Anthropic’s Fable 5 Directive: Overnight Export Control Authority and Its Implications for the Commercial Space Industry

June 16, 2026

On the evening of June 12, 2026, Anthropic received a directive from the United States government at 5:21 p.m. Eastern Time. The instruction was unambiguous: suspend all access to Fable 5 and Mythos 5 for any foreign national, whether residing inside or outside the United States, including Anthropic’s own employees who are non-U.S. citizens. Within hours, both models went offline for every customer worldwide. No advance notice. No transitional period. No grandfathering of existing contracts. A commercial product generating active revenue was switched off overnight.

The government’s stated rationale was the discovery of a jailbreak technique capable of bypassing Fable 5’s safeguards and, in particular, those designed to prevent access to the advanced cybersecurity capabilities embedded in Mythos, the underlying frontier model. The directive cited national security authorities but provided no further specifics. Anthropic responded with transparency, publicly noting that its own review of the demonstrated jailbreak found only minor, previously known vulnerabilities discoverable through other publicly available models. The company characterized the shutdown as a misunderstanding and committed to restoring access promptly.

The legal mechanism at work here is not novel. What is

remarkable is its application at this scale and speed to a consumer-facing AI platform.

Legal Architecture

The Export Administration Regulations ("EAR") have for decades governed the transfer of dual-use technology which are items with both civilian and military applications. Under the EAR, the release of controlled technology or source code to a foreign national within the United States constitutes a deemed export to that person's home country. This means that domestic access, not merely cross-border transfer, can trigger export control obligations.

The regulatory landscape governing advanced AI specifically has been in considerable flux. In January 2025, the Commerce Department's Bureau of Industry and Security issued an interim final rule called the Framework for Artificial Intelligence Diffusion. The rule would have introduced new controls and extended U.S. export control jurisdiction to foreign-made items that are the direct product of U.S. technology, regardless of where they are accessed. That rule never took effect and was rescinded on grounds that it was overly bureaucratic, stifled American innovation, and undermined U.S. diplomatic relations. Whilst a replacement rule has yet to be promulgated, the EAR framework, including its longstanding dual-use technology controls and deemed export provisions, remains operative.

What the Fable 5 episode illustrates is that the legal architecture already in place, without any frontier-specific AI rule, is sufficient for the government to suspend access to a commercial AI product overnight. The authority does not depend on a new regulation tailored to AI. It derives from the broad scope of existing national security authorities. The Fable 5 directive is a demonstration of what that authority can do.

A Lesson for Commercial Space Industry

The commercial space industry operates under an analogous, and in some respects more demanding, regulatory framework. Space-related technologies sit at the intersection of the EAR and the International Traffic in Arms Regulations ("ITAR"). The U.S. Munitions List, against which ITAR is enforced, has historically encompassed satellites, launch vehicles, propulsion systems, guidance technologies, and related software.

A commercial space operator providing satellite imagery services, orbital data relay, or launch support to an international customer base is, structurally, in the same position as Anthropic was before June 12. Whilst the service is U.S.-origin technology, it is accessible to foreign nationals and the government retains plenary authority to suspend that access, unilaterally, upon a determination of national security concern.

History has already furnished a sobering illustration of how swiftly that authority can reshape an industry. In the mid-1990s, Hughes Electronics and Loral Space & Communications both faced severe legal consequences after sharing technical analysis with Chinese engineers following the catastrophic failure of Chinese rockets carrying their satellites during launches. The State Department alleged that both companies had transferred sensitive technical data to Chinese engineers without prior government authorization and U.S. officials concluded the data could be used to improve the accuracy and reliability of Chinese ballistic missiles. The charges against Hughes and Boeing Satellite Systems (which had acquired Hughes' satellite division in 2000) were issued in a 2002 letter alleging 123 violations of the Arms Export Control Act and the ITAR. Hughes and Boeing ultimately settled for $32 million.

The political and regulatory fallout from this instance was

substantial and enduring. Congress enacted a new national defense authorization related act, which transferred jurisdiction over all satellite exports from the Department of Commerce back to the Department of State, placing them squarely under the U.S. Munitions List and the more restrictive ITAR licensing regime. This restructuring remained in force for over a decade, constraining the commercial satellite industry's competitiveness until Congress repealed the relevant provisions in the National Defense Authorization Act for Fiscal Year 2013. Comparably, whilst that episode unfolded over months of investigation, the Fable 5 directive unfolded in hours.

Takeaway

What June 12, 2026, demonstrated is that the U.S. government has both the legal authority and the operational willingness to issue a technology access suspension directive without advance notice, without detailed justification, and without a transitional framework. Moreover, a commercial technology company has no practical mechanism to resist compliance before acting. Anthropic had no meaningful avenue to contest the directive before complying. Its customers had no recourse. Its foreign national employees could not continue working with the affected models.

For commercial space operators, this scenario should prompt an honest inventory of risk. A satellite imagery company serving defense-adjacent customers in mixed-nationality jurisdictions. A launch service provider whose operations involve foreign nationals at mission control. An on-orbit servicing company whose telemetry systems constitute controlled technology. Any of these entities could, upon a government determination, find their operational licenses suspended, their services cut off, and their revenue interrupted with no more notice than Anthropic received. Advanced technology sectors operating at the frontier are, in the eyes of U.S. national security law, custodians of controlled capabilities. The government's

authority to restrict access to those capabilities is broad and immediate, and not dependent on commercial inconvenience. Commercial space companies would be wise to internalize that reality now, before a directive arrives at 5:21 in the afternoon with no advance notice and no specific explanation.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile: https://waselandwasel.com/about/abdulla-abuwasel/

Congress Introduces Legislation for Orbital Data Centers: Analyzing the Cruz–Hickenlooper NEW HORIZON Act

June 16, 2026

Senator Ted Cruz, joined by Senator John Hickenlooper, has introduced the Nodes, Enterprise Workloads, and Hybrid Operations, Resilience, Integration, Zero-Trust, Orbital Networks Act (the "NEW HORIZON Act"). The Act would, for the first time, statutorily direct the Department of Defense ("DoD") to operationally evaluate commercially available orbital data center services and space-based cloud computing capabilities. While the bill is modest in length, its implications for the commercial space industry are anything but. It signals that Congress now views in-orbit computing not as a speculative technology, but as prospective national

security infrastructure.

