

Assured Access: Closing India's Dual-Use Space Dependency Gap



Dr Shrawani Shagun

Visiting Research Fellow, CAPSS

19 September, 2026

Keywords: Dual-Use, Dual-Use Space Systems, Assured Access, Commercial Space Services, Dependency Risk, International Humanitarian Law

Introduction

In 2022, SpaceX declined to activate requested Starlink coverage near Sevastopol, Crimea, after Ukrainian forces sought connectivity for an anticipated strike on the Russian Black Sea Fleet.¹ In March 2025, the United States temporarily suspended Ukraine's access to the Global Enhanced GEOINT Delivery (G-EGD) system, cutting off United States (US) government-mediated commercial satellite imagery that Ukrainian forces had built operational plans around.² A military commander made neither decision, nor was it subject to any legal review process available to the dependent State. Both were unilateral commercial or executive decisions, made by the provider or the provider's home government, for reasons entirely outside the dependent State's own assessment of military necessity.

These episodes are not distant case studies. They describe a structural vulnerability that applies equally to any State, including India, that relies on foreign-owned, commercially operated space systems for military and civilian functions. This article argues that India's growing dependence on dual-use commercial space services creates a single point of failure that current acquisition, targeting, and licensing processes are ill-equipped to address. Space technology carries an inescapable 'original sin'³—it was forged by military-industrial complexes for warfighting and intelligence, with commercial and civilian applications evolving subsequently. Modern satellite networks have consequently become the 'tethers of modernity,' where civil infrastructure and warfighting capabilities are inextricably entangled. Assessing a dual-use space asset solely as a

static physical object overlooks the proprietary, contractual, and geopolitical networks that determine who actually controls the capability in a crisis.⁴ It proposes three institutionally grounded reforms, extending weapons review, embedding dependency mapping into targeting doctrine, and building continuity safeguards into commercial space licensing, each calibrated to close this gap without slowing acquisition timelines or diffusing operational authority.

The Problem: Foreign Commercial Control as a Single Point of Failure?

India's expanding use of commercial and foreign-government-mediated space services, satellite communications, high-resolution imagery, positioning augmentation, weather and disaster data, has created a dependency structure that remains largely invisible to standard acquisition and targeting processes. The risk is concrete, not theoretical. India's institutional response to GPS reliability concerns, reflected in the development of Navigation of Indian Constellation (NavIC) and indigenous Satellite Communication (SATCOM) capacity, already recognises this vulnerability in the positioning, navigation, and timing (PNT) domain. That same logic has not yet been systematically extended to commercial imagery, broadband satellite communications, or weather and disaster-data dependencies, where India's exposure to foreign commercial decision-making remains substantial and largely unassessed.

The underlying legal architecture compounds the problem. Access to space-based services is governed not primarily by international humanitarian law but by a dense web of intellectual property protections, export-control measures, and commercial contracts that allocate proprietary rights and determine who may use, modify, withhold, or interrupt services once a crisis begins.⁵ A dependent State's forces may have full legal authority to conduct an operation and still find the underlying capability unavailable, because a foreign provider or its home government has exercised a contractual or policy discretion unrelated to that State's own assessment of the situation.

Extending Weapons Review to Capture Dependency Risk

Weapons and capability review under Article 36 of Additional Protocol I (AP I) of the Geneva Conventions and equivalent internal legal review processes typically assess technical performance, accuracy, effects, and reliability, without examining the ownership, licensing, and supply chain structure through which a dual-use space capability is accessed.⁶ A satellite-denial capability, a leased satellite communications channel, or a licensed imagery feed can pass technical review while carrying an unassessed dependency risk: who owns the platform, who can suspend the service,

and what happens operationally if they do. This institutional blind spot reflects what Anit Mukherjee diagnoses in *The Absent Dialogue* as the systemic isolation of military planning from civilian bureaucratic and technical expertise. When capability reviews occur in institutional silos, they evaluate technical accuracy while missing foreign licensing restrictions, commercial kill-switches, and single-provider dependencies.⁷ As Colin Gray emphasises in *The Strategy Bridge*, strategy must bridge tactical military means to desired political ends. Expanding Article 36 review panels to include structured, time-bound input from civilian ministries (such as Agriculture, Telecom, and External Affairs) repairs this bridge, ensuring that peacetime acquisition audits identify commercial dependency risks before a capability is integrated into operational plans.⁸

