

Two Markets, One Space Asset: Allocating Commercial and Defence Value

A transaction framework for separating customer, security, access, regulatory and capital value in dual-use space businesses

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

One satellite, sensor network or space-data platform can support commercial customers and national-security missions. The physical asset may be shared while customer rights, service levels, data handling, priority access, security controls, regulatory permissions, financing and cash conversion differ materially. A transaction model that applies one revenue multiple or one backlog measure to the whole business can therefore misstate both risk and value.

This paper develops a Dual-Market Space Value Framework for acquisitions, joint ventures and growth-capital decisions. It separates six layers: physical infrastructure; payload and processing capacity; customer and mission rights; data and intellectual-property rights; security and regulatory obligations; and contract economics. It then tests whether the same asset can lawfully, technically and commercially serve both markets through peacetime, surge and crisis conditions. The method connects each revenue stream to a named asset, orbital or ground resource, licence, contract, acceptance event, service obligation, customer priority rule and cash-conversion path.

A wholly hypothetical case examines a space-data operator with USD 96 million of annual revenue, USD 210 million of management-reported backlog and a proposed USD 740 million enterprise value. Evidence review reallocates revenue and backlog across commercial, civil-government and defence mission lanes; distinguishes shared from reserved capacity; recognises delivery, licensing and renewal dependencies; and tests a crisis-priority scenario. The illustrative analysis retains USD 158 million of executable backlog, adjusts maintainable EBITDA from USD 24 million to USD 17 million, and places USD 68 million of proposed value behind observable customer, security, capacity and collection milestones. Every figure is an illustrative management assumption. It is not observed company data, a market benchmark, a forecast, a military assessment or a valuation opinion.

The evidence base includes the 2024 U.S. Department of Defense Commercial Space Integration Strategy; the U.S. Space Force Commercial Space Strategy; current U.S. Government Accountability Office work on commercial space data and satellite communications; the UK Defence Space Strategy and space-domain-awareness requirements; NOAA remote-sensing licensing policy; FCC satellite licensing and orbital-debris rules; U.S. export-control and foreign-investment sources; NIST secure-software guidance; and IFRS requirements for business combinations, fair value, revenue and intangible assets. The conclusion is that dual-use value should be allocated through evidenced rights and

constraints. Buyers should pay for durable access, accepted service and collected cash; approval-dependent defence expansion and untested crisis economics should sit behind transaction protection.

JEL Classification: G34, H56, L14, L93, O32, O38

Keywords: dual-use space, space M&A, commercial space, defence procurement, satellite services, capacity allocation, data rights, export controls, valuation, national security

This paper is an educational and structural analysis prepared for research purposes. It is not investment advice, an offer, or a solicitation. It contains no client information.

1. DEFINE THE TRANSACTION DECISION

The transaction decision is whether one space asset or integrated platform can produce durable value across commercial and defence markets without creating unpriced conflicts over capacity, control, data, security or customer priority. The buyer needs to understand what is genuinely shared, what must remain separated and which rights change during crisis or government direction.

The relevant asset can include spacecraft, hosted payloads, sensors, ground stations, network orchestration, processing infrastructure, data archives, analytics, software, spectrum access and customer distribution. Legal ownership of the spacecraft is only one part of control. A customer can hold priority tasking, reserved capacity, protected data access or step-in rights that alter the economic freedom available to the owner.

The framework treats value as a chain from mission need to collected cash. A revenue opportunity receives transaction value when the required asset exists, usable capacity is available, the operator holds the relevant permission, the customer can contract, the service can pass acceptance, the data can be delivered under the agreed rights and the resulting invoice can be collected.

Table 1. Evidence required before dual-market value is recognised

Evidence layer	Core question	Minimum record	Transaction consequence
Asset	Which physical and digital resources deliver the service?	Asset register, configuration, ownership, health and dependency map	Defines the productive base
Capacity	What can be shared, reserved, surged or displaced?	Capacity unit, allocation rules, utilisation, constraints and priority rights	Defines available supply
Customer	Which party buys which outcome under which route?	Contract, task order, licence, acceptance and renewal evidence	Defines executable demand
Rights	Who may task, use, retain, combine and redistribute outputs?	Data licence, IP schedule, customer rights and restrictions	Defines monetisable freedom
Security and regulation	Which approvals govern ownership, operation and delivery?	Licences, classifications, security controls, export files and change obligations	Defines lawful execution
Economics	How do revenue, cost, capex and cash behave by mission lane?	Unit economics, billing, collection, support, insurance and replacement profile	Defines price and terms

Each evidence layer should be connected to a defined asset, customer, contract and operating state.

2. MAP THE ASSET AS A SYSTEM RATHER THAN A SATELLITE

A dual-use space business is a system of systems. Spacecraft can depend on launch services, spectrum coordination, ground-station availability, cloud regions, secure networks, mapping or timing data, customer terminals, software vendors and specialised engineering teams. Failure outside the spacecraft can interrupt revenue while the on-orbit asset remains healthy.

The buyer should construct an end-to-end service map from customer request to delivered output. The map should show tasking authority, scheduling, uplink, collection, downlink, processing, quality control, dissemination, customer acceptance and support. It should also identify which steps are common across markets and which require protected personnel, facilities, networks or procedures.

The map should distinguish owned resources, leased resources, customer-furnished equipment and third-party dependencies. Shared infrastructure can improve utilisation and margin. It can also create concentration risk when both commercial and defence services depend on the same ground station, cloud account, identity service or specialist team.