What the Bill Is

The NEW HORIZON Act is a pilot program authorization. It directs the Secretary of Defense, acting through the Director of the Defense Innovation Unit ("DIU"), to carry out an operational pilot program under the existing Hybrid Space Architecture initiative within one year of enactment. The program's mandate is to evaluate the use of commercially available orbital data center services relevant to national security space and joint mission requirements, with the authority sunsetting five years after enactment.

The congressional findings underpinning the bill articulate a problem the industry has long understood: modern national security space missions generate ever-increasing volumes of sensor and platform data, while reliance on ground-based processing introduces latency, bandwidth constraints, and vulnerabilities that degrade operational effectiveness in contested environments. Congress finds that commercial industry is developing the in-space processing, storage, and analytics capabilities that may resolve this bottleneck and an operational pilot is necessary to test military utility through real-world mission use cases before any broader adoption or sustained acquisition.

Notably, the bill also supplies a statutory definition for orbital data centers, something the sector has lacked. An "orbital data center" is defined as a space-based computing, data storage, or networking capability — whether a single spacecraft, hosted payload, or distributed orbital architecture — designed primarily to provide persistent, scalable, or shared in-orbit processing as a distinct operational capability, rather than as a function ancillary to a spacecraft's primary mission. That distinction between dedicated capability and ancillary function will matter considerably as agencies, insurers, and contracting parties

begin referencing the term.

What the Bill Outlines

The pilot program is built around seven enumerated purposes, spanning the assessment of military utility, operational integration into existing and planned DoD architectures, and the resilience, latency, security, and mission assurance benefits of in-space data processing. Two purposes warrant particular attention. First, the program must evaluate concepts of operations for the protection and defense of orbital data center assets against kinetic, non-kinetic, and cyber threats. This is an ostensible acknowledgment from the DoD that commercial compute infrastructure in orbit may become a target. Second, it must evaluate interoperable, commercially provided infrastructure sourced from multiple vendors, a clear congressional preference against single-provider lock-in.

In scope, the Secretary may employ commercial orbital data center services in support of real-world mission scenarios — including intelligence, space domain awareness, command and control, and data transport — and may conduct testing, demonstration, and limited operational employment. The Secretary is directed to encourage competitive participation from non-traditional defense contractors and commercial space providers.

The most consequential provisions for industry are the security requirements. Any orbital data center service processing, storing, or transmitting sensitive or classified information must implement zero-trust architecture, encryption, identity and access management, and insider threat protections; risk-management measures addressing supply chain vulnerabilities and foreign ownership, control, or influence ("FOCI"); redundancy, failover, and rapid reconstitution capabilities; secured telemetry, tracking, and command links with anti-spoofing and anti-jamming protections; hardened ground segments and software supply chains; and workload

isolation, tenant separation, and data sovereignty safeguards against cross-tenant or provider access.

The Secretary must consult with the Assistant Secretary of Defense for Space Policy, the service acquisition executives, the Space Force, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency, and must brief the congressional defense committees by December 31, 2028, including recommendations regarding future acquisition and the security requirements for any future program of record.

What It Could Mean for the Industry

For commercial operators, the bill is a door and a filter. The door is that DIU becomes a statutory front-of-house for orbital compute providers, with congressional direction to draw in non-traditional contractors and an explicit pathway toward programs of record. Whereas the filter is that the security provisions will function as de facto market standards. Providers whose architectures cannot demonstrate zero-trust compliance, FOCI-clean supply chains, and verifiable tenant separation will be structurally excluded from the defense market and, given the gravitational pull of defense requirements on commercial contracting, likely disadvantaged in adjacent commercial markets as well.

Counsel advising orbital infrastructure companies should treat the bill as a compliance roadmap now, not upon enactment. Capital structures should be reviewed for FOCI exposure, vendor agreements for supply chain attestations, and service-level architectures for the isolation and reconstitution capabilities Congress has signaled it expects. The NEW HORIZON Act is a pilot but, in defense acquisition, pilots are how markets are made.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile: https://waselandwasel.com/about/abdulla-abuwasel/

Environmental Liability in Commercial Space Launches: Examining the South Texas Mass Tort Case Against SpaceX

June 16, 2026

On April 30, 2026, eighty plaintiffs filed a federal complaint in the U.S. District Court for the Southern District of Texas against Space Exploration Technologies Corp. ("SpaceX"). The case, *Aguilar et al. v. Space Exploration Technologies Corp.*, No. 1:26-cv-00485, alleges that repeated Starship launch and landing operations at the Starbase facility in Cameron County have caused structural damage to homes across Port Isabel, South Padre Island, and Laguna Vista. Asserting claims of negligence, gross negligence, and trespass under the exclusive federal jurisdiction of the Commercial Space Launch Act ("CSLA"), the case has the potential to reshape the legal relationship between commercial launch operators and neighboring communities.

The Complaint

The plaintiffs are homeowners residing roughly six to twenty-two miles from Starbase's launch pads. The complaint alleges

that eleven Starship/Super Heavy test flights between April 2023 and October 2025, together with earlier sub-orbital tests and static firings, subjected their properties to intense acoustic energy. The complaint relies on peer-reviewed research by Brigham Young University scientists whose field measurements during the fifth and sixth test flights recorded maximum unweighted sound levels exceeding a threshold that SpaceX's own assessments and FAA environmental reviews recognize as the onset of structural damage risk. Sonic boom overpressures near and exceeding such a threshold were recorded at the closest locations, which is generally associated with windows shattering and superficial structural damage.

Critically, the complaint draws on SpaceX's own regulatory submissions, including a 2024 corporate statement acknowledging a "gap in data" regarding acoustic prediction for its Raptor engines. The plaintiffs frame this as evidence that SpaceX has been operating at the frontier of acoustic science while conducting the most powerful rocket launches in history, establishing both foreseeability and conscious indifference to risk.

Legal Claims and Statutory Framework

The complaint asserts three causes of action. First, the negligence claim alleges that SpaceX failed to conduct adequate pre- and post-launch studies and proceeded despite a high likelihood of property damage. Second, the gross negligence claim seeks exemplary damages, arguing that SpaceX had actual awareness of acoustic risks, especially after the inaugural April 2023 test destroyed its own launch pad, yet continued with conscious indifference. Lastly, the trespass claim contends that SpaceX intentionally caused acoustic energy to enter the plaintiffs' properties without consent, resulting in physical harm.

