space capabilities into disaster response, border management, and critical infrastructure protection.	MHA, NDMA, States, ISRO	Enhanced public safety and resilience
International Partnerships	Indo-Pacific Cooperation	• Expand cooperation in SSA, space awareness, secure communications, and capacity building.	MEA, MoD, ISRO	Regional strategic influence
Global South Leadership	Capacity Building & Development Partnerships	• Provide satellite services, disaster support, and technical assistance to partner nations.	MEA, ISRO, SIA-India	Leadership in the Global South
Global Governance	Responsible Space Leadership	• Support norms for sustainability, STM, debris mitigation, and responsible behaviour.	MEA, DoS, International Partners	Increased global influence and credibility