3. DEFINE THE COMMERCIAL AND DEFENCE MISSION LANES

Market labels are too broad for allocation. Commercial revenue can include recurring data subscriptions, tasking, analytics, capacity leases, managed services and integration. Defence revenue can include demonstrations, research awards, indefinite-delivery vehicles, task orders, operational

service contracts, surge access and classified support. Civil-government revenue can sit between these lanes and should remain separately visible.

Each mission lane should specify customer, user, decision supported, geography, latency, availability, data rights, security level, contract route and acceptance. The same image or communication link can carry different value when timing, exclusivity, reliability or permitted use changes.

The U.S. Department of Defense Commercial Space Integration Strategy identifies a need to integrate commercial solutions before crisis and to secure access through contracts or other agreements. The U.S. Space Force Commercial Space Strategy frames commercial integration within hybrid architectures. These policy directions support market opportunity. They do not establish that a particular vendor has funded demand, operational acceptance or protected access.

4. DECOMPOSE THE ASSET INTO ALLOCABLE VALUE LAYERS

The first layer is physical infrastructure: bus, payload, antennas, terminals, ground stations and processing hardware. The second is service capacity: collection opportunities, bandwidth, coverage, revisit, compute, storage and analyst throughput. The third is contractual access: reserved capacity, priority tasking, minimum purchases, renewal options and termination rights.

The fourth layer is data and intellectual property. A buyer may own a sensor and still face restrictions on customer data, derived products, algorithms, software components or model training. The fifth is regulatory and security permission. Licences, export classifications, facility clearances and ownership conditions can determine who may operate or access the system. The sixth is commercial execution: sales channels, frameworks, primes, customer relationships, acceptance history and cash collection.

Allocation should occur at each layer. A single percentage applied to total enterprise value obscures whether the defence element is an accepted service, a contingent procurement route or a strategic option. The model should allow different evidence weights, discount rates, milestones and transaction protections by layer.

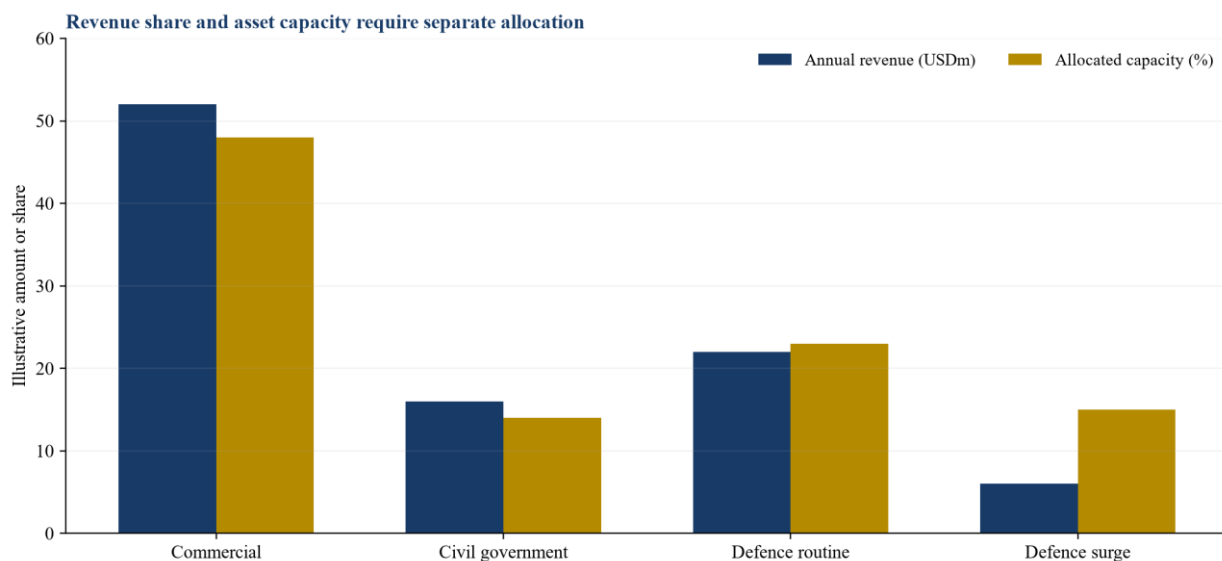


Figure 1. Hypothetical allocation of annual revenue and shared capacity by mission lane
All values are illustrative management assumptions and do not describe any company or programme.

5. MEASURE CAPACITY IN OPERATIONAL UNITS

Capacity should be expressed in units that match the service. Earth-observation capacity can be collection opportunities, square kilometres, revisit slots or processed products. Communications capacity can be bandwidth, beams, terminals, geographic coverage or guaranteed throughput. Space-domain-awareness capacity can be sensor time, track updates, conjunction analyses or alerts.

Headline spacecraft capacity can overstate saleable supply. Weather, geometry, interference, ground availability, maintenance, data-processing limits and customer priority can reduce usable capacity. The buyer should reconcile theoretical capacity, scheduled capacity, executed service and accepted output for representative periods.

Reserved capacity should be treated differently from minimum purchase. A customer may hold priority rights without paying for full utilisation. Another may pay a fixed availability charge plus variable usage. The model should allocate both revenue and opportunity cost so that a defence reservation is not counted as free capacity available to commercial customers.

6. TEST PEACETIME, SURGE AND CRISIS ALLOCATION

The asset should be modelled under at least three operating states. Peacetime reflects ordinary customer schedules and maintenance. Surge reflects a temporary increase in government demand while commercial service continues with agreed prioritisation. Crisis reflects stronger government direction, geographic restrictions, cyber pressure, constrained ground infrastructure or contractual step-in.

For each state, the model should identify who controls tasking, which customers can be displaced, the compensation mechanism, the security configuration and the effect on service-level commitments. The buyer should also determine whether commercial customers can terminate or claim credits when priority shifts.