Jurisdiction rests on 51 U.S.C. § 50914(g), which grants

federal courts exclusive jurisdiction over third-party property damage claims arising from licensed launch activities. This provision confirms that the CSLA contemplates such suits but does not immunize the licensee. SpaceX is required under the statute to carry up to $500 million in third-party liability insurance, and the FAA's 2022 environmental assessment explicitly stated that SpaceX would be responsible for resolving structural damages caused by sonic booms.

Potential Legal Consequences

The outcome will turn on causation: whether the plaintiffs can demonstrate that launch-generated acoustic energy, rather than pre-existing deficiencies or other factors, caused their alleged damages. The complaint does not itemize specific harm to each property, which will demand expert engineering and acoustic testimony. SpaceX may challenge the causal link and argue for regulatory compliance.

However, regulatory compliance is not typically a complete defense to tort claims under Texas law; an FAA launch license does not, by itself, insulate a licensee from negligence or trespass liability. The gross negligence claim, if successful, could expose SpaceX to exemplary damages well beyond compensatory relief. The plaintiffs' strategy of grounding their case in SpaceX's own admissions and peer-reviewed acoustic data gives it a scientific credibility that may prove difficult to overcome at summary judgment.

Industry Implications

The ripple effects of this case will likely extend well beyond South Texas. The FAA authorized up to 25 Starship launches per year from Boca Chica in 2025, and similar acoustic concerns have been flagged at Cape Canaveral, Florida, where SpaceX is building another Starship launch site. A substantial damages award or a judicially imposed constraint could prompt a

reassessment of how launch site proximity to residential communities is evaluated during environmental review.

The case also exposes a gap in the CSLA framework: while the statute requires insurance and channels claims to federal court, it does not establish a dedicated compensation mechanism for communities chronically affected by launch operations (e.g., like airport regimes or military installations). As vehicles grow more powerful and cadences increase, policymakers may need to reconsider whether this framework adequately balances interest in space access with the existing property rights of neighboring populations. For operators planning new or expanded sites, this lawsuit is a timely reminder to integrate acoustic modeling and community engagement from the outset.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/abdulla-abuwasel/

Civilian Space Facilities in an Era of Armed Conflict: Dual Use Military Targets

June 16, 2026

The strikes conducted against the IRGC Aerospace Force Headquarters in Tehran in March 2026, followed days later by the bombing of a building at the Iran University of Science and Technology (“IUST”) on March 28, have introduced a crucial question for the global commercial space industry: at what

point does a civilian aerospace facility lose the protection its designation is understood to afford it?

The answer, as these events demonstrate, carries direct and immediate consequences for every private company, university research program, and commercial operator that shares infrastructure, personnel, or technology with a state-affiliated space program operating in a contested geopolitical environment.

The justification advanced for the Aerospace Headquarters strike was that the facility served simultaneously as a research center for civilian satellite operations and as a command-and-control node for military satellite programs, including those assessed to have provided surveillance and intelligence capabilities over a wide regional theater. The core assertion was function, not designation. Whether or not one accepts that characterization, the doctrinal logic underlying it is well-established: a facility's protected status under international law is determined by what it does, not by how it is labeled. The moment a civilian asset makes an effective contribution to military action and its destruction offers a definite military advantage, its civilian character becomes legally contestable.

The IUST situation is more layered and, for the international academic and commercial space community, more immediately concerning. Founded in 1929 as Iran's first institution to train engineers, IUST is a ranked technical university with thousands of students across dozens of fields of engineering and science; an institution whose civilian educational mission is not in reasonable dispute. Yet, the IUST faculty have conducted research with direct applications for unmanned aerial vehicles and, in 2022, the Japanese government listed the university as an entity of concern for proliferation relating to missiles and nuclear weapons. More concretely, the Zafar satellite project was developed by IUST in direct partnership with the Iranian Space Agency, a joint venture

that exemplifies the close collaboration between Iran's academic institutions and its governmental space bodies.

This is the dual-use problem made operational and inescapable. The same department that produces graduate engineers for a country's commercial aerospace sector also advances propulsion and systems research that feeds its state satellite program. The same laboratory that publishes peer-reviewed papers on orbital mechanics may contribute to launch vehicle development whose applications extend well beyond scientific inquiry. Civilian designation, in this context, functions as a starting presumption, rather than a permanent shield once thought to have existed.

The Chamran-1 satellite, launched in 2024 and developed at facilities that have since been destroyed, was characterized as a research and technology demonstration mission. The distinction between a research asset and an operational intelligence platform, it turns out, was one of framing rather than function. That gap, between what a facility or satellite is called and what it materially enables, is precisely where the commercial space industry's legal exposure now lives.

The consequences are significant and practical. Export control regimes, from the U.S. International Traffic in Arms Regulations to the EU Dual-Use Regulation, already require licensing determinations that assess whether a given technology could serve military ends in the hands of the recipient state or institution. What the current conflict has demonstrated is that the same analysis must now be applied at the facility and institutional level. A ground station that processes both civilian and military satellite telemetry, a university department that collaborates with both private launch operators and a state defense ministry, and a space research center that hosts both commercial payload integration and command-and-control infrastructure for a state constellation are all, under the targeting logic now being applied in practice, facilities whose protected status is

genuinely uncertain.

For commercial operators with supply chains, personnel exchanges, or data-sharing arrangements that touch state-affiliated aerospace programs in conflict-prone jurisdictions, the exposure is a test. Insurance underwriters are already reviewing war-risk exclusion clauses in light of the recent strikes. Technology transfer counterparties face renewed scrutiny from export control authorities examining whether components supplied to ostensibly civilian programs ultimately served infrastructure now treated as a military objective. Foreign academic institutions that maintained research partnerships with IUST, a university that appears in multiple government proliferation-concern registries while simultaneously ranking among the top technical universities in Asia, now confront the uncomfortable possibility that their cooperation agreements linked them, however indirectly, to infrastructure that has been bombed.

The lesson the commercial space industry must draw from March 2026 is this: civilian designation is not self-executing. It must be earned, maintained, and verifiable through a facility’s actual function, not merely its stated purpose. In a conflict environment where space is an active warfighting domain and dual-use infrastructure is a recognized and contested military objective, the burden of demonstrating civilian character has, in practice, shifted toward the operator. Companies, universities, and research institutions that have not yet audited their institutional relationships with state-affiliated space programs should do so now as a matter of legal caution and institutional survival.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/abdulla-abuwasel/

Geopolitical Tensions and Force Majeure in the Commercial Space Economy

June 16, 2026

The commercial space industry operates at the precise intersection of private enterprise and state sovereignty. It is therefore uniquely vulnerable when those sovereignties come into direct conflict. The escalating geopolitical tensions between the United States and the Islamic Republic of Iran present a case study in how diplomatic friction translates, with considerable legal consequence, into force majeure events across commercial space contracts. As practitioners advising operators, investors, and institutions in this sector, it is necessary to examine this phenomenon not as a distant geopolitical abstraction but as an active and pressing contractual reality.