This gap is not, at bottom, a question of formal ownership. A reviewing State typically retains nominal contracting authority over the systems it fields. The more consequential gap lies in positive and procedural control: the capacity to track the source, supply chain, and operational capability of a dual-use asset, to guard against both misuse and unanticipated loss of access.⁹ Closing this gap does not require a new standing review board or public disclosure of sensitive ownership details, either of which would create delay or expose the reviewed system to additional risk. It requires extending existing review processes to include a dependency-risk checklist at the acquisition or licensing stage, covering ownership and licensing structure; contractual suspension or geofencing powers held by the provider or its home government; the availability of domestic or allied redundancy; and supply-chain traceability consistent with existing export-control practice. Civilian-ministry input, where a capability has documented large-scale civilian dependency, should be sought as a time-bound advisory input rather than a co-equal sign-off, preserving the pace of existing acquisition decisions.

Dependency Mapping as a Targeting Doctrine Reform

Targeting doctrine assesses whether an object is a legitimate military objective by reference to its nature, location, purpose, or use, and applies proportionality and precaution analysis based on the information available to the targeting cell.¹⁰ For dual-use space objects, the relevant civilian dependency is frequently extraterritorial and diffuse. Standard collateral-damage estimation, built around physical proximity to the target, largely misses this. A satellite disruption may cause negligible harm near a ground station while disabling disaster warning, agricultural data, or medical logistics for a population thousands of kilometres away—harm that proximity-based estimation has no established method of capturing.

Structured dependency mapping addresses this gap directly. Before approving interference with a dual-use space system, planners should identify categories of civilian users dependent on the affected service, including users outside the immediate area of operations, and assess whether redundant or alternative options exist for those users. Where dependency data is incomplete, doctrine should favour reversible, localised, non-kinetic degradation, cyber, spoofing, or temporary interference over destructive kinetic options, wherever such non-kinetic means are operationally feasible and achieve a comparable military effect. This doctrinal preference is grounded in operational reversibility and reduced escalation risk; it does not convert Article 57's precaution obligation into a categorical requirement to use non-kinetic means irrespective of feasibility, which remains a commander's judgment based on the capability actually available at the time.¹¹

This doctrinal preference operationalises Article 57 of Additional Protocol I through Emile Simpson's targeting framework in *War from the Ground Up*: moving from 'Can I?' (the legal threshold under Article 52(2)) to 'Should I?' (strategic alignment) and 'Must I?' (the obligation of precaution). A co-opted dual-use satellite meets the 'Can I?' test as a legitimate military objective.¹²

Article 57's precaution principle obligates planners to assess diffuse, downstream civilian impacts thousands of kilometres away. In space, where physical destruction creates irreversible orbital debris and widespread collateral disruption, non-kinetic interference (cyber, jamming, or laser dazzling) functions as a pure denial strategy—as conceptualised by Robert Pape in *Bombing to Win* and John Klein in *Space Warfare*. It blocks the adversary's Celestial Line of Communication (CLOC) without inflicting indiscriminate societal punishment or violating the 1972 Liability Convention.¹³

Continuity Safeguards in Commercial Space Licensing

India's commercial space sector and its reliance on foreign commercial providers currently operate without standard contractual protections against arbitrary service suspension during a crisis. Standard commercial contracts typically include broad limitation-of-liability clauses and unilateral suspension rights that leave dependent users, including government and critical-infrastructure users, with no recourse if a provider or its home government withdraws access.

Baseline continuity clauses in licensing conditions would close this gap without new legislation. These should define a protected category of continuity services- disaster warning, emergency communications, and critical infrastructure timing support- that retain at least minimum functional access even when other services are restricted, require advance notice of major service

interruption, and create a procurement preference for providers offering such guarantees. This positions India as a rule-setter rather than a rule-taker in the commercial space era, a stance justified first by India's own strategic interest in assured access, with the broader benefit to other dependent States, particularly in the Global South, following as a secondary and welcome consequence rather than the primary rationale.

Mandating continuity clauses and liability indemnification in commercial space contracts represents an essential evolution in 'Social Technologies'—the institutional structures, laws, and contracts that must keep pace with advancing physical hardware.¹⁴ As private mega-constellations dominate Low Earth Orbit, relying on unexamined commercial end-user license agreements (EULAs) leaves state security at the mercy of private corporate discretion. Standardising humanitarian continuity safeguards in domestic licensing rules ensures that India's legal architecture evolves in step with its space hardware.