GAO's 2026 review of commercial space data reported purchasing and use challenges involving licensing costs, perceived restrictions and long-term access. It also described commercial-provider restrictions introduced during a 2026 regional crisis. These findings show why crisis allocation must be traced through actual contracts and operating rules rather than assumed from ordinary utilisation.

7. SEPARATE AVAILABILITY VALUE FROM USAGE VALUE

Defence customers can value assured access even when utilisation is low. Commercial customers often pay for recurring usage, data volumes, seats, coverage or outcomes. A blended utilisation metric can therefore understate the value of readiness and overstate the value of unused capacity.

The pricing bridge should separate availability fees, reserved-capacity payments, tasking charges, delivered-data charges, analytics, integration, terminals, support and surge premiums. Each component should have a corresponding obligation and acceptance record. The buyer should test whether availability revenue requires specific redundancy, staffing, spares, cybersecurity or exercise participation.

An availability premium is credible when the operator demonstrates readiness and the customer has a contractual obligation to pay. An unfunded promise of future priority is an option. The option can influence strategic rationale while remaining outside base-case enterprise value until funding and terms are established.

8. BUILD THE RIGHTS STACK

Rights determine whether shared physical infrastructure creates shared economic value. The rights stack should cover tasking, access, exclusivity, data ownership, derived-data use, redistribution, retention, training, algorithm development, audit, disclosure, subcontracting and post-termination use.

Commercial licences may allow broad internal use while restricting redistribution. Defence contracts may create government-purpose rights, unlimited rights, protected technical data or customer-specific restrictions. Customer-furnished data may be usable only for a defined mission. The buyer should obtain the executed agreements and map rights by dataset, software component, model and output.

The acquisition model should identify rights that survive a change of control and rights that require consent. A business can report recurring revenue while relying on a customer licence, spectrum arrangement or distribution agreement that can terminate or narrow after the transaction.

9. PRICE DATA RIGHTS AND EXCLUSIVITY

Data value depends on reproducibility, coverage, timeliness, accuracy, provenance, customer rights and alternative supply. A large archive can have limited value when collection conditions are inconsistent, metadata is incomplete or customers own the economically relevant outputs.

Exclusivity should be decomposed by geography, time, sensor mode, customer class and use case. A defence customer can receive limited exclusivity around a mission without preventing commercial sales elsewhere. A broad restriction can materially reduce the addressable market and should be reflected in price, terms or operating structure.

The buyer should test whether derived analytics can be trained or improved using customer data. Consent, confidentiality, export controls and classification can prevent reuse. Model improvement should not be valued from inaccessible data.

10. DISTINGUISH FRAMEWORK ACCESS FROM FUNDED BACKLOG

Government frameworks, contract vehicles and vendor catalogues can shorten procurement. They do not create revenue without funded orders. A headline ceiling can describe the maximum value available across multiple suppliers and years while the target holds a small or uncertain share.

Backlog should be rebuilt at contract-line or task-order level. The schedule should show customer, service, funding, period, cancellation, option, acceptance, billing, collection, capacity commitment and delivery dependency. Unexercised options and unfunded ceilings should be disclosed separately.

Commercial backlog also requires scrutiny. Multi-year subscriptions may permit termination for convenience, volume reduction or service credits. Renewals should be supported by historical

behaviour, service performance and customer budget. The buyer should avoid treating every remaining contract month as equally executable.

Table 2. Allocation rules for common dual-use contract forms

Contract form	Economic evidence	Capacity consequence	Base-case treatment
Subscription	Executed term, minimum fee, usage and renewal history	Planned recurring capacity	Recognise contracted minimum subject to performance and termination
Tasking order	Funded order, acceptance and delivery schedule	Specific collection or processing allocation	Recognise funded executable work
Framework ceiling	Award, eligible scope and ordering history	No capacity until ordered	Exclude ceiling; disclose access option
Reserved capacity	Availability payment and priority rule	Removes or subordinates alternative use	Recognise fee and related opportunity cost
Surge option	Trigger, price, exercise authority and notice	Contingent displacement or expansion	Scenario value or milestone
Hosted payload	Payload rights, bus services, launch and operations obligations	Shared platform with dedicated mission resource	Model contractual service and failure allocation

Contract labels should be replaced by the executed economic and legal terms during diligence.

11. TEST PROCUREMENT ROUTE AND CUSTOMER AUTHORITY

Defence demand can pass through a prime contractor, government agency, marketplace, framework, research office or international partner. Each route creates different eligibility, security, pricing, audit, intellectual-property and payment requirements.

The buyer should identify the contracting authority and operational user. A programme office may sponsor a demonstration while another organisation controls production procurement. A combatant command can express mission demand while funding and contracting sit elsewhere. The value case should connect user need to a lawful and funded procurement path.

GAO's work on commercial satellite communications describes the U.S. Department of Defense's move toward hybrid architectures and its use of new commercial contracting approaches. The evidence supports the importance of integration and procurement design. It also records continuing coordination and reporting challenges, which should be treated as execution dependencies in a transaction case.

12. VERIFY OPERATIONAL ACCEPTANCE

Demonstration success does not equal accepted operational service. Acceptance evidence should identify the configuration, environment, test authority, measures, results, limitations and period of validity. The buyer should distinguish laboratory, exercise, pilot, initial operational use and sustained production service.

Operational acceptance can be customer-specific. A product accepted by one agency or allied customer may require new security, interface, spectrum, geographic or performance approval

elsewhere. The expansion model should state which evidence can be reused and which steps must be repeated.