The Legal Architecture of Force Majeure in Space Commerce

In commercial space agreements, force majeure clauses typically enumerate government actions, export license denials, sanctions regimes, and regulatory prohibitions as qualifying triggering events. The breadth of such clauses matters enormously, because in the space industry, performance is invariably conditioned upon a layered web of regulatory approvals.

The commercial space industry is structurally more susceptible to geopolitically induced force majeure than most other sectors, for three reasons. First, performance under space contracts requires regulatory approvals from multiple

sovereign jurisdictions, any one of which may be revoked for reasons entirely unrelated to commercial conduct. Second, the technology involved is dual-use by nature; the same propulsion system that services a commercial telecommunications satellite may fall within the scope of munitions controls. Third, insurance and financing arrangements in the sector are often conditioned on export compliance clearances, such that a sanctions escalation can trigger defaults across an entire capital structure simultaneously.

When geopolitical tensions intensify, as they have periodically, the United States government has expanded the scope of secondary sanctions, tightened technology transfer controls, and revoked or withheld export licenses for satellite components, launch services, and ground station technology.

The AsiaSat Precedent: Geopolitics as a Contractual Trigger

The most instructive case study currently before the industry is the AsiaSat dispute with India. India’s National Space Promotion and Authorisation Centre decided to withdraw authorization for AsiaSat’s AS-5 and AS-7 satellites beyond March 31, 2026, citing national security concerns stemming from AsiaSat’s significant Chinese government ownership through CITIC Group Corporation. The decision was not a commercial judgment, but a sovereign geopolitical act directed at the ownership structure behind the operator.

The downstream contractual consequences were immediate. AsiaSat’s current permission expires at the end of March, forcing broadcasters to migrate to other satellites or face channel blackouts. Without this approval, AsiaSat cannot legally provide satellite capacity in India, effectively forcing broadcasters to look for alternative transmission arrangements. Broadcasters including Zee Entertainment Enterprises and JioStar, part of Reliance Industries, must now move their services; Zee has already switched to Intelsat and

ISRO’s GSAT satellites.

The contractual dispute that followed is where the case becomes jurisprudentially significant. AsiaSat has issued a “trigger notice” to the Indian government under a bilateral investment treaty, formally signaling a potential legal challenge, and has simultaneously sent arbitration notices to broadcasters including JioStar and Zee, initiating dispute-resolution proceedings. AsiaSat’s commercial position is that its agreements were not India-specific as its contracts were not limited to India and customers could continue to use the same bandwidth to provide services elsewhere. The broadcasters reject that framing entirely.

India’s 2024 guidelines further require foreign satellite operators to operate through Indian entities and factor in geopolitical ties, while limiting service approvals to a satellite’s operational life or five years, whichever is earlier. The regulatory architecture, in other words, was designed to give geopolitical considerations dispositive weight over commercial continuity. AsiaSat’s decision to pursue a bilateral investment treaty claim presents a significant legal hurdle, as India does not have a direct BIT with Hong Kong for investment protection beyond tax matters, and enforcing BIT claims against governments is known to be difficult and lengthy.

The Iran Parallel: An Active and Unfolding Crisis

The AsiaSat dispute illustrates what happens when geopolitics terminates a satellite operator’s market access. The U.S.-Iran tensions present the same structural risk, with broader contractual exposure across the entire space value chain.

Since the tensions between the U.S. and Iran commenced, a number of oil and commodities companies have invoked force majeure. QatarEnergy, which operates the world’s largest liquefied natural gas export facility, declared force majeure

to avoid penalties for missing contracted deliveries. Aluminium Bahrain similarly suspended deliveries to some customers, citing risks of shipping through the Strait of Hormuz. The contractual mechanisms being invoked across these commodity sectors are identical to those embedded in commercial space agreements.

For the space industry specifically, the pathways of exposure are distinct from commodities but no less severe. U.S. export control law, principally the Export Administration Regulations and the International Traffic in Arms Regulations, imposes comprehensive restrictions on the transfer of space technology to designated adversary nations. Iran remains among the most heavily sanctioned jurisdictions globally. Common triggering events such as “acts of war,” may capture Iran-related disruptions, but the more difficult question will arise for supply chain failures that are not directly caused by war or government-mandated embargo but are instead the downstream economic consequence of regional conflict. Launch service agreements, satellite manufacturing contracts, spectrum coordination, and orbital insurance arrangements are all vulnerable to this secondary contagion.

Sanctions and export controls relating to the Iran conflict may independently prohibit performance and may or may not qualify as force majeure under the governing law. A sovereign ban that is itself a breach of sanctions does not automatically become force majeure. This creates a compounded risk for operators: the very act of attempting to invoke force majeure may expose them to sanctions liability if the performance they are excusing was already legally prohibited.

A deterioration of U.S.-Iran relations, whether manifesting as a military confrontation in the Persian Gulf, a further Iranian nuclear escalation, or a fresh round of maximum-pressure sanctions designations, would predictably generate force majeure claims across several categories of space commercial agreement: satellite manufacturing contracts

involving Iranian-backed investment entities; launch services agreements where trajectories or ground stations fall within OFAC-designated operational theaters; orbital slot licensing disputes where spectrum coordination through the International Telecommunication Union implicates sanctioned state entities; and, as the AsiaSat case demonstrates, capacity lease agreements where the nexus to a geopolitically disfavored ownership structure supplies the regulatory trigger.

Drafting Against Geopolitical Risk

Competent space counsel should treat geopolitical risk as a drafting imperative rather than a boilerplate contingency.

Force majeure clauses in commercial space agreements should specifically enumerate sanctions regime changes, export license revocations, and government-mandated service terminations as qualifying events, while simultaneously specifying the notice obligations, mitigation duties, and termination rights that flow from each. The AsiaSat dispute has illustrated that an operator’s failure to anticipate and contractually allocate this risk can leave it in the position of asserting arbitration claims against counterparties who have no commercially viable choice but to comply with the regulatory mandate they have been issued.