Conclusion

The vulnerability exposed by the Starlink and G-EGD episodes is structural, not incidental. Any State that depends on foreign-owned, commercially governed space systems for military and civilian functions is exposed to decisions made by providers and their home governments for reasons unrelated to that State's own operational requirements. The reforms proposed here dependency-risk review at the acquisition stage, structured dependency mapping in targeting doctrine, and continuity safeguards in commercial licensing—are designed to close this gap while preserving the speed and operational authority required by acquisition and targeting processes. None of these measures depends on new legislation, additional bureaucratic layers, or public disclosure of sensitive information. They require only that India apply, to its wider portfolio of dual-use space dependencies, the same institutional foresight already reflected in its investment in NavIC and indigenous satellite communications: closing a demonstrated vulnerability before, not after, a crisis exposes it.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Aerospace Power and Strategic Studies [CAPSS])

Notes:

- ¹ "Ukraine: Musk Defends Starlink Decision on Crimea Strike," *Deutsche Welle*, September 09, 2023, <https://www.dw.com/en/ukraine-musk-defends-starlink-decision-on-crimea-strike/a-66764304>. Accessed on August 16, 2026.
- ² "U.S. Government Revokes Some Access to Satellite Imagery for Ukraine," *Reuters*, March 07, 2025, <https://www.reuters.com/world/us-aerospace-firm-maxar-disables-satellite-photos-ukraine-2025-03-07/>; Yuri Zoria, "Maxar confirms US government blocked Ukrainian access to satellite data," *Euromaiden Press*, March 08, 2025, <https://euromaidanpress.com/2025/03/08/maxar-confirms-us-government-blocked-ukrainian-access-to-satellite-data/>. Accessed on August 16, 2026.
- ³ Bleddyn E. Bowen, *Original Sin: Power, Technology and War in Outer Space* (London: Hurst & Company, 2022), pp. 4–5.
- ⁴ *Ibid.*, pp. 13–14, 245.
- ⁵ World Intellectual Property Organization, *Intellectual Property and Space Activities: WIPO Contribution to OECD* (Geneva: WIPO, 2004), pp. 5–8, <https://www.wipo.int/edocs/pubdocs/en/intproperty/spaceactivities.pdf>. Accessed on August 16, 2026.
- ⁶ "Article 36 Reviews: Dealing with the Challenges Posed by Emerging Technologies," *Stockholm International Peace Research Institute* (SIPRI). December 2017, pp. 4–34, Available at: https://www.sipri.org/sites/default/files/2017-12/article_36_report_1712.pdf. Accessed on 19/08/2026; International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949 (AP I), 1125 UNTS 3, Art. 36, p. 30, Available at: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf. Accessed on August 21, 2026.
- ⁷ Anit Mukherjee, *The Absent Dialogue: Politicians, Bureaucrats, and the Military in India* (New York: Oxford University Press, 2019), pp. 5, 32, 273–274.
- ⁸ Colin S. Gray, *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2010), pp. 29–31.
- ⁹ Michael N. Schmitt (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), pp. 114–115.
- ¹⁰ "Article 52-General protection of civilian objects," International Humanitarian Law Database, <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52>. Accessed on August 17, 2026.
- ¹¹ "Article 57 - Precautions in attack," International Humanitarian Law Database, <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-57>; Schmitt, n. 9.
- ¹² Emile Simpson, *War from the Ground Up: Twenty-First-Century Combat as Politics* (New York: Oxford University Press, 2012), p. 178.
- ¹³ John J. Klein, *Space Warfare: Strategy, Principles and Policy* (London: Routledge, 2006), pp. 51–52, 83–84. Klein's framework suggests that 'blocking' or controlling an adversary's lines of communication does not require kinetic destruction; localised, non-kinetic measures such as withholding commercial services or electronic interference achieve the same strategic denial without generating long-lasting orbital debris.
- ¹⁴ Eric D. Beinhocker, *The Origin of Wealth: Evolution, Complexity, and the Radical Remaking of Economics* (Boston: Harvard Business School Press, 2006), pp. 15–16, 244–245, 261–262. Beinhocker defines 'Physical Technologies' as methods for transforming matter, energy, and information, whereas "Social Technologies" are the designs, rules, and contracts used to organise humans. He argues that economic progress is driven by the tight co-evolutionary dance between the two.