Acceptance should be connected to revenue recognition and cash. A technically successful delivery can remain unbilled or disputed when contractual documentation is incomplete. The buyer should trace representative orders from tasking through acceptance, invoice and bank receipt.

13. MAP SECURITY ARCHITECTURE AND PROTECTED OPERATIONS

The shared asset can support separated security domains only when identity, networks, keys, data stores, logging, personnel and operating procedures enforce the separation. A diagram should be supported by configuration and test evidence.

The security review should cover ground systems, spacecraft command, supply chain, software delivery, cloud services, terminals and customer interfaces. NIST's Secure Software Development Framework provides a current baseline for secure development practices. Sector and customer requirements can add stronger controls.

The transaction itself can change risk. New owners, directors, lenders, administrators or service providers may affect access eligibility and customer confidence. The integration plan should identify which systems, personnel and contracts must remain ring-fenced until approvals are obtained.

14. TREAT RESILIENCE AS A DELIVERED SERVICE ATTRIBUTE

Resilience can come from distributed constellations, multiple orbits, alternative ground stations, diverse suppliers, protected networks, spare capacity, reconstitution or interoperability. The buyer should avoid applying a resilience premium to architectural claims without tested outcomes.

The asset register should identify single points of failure and recovery time. Exercises and incident records should show whether alternate paths work under load. Insurance can transfer defined financial loss while leaving service interruption, customer harm and strategic consequences with the operator.

Resilience investment should be allocated to the customers or mission lanes that require it. A commercial customer may accept a lower service level at a lower price. A defence customer may require protected availability, alternate paths and exercises. Shared resilience can create value when both markets benefit and cost allocation is transparent.

15. RECONCILE REGULATORY LICENCES TO THE TRANSACTION PERIMETER

Space operations can require licensing across communications, remote sensing, launch, spectrum, market access, orbital debris, ground infrastructure and data handling. The applicable regime depends on jurisdiction and service.

NOAA's commercial remote-sensing framework describes U.S. licensing of private remote-sensing systems alongside national-security and foreign-policy considerations. FCC satellite licensing under Part 25 includes technical, interference and orbital-debris requirements. A buyer should map each

licence to the legal entity, asset, configuration, authorised service, geography and change-of-control obligation.

The transaction perimeter should match the licences. Buying intellectual property without the operating entity may leave the buyer unable to deliver. Buying the operating entity can introduce ownership review, reporting or mitigation. The closing plan should state required filings, consents, interim covenants and long-stop dates.

16. MAP EXPORT CONTROL AND TECHNICAL-ACCESS CONSTRAINTS

Spacecraft, payloads, software, technical data, encryption and services can be controlled under different regimes. U.S. BIS guidance explains that releases of controlled technology or source code to foreign persons can constitute exports, including deemed exports. The precise classification and licensing position requires current specialist advice.

The diligence room should use role-based access. The buyer should obtain classification files, licences, provisos, technology-control plans, nationality restrictions, re-export conditions and records of prior disclosures. Redaction should preserve enough evidence for valuation while preventing unauthorised technical transfer.

The operating model should test post-close staffing, board access, integration tools and cross-border support. A synergy that depends on engineers sharing controlled technical data may be delayed or unavailable. Such synergy should remain outside base value until lawful access is established.

17. ADDRESS FOREIGN-INVESTMENT REVIEW EARLY

National-security review can apply to control and certain non-controlling investments. CFIUS operates under section 721 of the U.S. Defense Production Act and can review transactions involving critical technology, critical infrastructure and sensitive personal data. Other jurisdictions have separate investment-security regimes.

The buyer should prepare an ownership and control map, investor rights schedule, technology and customer profile, government-contract inventory, facilities map and mitigation history. Financing sources and co-investors should be included because governance, information and influence rights can matter.

Transaction timing should include declaration or notice preparation, review, investigation, mitigation negotiation and customer engagement where appropriate. The purchase agreement should allocate filing control, cooperation, acceptable mitigation, outside date and termination consequences.

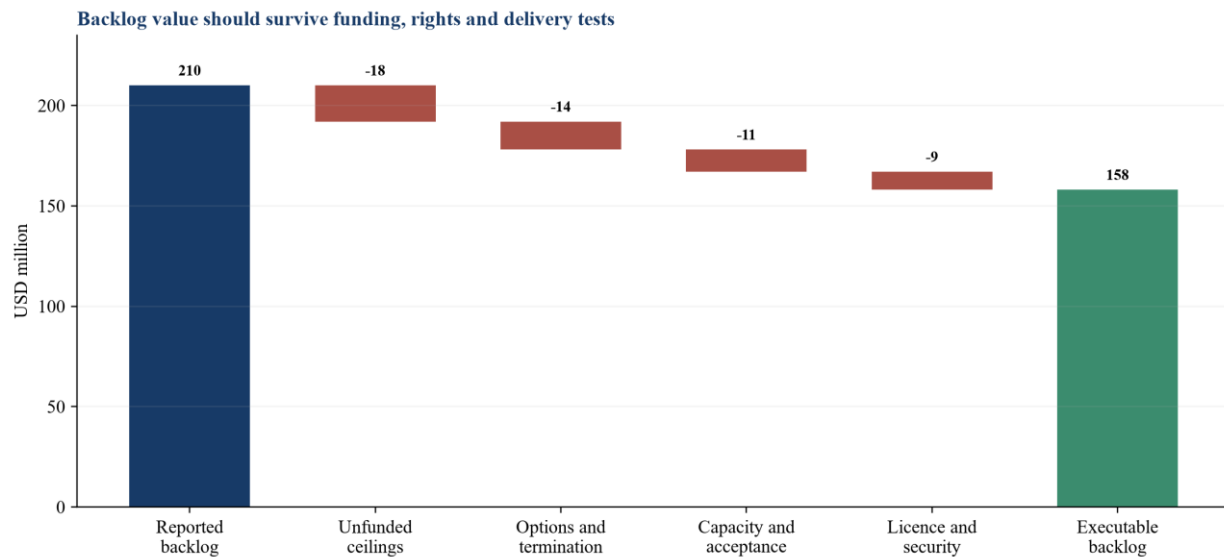


Figure 2. Hypothetical evidence retention from reported backlog to executable backlog
The bridge uses illustrative management assumptions and is not a market forecast or company assessment.