The commercial space sector has long prided itself on its capacity to transcend political borders. The legal realities of geopolitics suggest that this aspiration, however worthy, must be balanced against rigorous contractual foresight.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/abdulla-abuwasel/

Musk Announces SpaceX to Build Self-Growing City on the Moon Within 10 Years

June 16, 2026

It is not unbeknown to the public that NASA, for over a decade now, has been working to get humans back on the Moon. This has been a long and challenging journey that has successfully culminated in the Artemis II launch to the Moon this year. On the other side of the aisle, SpaceX and Musk have publicly stood ground on their desire to push the journey just a few kilometers further to Mars instead. However, on 8 February 2026, via X (formerly, Twitter), Musk announced:

"[…] SpaceX has already shifted focus to building a self-growing city on the Moon, as we can potentially achieve that in less than 10 years, whereas Mars would take 20+ years […] That said, SpaceX will also strive to build a Mars city and begin doing so in about 5 to 7 years, but the overriding priority is securing the future of civilization and the Moon is faster."

(emphasis added)

The phrasing matters. Musk did not describe a "base," a "camp," or even a "permanent presence." He chose "self-growing city" a term that, in space systems language, implies a settlement that can expand its own capacity faster than Earth can sustain it through resupply. In other words, the decisive milestone is poised to be the point at which the city can manufacture, repair, and reproduce the core inputs of life and industry on-site, with Earth shifting from a lifeline to a partner.

This emphasis on speed is also crucial. In the expanded

announcement, Musk explicitly contrasted lunar cadence with Martian cadence because the former provides frequent launch opportunities and short transit times allowing rapid iteration, while Mars imposes long windows between optimal departures and months-long transfers. The Moon, in Musk's framing, is simply the faster pathway to the larger objective, reducing the risk that a disruption on Earth can strand an off-world population before it is self-sufficient.

What a "self-growing city" would actually mean

A credible "self-growing" settlement is less a single project than a layered stack of capabilities that compound over time.

First, a survivable envelope or atmosphere. A city would begin with pressurized volume, radiation protection, thermal control, and redundancy. On the Moon that likely means habitats that are either buried, barriered, or shielded with regolith. Engineering for sustained occupancy is necessary to turn temporary infrastructure into long-term habitat.

Second, reliable power at city scale. Early lunar outposts can run on solar with storage; a city that grows needs power that is both scalable and resilient through lunar night, dust, and operational contingencies. That can mean distributed solar fields, large-scale storage, and, notably, nuclear surface power (see more on the plans for this here). The commercial point is that power becomes the first utility market of the lunar economy, and everything else prices off it.

Third, closed-loop life support and food production. "Self-growing" implies that water, oxygen, and consumables are not flown in as a permanent operating model. A settlement can still import specialty components, medicines, and high-value electronics but it cannot depend indefinitely on routine shipments of basic life inputs without remaining fragile by design.

Fourth, industrial metabolism by extraction, processing, and

manufacturing. This is where “city” plays a critical role in an envisioned lunar economy. A lunar settlement that grows must be able to produce increasing quantities of:

- structural materials (regolith-based bricks, sintered surfaces, composites),
- spare parts and tools (additive manufacturing),
- propellants and volatiles if polar ice is exploited, and
- replacement infrastructure (power hardware, pressure shells, mobility platforms).

In practical terms, “self-growing” means establishing an industrial base: each new machine, habitat module, or power unit increases the settlement’s ability to build the next one.

Fifth, governance by logistics. A lunar city will function as a managed system: inventory control, redundancy planning, maintenance cycles, and emergency protocols will be as central as rockets. The romantic imagery of flags and footprints matters less than the operational question of whether the settlement can survive a sustained interruption of Earth resupply.

Why the Moon becomes strategically attractive

Musk’s core argument is speed. The Moon is close enough to allow rapid learning cycles (launch, land, test, fix, repeat) on timelines that resemble industrial development rather than expeditionary exploration.

That matters because establishment of a large-scale settlement will not be a single “mission.” It will be an accumulation of failures and successes: life support anomalies, dust mitigation, thermal shock, power reliability, human factors, medical contingencies. A two-day transit and frequent windows change the economics of failure.

It also matters because NASA’s own lunar return effort remains on a near-term timetable. As of early February 2026, NASA

indicated Artemis II is targeting no earlier than March 2026 following issues identified during a fueling test. Against that backdrop, a public SpaceX narrative that the Moon is the near-term priority signals an alignment with where the most immediate institutional demand sits.

What this shift means for the industry

If SpaceX truly prioritizes a lunar city three effects follow across the market.

1) The lunar economy becomes real and fast.
A city implies persistent demand for cargo, construction, power, comms, navigation, mobility, and surface operations. That demand creates bankable markets for companies that are not launch providers: mining and excavation, robotics, thermal systems, pressure vessel manufacturing, radiation shielding, surface mobility, and autonomous operations.

2) “Cislunar logistics” becomes the main arena of competition.
A high-value advantage of establishing a lunar settlement is cadence. Any actor that can move mass routinely will set the tempo for everyone else. Musk’s own commentary places “millions of tons” and scale at the center of the ambition. The competitive response will not only come from rival launch systems, but from anyone building cislunar transportation, depots, tugs, and surface freight capacity.

3) Regulation, liability, and contract standards will tighten.
A city forces the legal questions to mature. Risk will address launch and reentry, but expand to long-duration habitation, industrial activity, and sustained operations in proximity to other actors. That pushes regulators and contracting authorities toward stricter requirements on safety cases, mission assurance, spectrum discipline, debris and traffic coordination, and insurance coverage tailored to continuous lunar operations.

It also changes the commercial posture of space law. The legal

work shifts towards operational governance rather than mission approval: how activity is coordinated, how safety zones are treated in practice, how responsibility is allocated across operators and contractors, and how disputes are resolved when operations become continuous rather than episodic.

Conclusion

This is not a retreat from Mars so much as a recalibration of sequencing. Musk still describes Mars as a continuing objective, with work beginning in the five-to-seven-year range, but with the Moon as the overriding priority because it is faster.

If the Moon becomes the proving ground for genuine self-sufficiency via energy independence, industrial reproduction, and survivable logistics, then the lunar decade will be the architectural foundation for everything that follows.