18. BUILD THE COST AND CAPITAL MAP

The cost base should be separated into asset operations, ground infrastructure, data processing, customer delivery, security, regulatory compliance, insurance, corporate overhead and research and development. Shared costs need an allocation driver connected to use or required readiness.

Space businesses also carry lifecycle capital. Replacement spacecraft, replenishment launches, terminal fleets, ground upgrades, spectrum work, cybersecurity and data infrastructure can be required to sustain revenue. EBITDA without lifecycle capital can overstate distributable cash.

The buyer should build a cash calendar covering contracted receipts, milestone payments, launch deposits, long-lead components, insurance premiums, debt service and working capital. Government payment timing and commercial customer concentration should be modelled separately.

19. ALLOCATE SHARED COST WITHOUT HIDING MISSION ECONOMICS

Cost allocation should support decisions rather than merely satisfy accounting. Direct costs belong to the relevant customer or mission lane. Shared costs can be allocated by capacity, usage, engineering effort, security requirement, asset count or another causal driver.

A defence contract may create security and readiness costs that also improve the commercial platform. A commercial scale investment may reduce unit cost for government missions. The model should show both stand-alone economics and shared-platform economics so that neither lane appears profitable only because cost has been shifted elsewhere.

The board should review contribution after direct cost, avoidable shared cost, lifecycle capital and risk capital. This view supports pricing, customer selection and asset-investment decisions.

20. TEST PRICING ARCHITECTURE BY CUSTOMER OUTCOME

Commercial pricing can be usage-based, subscription, enterprise licence, coverage, terminal, transaction or analytics based. Defence pricing can include availability, fixed-price delivery, cost reimbursement, tasking, data products, integration and support.

Pricing should connect to the customer's decision and the constrained resource. Premium tasking can be priced around priority and latency. Protected communications can be priced around availability and assured performance. Analytics can be priced around delivered workflow or outcome where measurement and contracting permit.

The buyer should identify customer-specific discounts, most-favoured terms, free demonstrations, credits and pass-through cost. Reported average selling price can hide a low-margin defence integration burden or a commercial customer receiving broad rights at a narrow price.

21. APPLY REVENUE-RECOGNITION DISCIPLINE

IFRS 15 requires an entity to identify contracts, performance obligations, transaction price, allocation and satisfaction of obligations. Dual-use space contracts can contain hardware, access, capacity, data, analytics, integration, support and options.

The transaction review should reconcile management reporting to contract accounting. Upfront cash may relate to future service. Milestone revenue may depend on acceptance. Variable consideration, service credits and termination can affect recognised revenue. Contract assets and liabilities should be understood by mission lane.

The buyer should maintain a revenue evidence file for material contracts. It should include executed terms, modifications, performance obligations, allocation method, delivery, acceptance, invoice, collection and dispute status.

22. IDENTIFY INTANGIBLE ASSETS AND CONTINUING OBLIGATIONS

IFRS 3 and IAS 38 provide the accounting framework for identifying acquired intangible assets. Relevant assets can include customer relationships, contracts, licences, spectrum-related rights, technology, software, data, trademarks and non-contractual relationships where recognition requirements are met.

An accounting identification does not determine commercial value by itself. A customer relationship can depend on security approvals, incumbent personnel or programme funding. Technology value can depend on export rights, reproducible builds and continued access to controlled facilities.

The buyer should also identify obligations that travel with the asset: deorbit, debris mitigation, data protection, service continuity, security remediation, licence conditions, warranty, launch commitments and customer credits. These obligations belong in valuation and purchase agreement design.

23. BUILD A DUAL-MARKET VALUATION BRIDGE

Valuation should begin with revenue, margin, capital and risk by mission lane. Commercial recurring revenue can be assessed through retention, unit economics and capacity. Defence revenue requires funded backlog, procurement route, acceptance, rights, security and renewal evidence. Shared-platform value comes from measurable utilisation and cost effects.

The valuation bridge should show reported EBITDA, accounting adjustments, direct mission costs, shared-cost reallocation, lifecycle capital and risk-adjusted maintainable cash. Scenario analysis should separately test renewal, utilisation, launch delay, asset loss, licence restriction and crisis prioritisation.

The hypothetical case begins with USD 24 million of management-reported EBITDA. It removes USD 3 million of capitalised operating effort, adds USD 2 million of security and readiness cost, adds USD 1 million of customer-specific support and recognises USD 1 million of recurring regulatory and insurance cost. The illustrative maintainable EBITDA is USD 17 million before lifecycle capital.

Table 3. Hypothetical transaction value bridge

Value component	Management case	Evidence-adjusted case	Treatment
Base operating value	USD 600m	USD 545m	Supported by adjusted cash and executable backlog
Commercial cross-sell	USD 42m	USD 18m	Retain only named customers and usable capacity
Defence expansion	USD 56m	USD 12m	Retain funded and approval-supported opportunities
Shared-platform efficiency	USD 28m	USD 21m	Retain costed integration and utilisation effects
Strategic access premium	USD 14m	USD 8m	Limit to evidenced licences, routes and rights
Total enterprise value	USD 740m	USD 604m plus milestones	Place USD 68m of contingent value behind evidence

All figures are illustrative management assumptions; they are not market benchmarks, forecasts or valuation advice.

24. PREVENT DOUBLE COUNTING ACROSS VALUE COMPONENTS

Commercial revenue, defence access and shared capacity can describe the same economic resource. The model should not count a unit of capacity in commercial growth, defence surge and cost synergy simultaneously.

Every synergy should identify source, action, owner, timing, cost, approval and affected capacity. Revenue synergies should name the customer and contract route. Cost synergies should name the duplicated resource and confirm that resilience or security does not require duplication.

Strategic option value should remain visible without being mixed into base operating value. Milestones, earn-outs or staged investment can preserve upside while limiting payment for unverified expansion.

25. MODEL THE DOWNSIDE STATES

The downside model should include loss or degradation of an asset, launch delay, ground outage, cyber incident, spectrum conflict, export restriction, ownership mitigation, customer non-renewal, commercial displacement and government priority shift.

Each state should show revenue, service credit, recovery cost, insurance, customer termination, funding need and covenant effect. A scenario that moves revenue between markets may also change margin because readiness and integration costs differ.

The buyer should test correlated risk. A geopolitical event can increase defence demand while restricting commercial markets, stressing capacity and increasing cyber risk. Treating these effects as independent can understate downside and liquidity needs.

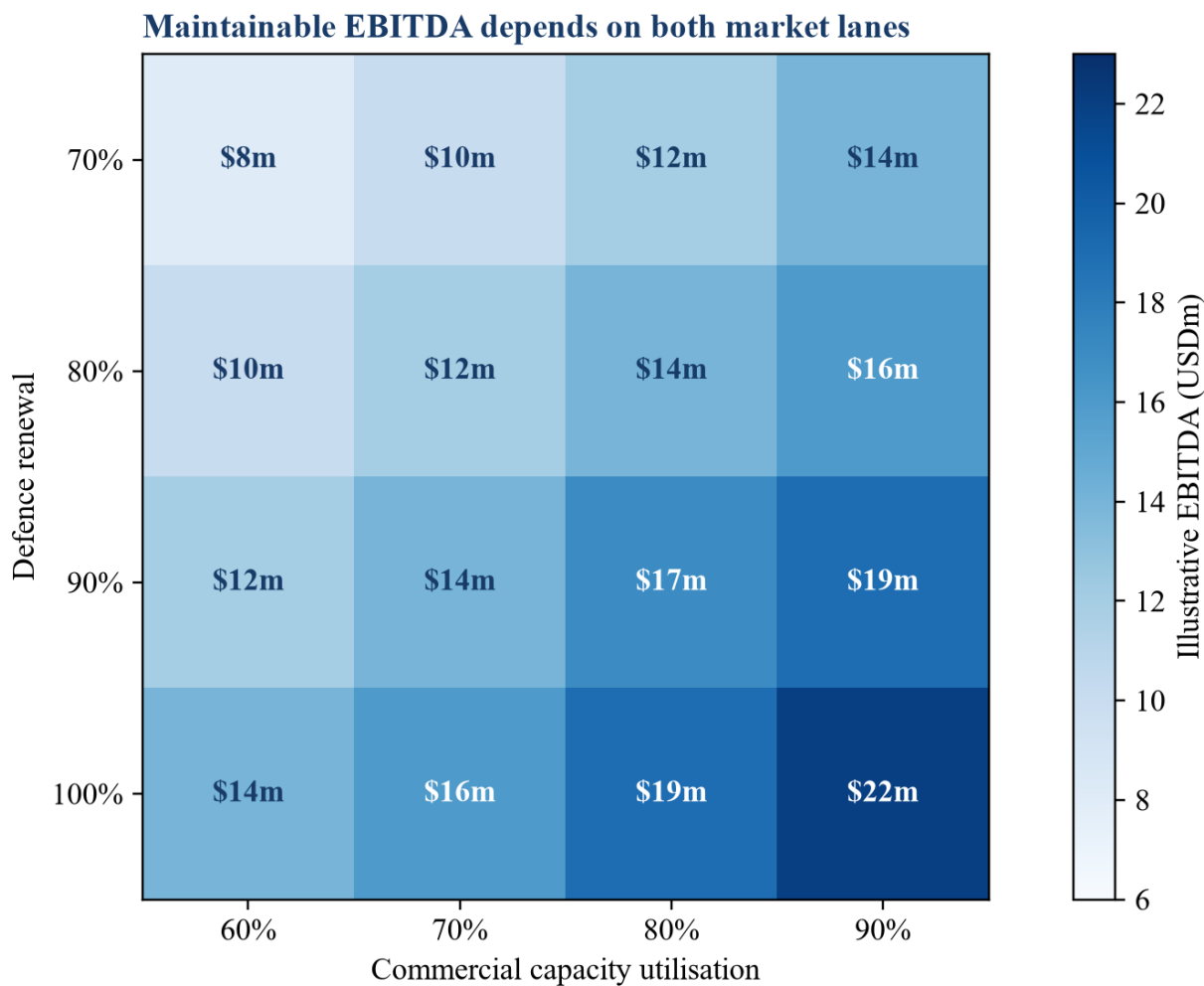


Figure 3. Hypothetical EBITDA sensitivity across utilisation and defence-renewal states
Values are illustrative management assumptions and exclude transaction financing.