So that means that we are all heading to the Moon, SpaceX included.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile: https://waselandwasel.com/about/abdulla-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Russian Spy Satellites Intercepting European Satellite Communications

June 16, 2026

European space security officials are increasingly concerned that two Russian “inspector” satellites have been used to collect communications associated with multiple European satellites, including traffic linked to government and military users. This has evidently been a sustained pattern over several years, with the alleged consequence being intelligence collection and a clearer mapping of how European satellite services could be constrained or disrupted in crisis conditions.

Such activity risks compromising sensitive information transmitted by the satellites but could also allow manipulation of the satellite flight paths or even lead to accidents.

What is reported to have happened

The reporting attributes the assessment to European security and intelligence officials who have been tracking two Russian spacecraft commonly referred to as Luch-1 and Luch-2. Officials reportedly believe these spacecraft were able to intercept communications from at least a dozen European satellites. The reporting also notes close approaches to a wider set of satellites over a multi-year period, which, if accurate, would reflect deliberate station-keeping near targets rather than incidental co-location in geostationary orbit.

A key technical qualifier is that interception risk is not uniform. A close look points to legacy vulnerabilities, including the fact that some older satellites may still rely on weak or unencrypted command links, creating exposure not only for confidentiality but also for command authentication and operational integrity.

None of this requires assuming a “weapon” in orbit. Persistent proximity operations, combined with modern signals-intelligence payloads, can be sufficient to collect metadata,

waveform characteristics, traffic volumes, and in some cases content, depending on encryption and link discipline. Even where encryption holds, the collector learns usage patterns, the contours of the ground segment, and system behavior under stress.

Why proximity operations matter commercially

Geostationary orbit is a commercial operating environment. Many satellites carry mixed traffic of commercial connectivity, leased capacity, and governmental payloads or services. That makes “space security” inseparable from commercial service continuity and contract performance.

Three immediate consequences follow.

First, security standards will move from guidance to gating. Encryption, authenticated command and telemetry, and disciplined key management are no longer features that win competitive bids. They are baseline conditions for eligibility, particularly for government and critical-infrastructure customers.

Second, underwriting and financing will harden around cyber-physical risk. The market already prices launch and debris risk. Persistent proximity and interception concerns introduce a more political category: contested-domain operating risk. That tends to produce tighter warranties, more onerous security representations, and narrower coverage around interference events.

Third, customers will demand assurance, not only service levels. Expect procurement language to expand beyond uptime and throughput into incident response timelines, sovereign control of command chains, ground segment resilience, and demonstrable ability to maintain service under interference conditions.

These pressures are intensified by Europe’s parallel policy

direction toward sovereign secure connectivity. In January 2026, public statements from the European Commission described the commencement of GOVSATCOM operations, explicitly framed as secure and encrypted governmental satellite communications under European control.

The legal consequences: duties exist, but enforcement is political

The legal framework for outer space has not suddenly become obsolete. It is, however, strained by conduct that sits *below* the threshold of overt attack while still producing strategic harm.

Under the Outer Space Treaty, States must conduct activities with “due regard” to the corresponding interests of other States, and where a State has reason to believe an activity would cause “potentially harmful interference,” it should undertake appropriate international consultations. This is not a direct prohibition on collection, and it does not neatly capture intelligence operations. It does, however, create a lawful diplomatic pathway: if proximity operations are credibly framed as creating a risk of harmful interference or unsafe behavior, consultations are the treaty-based mechanism to press the issue.

Separately, Article VI’s responsibility principle matters in today’s mixed government-commercial architecture: States bear international responsibility for national activities in outer space, including those by non-governmental entities, and must authorize and continuously supervise such activities. In practical terms, this pushes European regulators toward more explicit security supervision of licensed operators whose systems carry government traffic, and it strengthens the policy case for security conditions in licensing and procurement.

The radio layer adds another legal and regulatory vocabulary.

The International Telecommunication Union radio regime is designed to prevent harmful interference and imposes obligations on administrations regarding stations under their responsibility. If interception evolves into jamming, spoofing, or service disruption, that framework provides process and terminology even when remedies remain political.

The limiting factor across these regimes is attribution and proof. Legal consequences scale with confidence. That reality will drive investment in independent tracking, data fusion, and evidentiary discipline, because sustaining a position in a diplomatic, regulatory, or legal forum matters.

Strategic meaning: below-threshold pressure becomes normal

The most consequential implication is not that satellites can be listened to. It is that space is being treated as a continuously contested domain, and that this contest is increasingly conducted through activity that stays below the threshold of overt interference.

For operators, the lesson is straightforward: resilience must be engineered and contractually demonstrated.

For governments, the implication is equally clear: the line between commercial service and national capability is thin, and it will continue to thin. Hybrid payloads, shared capacity, and multi-use constellations bring efficiency, but they also bring shared exposure.

For Europe, this incident reporting will likely accelerate three tracks already underway: (1) hardening of legacy systems and uplink security practices; (2) procurement and licensing reforms that make security a condition of market access; and (3) sovereign and allied connectivity architectures that reduce single points of failure and impose higher security baselines.

The diplomatic posture should remain measured. The objective

is to reduce strategic ambiguity, raise the cost of intrusive behavior through collective standards and coordinated responses, and ensure that Europe’s commercial satellite market remains credible to the customers who depend on it.

In short, the future will not be defined by a single episode of proximity collection. It will be defined by whether Europe treats this as an intelligence curiosity, or as a governance and market-structure inflection point.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile: https://waselandwasel.com/about/abdulla-abuwasel/

The Private Sector’s Increasing Control on National Security

June 16, 2026

For much of the last century, national security was treated as a sovereign stack: intelligence, armed forces, and state-controlled strategic infrastructure. The private sector mattered, but mainly as a supplier.

That separation is thinning across the world. In a period defined by gray-zone pressure, cyber disruption, and sustained geopolitical competition, private firms increasingly operate the systems that keep states functional under stress. They design the networks that move data, the platforms that process it, the factories that scale production, and the services that

can be surged in crisis.

This is not a story about governments outsourcing security; states still carry legal authority, coercive power, and strategic responsibility. It is a story about where operational leverage now sits.

Critical Infrastructure and the "Public Risk"

The modern economy runs on privately owned and operated infrastructure that is strategically exposed. Undersea telecommunications cables, which carry the overwhelming majority of transoceanic digital communications, are owned and operated by private companies and consortia. This reality is now being treated as a geopolitical fact, not a technical footnote.

In the **United Kingdom**, this has led to the recognition of the "private ownership of public risk." Under the National Security and Investment (NSI) Act, the UK government now scrutinizes private acquisitions across 17 sensitive sectors, including AI and energy, treating commercial activity as a core national security vulnerability. Even the UK's nuclear deterrent relies on private firms like Lockheed Martin for maintenance, proving that sovereign capabilities are deeply integrated with private industry.

Similarly, in **Europe**, the NIS2 Directive expands cybersecurity obligations to thousands of private organizations. By making these firms legally responsible for risk management and incident reporting, the EU effectively treats the private sector as the frontline of the "sovereign stack".

The Industrial Base as a Security Instrument

Security competition has returned to a basic question: can capacity be produced fast enough, at scale, and under constraint? This question implicates private industry first. Multi-state security groups now emphasize the need to

aggregate demand and use longer-term orders to accelerate industrial capacity.

Australia provides a leading example of building “sovereign capabilities” through private partnerships. To support the AUKUS security partnership, Australia is leaning on private innovation in robotics and quantum technologies. Strategic mergers, such as the Australian firm Penten with the UK-based Amiosec, are now seen as essential to creating global providers of digital security for the state.

Space: A Case Study in Strategic Speed

Space illustrates how commercial services become strategic infrastructure in months, not decades. In recent conflicts, commercial satellite connectivity and sensing became operational necessities. This has triggered a shift in how states like **Canada** view their “digital ambition.” Canadian analysts are increasingly arguing for the modernization of the “sovereign stack” by better integrating private-sector cloud and AI solutions, moving away from rigid, state-only classification frameworks.

Analysis: Future Control and the Security Arithmetic

As we look toward the future, the private sector is fundamentally changing the state’s “security arithmetic”. Private firms do not carry sovereignty, but they carry strategic consequence, creating four recurring dilemmas:

1. **Rule-Setting:** Who sets the rules for access or technical restrictions when private services are used in conflict?
2. **Concentration Risk:** How do states avoid single points of commercial failure without destroying the economics of the private market?
3. **Cross-Border Friction:** How do global firms reconcile operations with sanctions and competing alliance expectations?
4. **Resilience Contracting:** How do governments contract for

resilience and “surge capacity” rather than just peacetime performance?

The future of national security will be defined by “dual-use” infrastructure, private runways, ports, and subsea cables that serve both commercial and military purposes. Intelligence is being redefined as private companies become part of “epistemic communities” integrated into state networks due to their specialized data analytics.

A mature approach treats the private sector as a standing component of national security planning. This requires pre-negotiated surge mechanisms, routine exercises that include industry as an operational partner, and the construction of the legal and technical scaffolding necessary to make private capability reliable when the pressure spikes. In a world of persistent competition, the decisive question is no longer just what the state can do, but how effectively it can command the private leverage it no longer directly owns.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile: https://waselandwasel.com/about/abdulla-abuwasel/

China Unveils Five-Year Space Strategy: Behind What Beijing is Building and Why it Matters

June 16, 2026

On 29 January 2026, China formally unveiled its next five-year roadmap for its space sector. Led by the China Aerospace Science and Technology Corporation (“CASC”), the plan sets out a coordinated national strategy spanning space tourism, orbital digital infrastructure, satellite megaconstellations, deep-space exploration, and space resource development.

Unlike earlier plans that focused primarily on launch capability and national missions, this roadmap is explicitly commercial. It reflects Beijing’s shift from building space access toward designing a full space economy, integrating transportation, data, communications, computing, and long-term off-Earth operations into a single industrial system.

Below is what China is planning over the next five years and what it means for operators, investors, and governments.

Space Tourism as a Regulated Market

China placed space tourism directly inside its national development framework, committing to achieve operational suborbital tourism within the five-year window, followed by a phased transition toward orbital passenger services.

This matters more for what it enables structurally. Human-rated vehicles drive reusable launch systems, crew safety standards, insurance markets, ground infrastructure, and regulatory frameworks for commercial human spaceflight. By incorporating tourism into state planning, China is signaling that these enabling layers will be built in parallel.

Several Chinese startups are already developing suborbital vehicles, but CASC’s endorsement elevates tourism from speculative private activity to state-supported industry. The practical outcome will likely be accelerated certification pathways, coordinated launch infrastructure, and easier access to capital. In effect, tourism becomes the catalyst for a broader commercial ecosystem.

For international operators, this introduces a new state-backed competitor in a market previously dominated by Western firms.

Space-Based Computing and AI

The most strategically significant element of the announcement is China’s commitment to develop space-based digital infrastructure, including orbital data processing and AI platforms.

These systems envision satellites performing compute-intensive tasks directly in orbit, forming a space-based cloud layer powered by continuous solar exposure and unconstrained by terrestrial energy grids. Rather than downlinking raw data to Earth for processing, China aims to analyze imagery, communications, and sensor outputs in space before transmitting refined products to ground users.

This architecture reshapes the economics of Earth observation, secure communications, autonomous navigation, and defense-adjacent analytics. It also introduces sovereign digital environments beyond traditional jurisdictional boundaries.

Western companies have discussed similar concepts, including SpaceX through its broader constellation strategy, but China is now embedding orbital computing directly into national industrial planning. Over the next five years, this is likely to drive large-scale satellite deployment, new spectrum requirements, and accelerated development of space-qualified processors and networking systems.

For regulators and operators alike, orbital computing raises unresolved issues around cybersecurity, liability, data governance, and congestion management.

Deep Space Capability and Talent Development

China is also expanding its deep space ambitions. Just days

before the announcement, the University of the Chinese Academy of Sciences launched a School of Space Exploration focused on advanced propulsion, trajectory modeling, and long-range mission design.

This move institutionalizes deep-space expertise inside China’s technical pipeline, ensuring a steady flow of engineers trained for lunar operations, autonomous spacecraft, and eventual interplanetary missions. The five-year plan frames the coming decade as a window for leapfrog development in deep-space technologies, linking talent cultivation directly to national exploration objectives.

Practically, this supports sustained lunar activity, robotic surface missions, and future crewed operations beyond low Earth orbit, all backed by a growing domestic workforce specialized in space disciplines.

Satellite Megaconstellations and Orbital Real Estate

China’s roadmap also reinforces its aggressive push into large satellite constellations.