26. DESIGN TRANSACTION PROTECTION AROUND EVIDENCE

Conditions precedent can cover regulatory approval, security consent, key licences, customer change-of-control consent and delivery of controlled records through authorised channels. Representations should address asset ownership, licences, export compliance, security incidents, contracts, backlog, data rights and government claims.

Holdbacks and indemnities can address known licensing, tax, export, security or customer disputes. Earn-outs should use observable measures such as funded orders, accepted service, collected cash, capacity availability or renewal. Vague strategic milestones create dispute risk.

Financing should reflect lifecycle capital and downside. Debt sizing based on reported EBITDA can be unsafe when launch, replacement or security expenditure is recurring. Covenants and liquidity reserves should account for asset events and delayed government collections.

27. BUILD THE CONFIRMATORY DILIGENCE ROOM

The data room should include asset and configuration records, licences, spectrum files, orbital and debris plans, insurance, contracts, task orders, customer licences, backlog, invoices, collections, security artefacts, export classifications, government filings, software repositories, data lineage and supplier agreements.

The review should use traceable samples. Select material commercial and defence contracts, then follow each from customer need through capacity allocation, delivery, acceptance, revenue and cash. Select critical assets and trace ownership, configuration, health, insurance, licence and replacement plan.

Protected information should remain within authorised channels. The transaction team should establish a clean-team protocol, access log, nationality restrictions and decision process for redacted evidence. Missing access is a diligence limitation and should be reflected in terms.

Table 4. Confirmatory diligence tests for a dual-use space transaction

Test	Evidence	Failure signal	Transaction response
Capacity	Reconcile theoretical, scheduled, executed and accepted service	Capacity sold twice or unavailable under priority rules	Reprice, reserve capacity or change commitments
Backlog	Trace funded orders and executable obligations	Ceiling, option or cancellable amount treated as firm	Exclude or milestone
Rights	Map tasking, use, retention, redistribution and change of control	Customer or supplier consent missing	Consent condition or ring-fence
Security	Test domain separation, access and incident response	Shared uncontrolled accounts or unreproducible controls	Remediation plan and holdback
Regulation	Match licence to entity, asset and service	Licence outside perimeter or ownership constraint	Restructure or condition closing
Cash	Trace acceptance, invoice and receipt	Revenue without collection evidence	Working-capital adjustment or earn-out

The test result should identify evidence, owner, exception and transaction response.

28. SEQUENCE THE FIRST ONE HUNDRED DAYS

The integration plan should preserve accepted service and regulatory compliance. The first phase freezes asset, licence, rights, security and customer baselines. The second establishes control of identity, repositories, finance, contract records and incident management. The third validates shared-platform initiatives in controlled environments.

Customer engagement should be sequenced by consent, mission criticality and commercial risk. Defence and regulated customers may require advance notice or approval. Commercial customers need clarity on service continuity and data use. Integration messaging should reflect executed rights rather than future ambition.

The combined company should establish one capacity and obligation register. Sales, operations, finance, security and legal teams should use the same definition of available capacity, reserved capacity, funded backlog and acceptance.

Integration should preserve service while control evidence is rebuilt

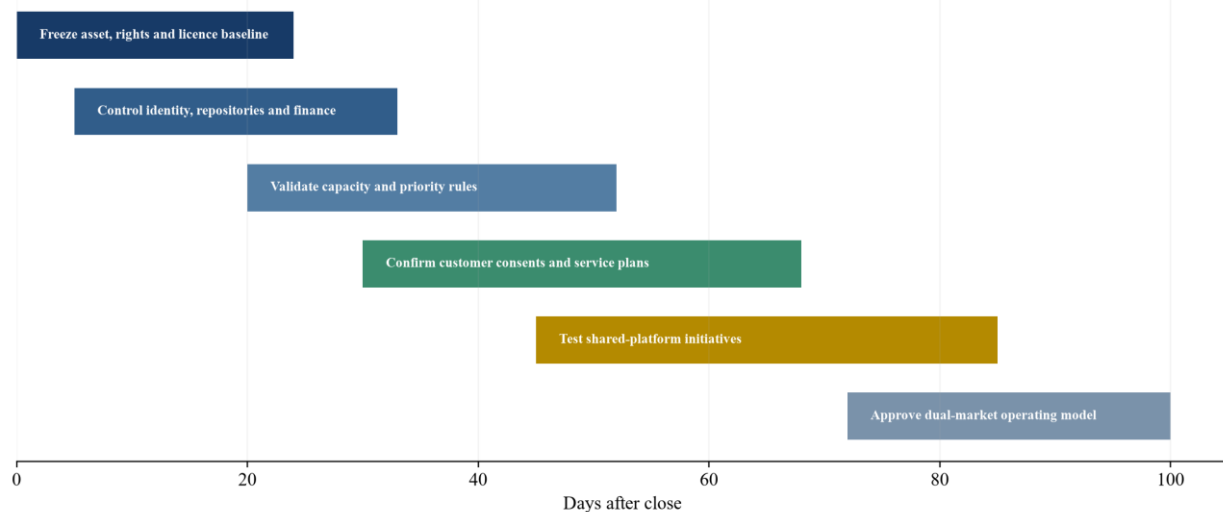


Figure 4. Hypothetical one-hundred-day dual-market integration sequence

Timing is illustrative and should be adapted to customer, security, licensing and operational requirements.

29. ESTABLISH DUAL-MARKET GOVERNANCE

The board needs an operating forum covering capacity, customer priority, security, licences, asset health, capital and crisis decisions. The forum should include commercial, government, operations, security, legal, finance and engineering leaders.

The capacity policy should define ordinary allocation, reservation, surge, conflict resolution and customer communication. Exceptions should be recorded with financial and operational consequences. The policy should align with contracts and lawful government direction.