Chinese entities have filed extensive applications with the International Telecommunication Union to reserve spectrum and orbital slots for future systems numbering in the hundreds of thousands over the coming decade. These filings secure scarce orbital resources while positioning China to compete directly with existing broadband constellations. Control over spectrum and orbital slots determines who can deploy at scale, who faces interference constraints, and who shapes future standards. China is acting early to lock in access, ensuring its operators retain strategic flexibility as orbital traffic intensifies.

For existing constellation operators, this signals tighter competition for spectrum coordination and growing geopolitical complexity in ITU processes.

Space Resources and the Groundwork for Off-Earth Utilization

While less detailed publicly, the five-year framework references space resource development as part of China's medium-term objectives. This points toward future lunar utilization architectures, including in-situ resource extraction, surface logistics, and energy generation.

Resource development is being planned alongside launch systems, robotics, navigation, and power infrastructure, indicating a long-term vision for sustained off-Earth presence rather than isolated exploration missions.

Over time, this approach supports permanent lunar operations and potential cis-lunar industrial activity.

What This Means

Taken together, China's five-year plan represents a transition from space capability to space ecosystem design.

Tourism accelerates human-rated vehicles. Orbital computing drives constellation growth. Megaconstellations justify launch cadence. Deep-space programs advance propulsion and autonomy. Resource utilization supports permanent operations. Each pillar reinforces the others, forming a vertically integrated strategy for space commerce.

This contrasts with the Western model, where commercial development remains spread across agencies, regulators, and private operators. China is synchronizing state capital, industrial policy, education, and orbital planning into a unified framework.

For commercial actors, this reshapes competitive assumptions across tourism, satellite services, and space-based data markets.

For governments, it underscores the urgency of spectrum diplomacy, regulatory coherence, and international norms

governing orbital infrastructure and space-based computing.

For everyone else, whether in the space industry or otherwise, it signals that by 2030 the world will be operating within an unprecedented, fully globalized space economy.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile: https://waselandwasel.com/about/abdulla-abuwasel/

The India–EU FTA Reshapes the Economics of Commercial Space

June 16, 2026

On 27 January 2026, India and the European Union closed negotiations on a landmark Free Trade Agreement that European Commission President Ursula von der Leyen publicly branded the "mother of all deals" ("FTA"). The scale of the FTA is hard to overstate. The EU estimates that tariffs will be eliminated or reduced on 96.6% of EU goods exports to India by value, while India's trade ministry points to preferential access for 99.5% of Indian exports into the European market. Implementation is expected within roughly a year, following legal review, which is anticipated to take five to six months.

The FTA is not a "space agreement" on its face, but it lays the industrial, digital, and investment rails for a substantial EU–India orbital corridor. And in the summit's formal Joint Statement, they explicitly place space inside the newly signed India–EU Security and Defence Partnership, and they record "productive discussions" at the inaugural India–EU

Space Dialogue held in Brussels in November 2025.

In the modern space economy, the decisive constraints are often diplomatic friction points in standards, in data governance, in procurement eligibility, and in supply-chain trust. Space companies scale when their components, engineers, capital, and data can move predictably across jurisdictions. The India–EU FTA is a trade corridor agreement that also functions, in practice, as a space-enabling agreement. The Joint Statement then gives it strategic ballast by naming space cooperation as part of the broader security and defense architecture and by mandating deeper work through the Space Dialogue across technology domains including earth observation, satellite navigation, space surveillance, and communications.

Start with manufacturing and the upstream stack. Space hardware is still a story of precision industrial inputs: avionics, electronics, advanced materials, test equipment, optics, and specialty chemicals. The European Commission's own sectoral framing of the FTA highlights gains in areas such as machinery and "avionics," which is a quiet but meaningful signal for aerospace supply chains. When tariffs come down and customs processes become more predictable, you make cross-border bill of materials strategies viable. Now move to the downstream stack, where the commercial space opportunity is likely to compound fastest. The Joint Statement elevates the India–EU Trade and Technology Council as the cornerstone for technology cooperation and ties it to work on resilient supply chains and protection of sensitive technologies, alongside collaboration on advanced areas like semiconductors, artificial intelligence, quantum, and 6G. For commercial space, this is core infrastructure. Earth observation analytics, satcom service delivery, on-orbit servicing planning, and space domain awareness toolchains are all data-heavy, model-heavy, and increasingly delivered as cross-border digital services. The more the two sides can converge on

trusted digital ecosystems, interoperable standards, and predictable compliance expectations, the more feasible it becomes to build EU–India "two-home" space ventures that sell into both markets.

The Joint Statement goes further by calling for EU–India Innovation Hubs, an EU–India Startup Partnership, and exploratory talks on associating India with Horizon Europe, the EU's flagship R&D program. That combination matters because commercial space is now a deep-tech financing story. Venture capital follows pathways to customer adoption and non-dilutive R&D leverage. When Indian companies can more naturally co-develop with European partners, and when European primes and scaleups can integrate Indian engineering and manufacturing capacity without the old trade penalties, you widen the funnel for bankable cross-border programs.

Where the strategic layer becomes commercially decisive is the explicit space language in the summit package. The Joint Statement notes the signing of the India–EU Security and Defence Partnership and lists "space" among the cooperation domains. It also specifies, in the implementation agenda, deeper cooperation through the Space Dialogue on earth observation, navigation, space surveillance, communications, and space security. That is the bridge between government-to-government alignment and private-sector "permission to operate." In practical terms, it de-risks three things' investors always consider: (1) whether collaboration will be politically durable, (2) whether sensitive technology boundaries will be managed through predictable rules rather than ad hoc politics, and (3) whether public procurement and institutional buying power can become a customer base for commercial offerings.

The 1-year implementation timeline is important for space ventures because it aligns with product cycles. Space startups that begin structuring now can hit the market as the agreement moves into action, with their supply chains, licensing

posture, and data compliance built for the new corridor. Space founders should also be cognizant of climate and carbon rules. There was no immediate exemption for Indian firms under the EU’s Carbon Border Adjustment Mechanism, which took effect on 1 January 2026, but there will be EU financial support aimed at emissions reductions. For space, that is both constraint and opportunity. Satellite-enabled measurement, reporting, and verification services, climate risk analytics, and maritime emissions monitoring become more valuable when trade partners are tightening carbon accounting and supply-chain transparency. In other words, the compliance burden can become a demand engine for downstream space data services.

As the FTA moves towards implementation, the foundations for a shared commercial space ecosystem are now firmly in place. For founders, investors, and operators willing to move early, this corridor offers scale, stability, and a genuine opportunity to build across continents.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/abdulla-abuwasel/