Board reporting should separate commercial, civil-government and defence revenue, contribution, backlog, capacity, acceptance, collection and lifecycle capital. It should also report asset health, licence conditions, security incidents, export matters and material customer dependencies.

30. RECOGNISE LIMITATIONS AND CONCLUDE

This framework does not validate a spacecraft, service, mission, licence, security posture, export classification, contract, accounting treatment or transaction. Requirements vary by jurisdiction, customer, asset and configuration. Current legal, technical, security, regulatory, tax, accounting, procurement and insurance advice is required.

The hypothetical case does not estimate a market multiple or a company's value. Public strategies and reports establish context. They do not prove private-company performance, funded demand, eligibility or operational access. Protected evidence should remain within authorised review channels.

Dual-use value is created when shared infrastructure supports separable and executable rights across customers. The buyer should know which capacity is available, who can direct it, which data can be used, which permissions survive ownership change, which obligations consume cash and which customer pays for readiness.

The strongest transaction case connects physical assets to accepted service and collected cash. Commercial scale can support defence resilience. Defence demand can support readiness and investment. Each benefit should be supported by contracts, capacity, rights, security, licences and operating evidence. Value should follow the evidence, and uncertainty should be allocated through price, structure and milestones.

REFERENCES

- [1] U.S. Department of Defense. Commercial Space Integration Strategy, 2024. <https://media.defense.gov/2024/Apr/02/2003427610/-1/-1/1/2024-DOD-COMMERCIAL-SPACE-INTEGRATION-STRATEGY.PDF>
- [2] U.S. Space Force. Commercial Space Strategy: Accelerating the Purposeful Pursuit of Hybrid Space Architectures, 8 April 2024. https://www.spaceforce.mil/Portals/2/Documents/Space%20Policy/USSF_Commercial_Space_Strategy.pdf
- [3] U.S. Government Accountability Office. National Security Space: DOD Has Opportunities to Improve Its Use of Commercial Data and Related Services, GAO-26-107959, August 2026. <https://www.gao.gov/products/gao-26-107959>
- [4] U.S. Government Accountability Office. DOD Satellite Communications: Reporting on Progress Needed to Provide Insight on New Approach, GAO-25-107034, April 2025. <https://www.gao.gov/products/gao-25-107034>
- [5] U.S. Government Accountability Office. National Security Space: Overview of Contracts for Commercial Satellite Imagery, GAO-23-106042, December 2022. <https://www.gao.gov/products/gao-23-106042>
- [6] UK Ministry of Defence. Defence Space Strategy: Operationalising the Space Domain, February 2022. <https://www.gov.uk/government/publications/defence-space-strategy-operationalising-the-space-domain/defence-space-strategy-operationalising-the-space-domain>
- [7] UK Ministry of Defence and UK Space Agency. Space Domain Awareness Requirements, updated August 2024. <https://www.gov.uk/government/publications/space-domain-awareness-requirements/>
- [8] UK Government. National Space Strategy. <https://www.gov.uk/government/publications/national-space-strategy/national-space-strategy>
- [9] U.S. Department of Commerce, Office of Space Commerce. U.S. Commercial Remote Sensing Space Policy. <https://www.space.commerce.gov.a.woc.noaa.gov/policy/u-s-commercial-remote-sensing-space-policy/>
- [10] National Oceanic and Atmospheric Administration. Commercial Space Policy. <https://www.noaa.gov/sites/default/files/legacy/document/2020/Jun/Commercial%2520Space%2520Policy.pdf>

- [11] Federal Communications Commission. Space Innovation; Mitigation of Orbital Debris in the New Space Age, FCC 22-74. <https://docs.fcc.gov/public/attachments/FCC-22-74A1.pdf>
- [12] Federal Communications Commission. Single Network Future: Supplemental Coverage from Space, FCC 24-28. <https://docs.fcc.gov/public/attachments/FCC-24-28A1.pdf>
- [13] U.S. Department of Commerce, Bureau of Industry and Security. Part 734: Scope of the Export Administration Regulations. <https://www.bis.gov/regulations/ear/734>
- [14] U.S. Department of Commerce, Bureau of Industry and Security. Determine What Is Subject to the EAR. <https://www.bis.gov/licensing/determine-what-is-subject-to-the-EAR>
- [15] U.S. Department of Commerce, Bureau of Industry and Security. Commerce Announces Series of Rules to Modernize Space-Related Export Controls, October 2024. <https://media.bis.gov/press-release/commerce-announces-series-rules-modernize-space-related-export-controls>
- [16] U.S. Department of the Treasury. The Committee on Foreign Investment in the United States. <https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/>
- [17] U.S. Department of the Treasury. CFIUS Annual Report to Congress for Calendar Year 2025, August 2026. <https://home.treasury.gov/news/press-releases/sb0599>
- [18] National Institute of Standards and Technology. Secure Software Development Framework, SP 800-218. <https://csrc.nist.gov/pubs/sp/800/218/final>
- [19] IFRS Foundation. IFRS 3 Business Combinations. <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/>
- [20] IFRS Foundation. IFRS 13 Fair Value Measurement. <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/>
- [21] IFRS Foundation. IFRS 15 Revenue from Contracts with Customers. <https://www.ifrs.org/issued-standards/list-of-standards/ifrs-15-revenue-from-contracts-with-customers/>
- [22] IFRS Foundation. IAS 38 Intangible Assets. <https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/>

ABOUT THE AUTHOR

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

<https://www.linkedin.com/in/ckadya/>

<https://www.matchpoint-partners.com/team/ck-adya.html>

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.