The Cost per Interception: Pricing Counter-Drone Detection and Response

A procurement and transaction framework for threat evolution, layered defence, system evidence and lifecycle economics

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Small uncrewed aircraft can impose disproportionate cost because the defender must maintain awareness, classify uncertain objects, obtain authority, select a response and manage consequences across every protected hour. Public debate often compares the purchase price of a drone with the marginal cost of an interceptor. That comparison omits the sensors, communications, command-and-control, operators, training, site integration, legal permissions, testing, maintenance, software updates, inventory, safety measures and recovery actions required to produce a reliable defensive outcome.

This paper develops a Counter-Drone Procurement and Valuation Framework for buyers, investors, operators and public authorities. It separates detection from identification, identification from threat assessment, and threat assessment from an authorised response. It prices the full mission thread across radar, radio-frequency, electro-optical, acoustic and cooperative sources; data fusion and command software; non-kinetic and kinetic response options; people, power and infrastructure; testing; replenishment; and lifecycle support. The framework measures cost per protected hour, cost per credible track, cost per authorised response and cost per successful mission outcome alongside the avoided loss at the protected site.

A wholly hypothetical case covers 18 customers, 46 protected sites, USD 28.0 million of annual revenue, USD 96 million of management-reported backlog and a claimed 92 percent detection rate. Management identifies USD 18.4 million of annual customer value and USD 12.6 million of buyer revenue and synergy. Evidence gates retain 31 sites, USD 41 million of funded and executable backlog, and a 74 percent evidence-weighted mission-completion rate within defined test conditions. The framework retains USD 7.2 million of annual customer value and USD 4.6 million of buyer revenue and synergy after adjustments for coverage, false alarms, authority, interoperability, saturation, production, support and cash conversion. 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 U.S. Department of Defense Strategy for Countering Unmanned Systems; NATO counter-UAS interoperability exercises; U.S. Government Accountability Office work on counter-drone technologies; Federal Aviation Administration guidance for detection and mitigation at airports; UK Ministry of Defence publications on uncrewed systems and directed-energy trials; current export-control sources; and accounting requirements for revenue, intangible assets, business combinations and fair value. The conclusion is that a low marginal cost per shot can improve one part of the economics.

Transaction value depends on a tested, authorised and supportable mission system whose cost, capacity and outcomes remain credible as threats evolve.

JEL Classification: G32, G34, H56, L64, O32, O38

Keywords: counter-drone, counter-UAS, detection, response, interception cost, defence procurement, layered defence, M&A, technology valuation

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 PROCUREMENT AND ACQUISITION DECISION

The decision is whether a counter-drone system can protect a specified site, force, asset or event against defined threats at a supportable lifecycle cost. The relevant unit is the complete defensive outcome. A low-cost effector has limited value when detection is unreliable, identification is slow, authority is absent, integration fails or the system cannot sustain repeated incidents.

Procurement and M&A teams should begin with the defended mission rather than a catalogue of sensors and effectors. The mission establishes the geography, operating hours, threat classes, acceptable disruption, decision authority, safety constraints and consequence of failure. These requirements determine the architecture and the value of the target company.

The framework tests six linked propositions. The threat and protected consequence are defined. Coverage and identification evidence match the site. Decision rights permit timely action. Response options are effective and proportionate. The system remains available under saturation and change. Contracts, production, support and cash are executable. Each proposition has a separate evidence record and valuation consequence.

Table 1. Evidence required before a counter-drone capability receives procurement or transaction value

Evidence layer	Core question	Minimum record	Decision consequence
Protected mission	What asset, airspace and consequence are covered?	Site geometry, operating concept, loss scenarios and constraints	Defines required service
Detection and identification	Which threats can be found and classified in relevant conditions?	Configuration, test plan, tracks, false alarms and limitations	Defines usable awareness
Authority and response	Who may act, when and with which option?	Legal analysis, rules, approvals, safety case and procedures	Defines actionable capability
Capacity and resilience	Can the system handle repetition, saturation and change?	Simultaneous tracks, magazine, recharge, recovery and updates	Defines endurance
Delivery and support	Can the supplier deploy and sustain the configuration?	Bill of materials, acceptance, service levels and spares	Defines executability
Economics	Does the mission produce durable value and cash?	Lifecycle cost, avoided loss, margin, working capital and collection	Defines price and terms

Detection, authority, response and lifecycle evidence should be reviewed as one mission thread.

2. DEFINE THE PROTECTED MISSION AND CONSEQUENCE

A military installation, airport, prison, power plant, public event and industrial site face different operating constraints. The protected area may include open approaches, dense urban clutter, authorised aviation, electromagnetic congestion and third-party property. A product claim expressed only as range or probability of detection cannot establish mission fitness.

The buyer should document the asset, operating hours, perimeter, altitude bands, neighbouring activity, critical windows and acceptable interruptions. The consequence model should distinguish safety, operational delay, physical damage, information loss, public confidence and recovery cost. Avoided loss should be expressed as scenarios with probabilities and limits, not as an assumed saving.

The mission record should name the operator, accountable authority, escalation route and recovery owner. It should also state which threats remain outside scope. Clear exclusions improve procurement discipline because they prevent a demonstration result from becoming an implied promise to defeat every drone in every environment.

3. BUILD A THREAT AND ADAPTATION REGISTER

Threats differ by size, speed, altitude, payload, emissions, navigation, autonomy, number and operating pattern. Cooperative commercial aircraft, modified systems, pre-programmed aircraft, fibre-linked platforms and swarms can present different detection and response problems. A product optimised for one class may provide little evidence for another.

The U.S. Department of Defense's 2024 counter-unmanned-systems fact sheet calls for deeper understanding of trends, improved detection and characterisation, faster delivery, open modular solutions and a reduction in the cost imbalance between threats and countermeasures. The UK Defence Drone Strategy likewise describes adaptation measured in weeks. These public positions make threat evolution a procurement requirement rather than a remote technology risk.

The register should connect each threat class to observed evidence, plausible evolution, sensor response, identification method, authorised options and residual exposure. Dates and sources matter. A board should know when an assumption last changed and how quickly the supplier can update software, models, waveforms, interfaces and operating procedures.

4. PRICE THE COMPLETE MISSION CHAIN

The complete chain is detect, track, identify, assess, authorise, respond, confirm and recover. Each stage consumes time and can fail. Price should include the hardware and software required at every stage plus people, training, power, networks, facilities, testing, licences, maintenance, spares, data and command integration.

Marginal effector cost is only one component. A directed-energy system may have a low stated cost per firing while requiring acquisition, power, cooling, sensors, tracking, platform integration, maintenance and trained operators. A missile can have a high unit cost while providing reach or conditions that another effector cannot. The correct comparison is mission-specific cost and effectiveness.

Diligence should build a cost ledger by site, threat class and operating hour. Shared infrastructure should be allocated consistently. Non-recurring integration should be separated from recurring support. Costs deferred to the customer, prime contractor or government-furnished system should remain visible because a transaction can transfer or expand those obligations.

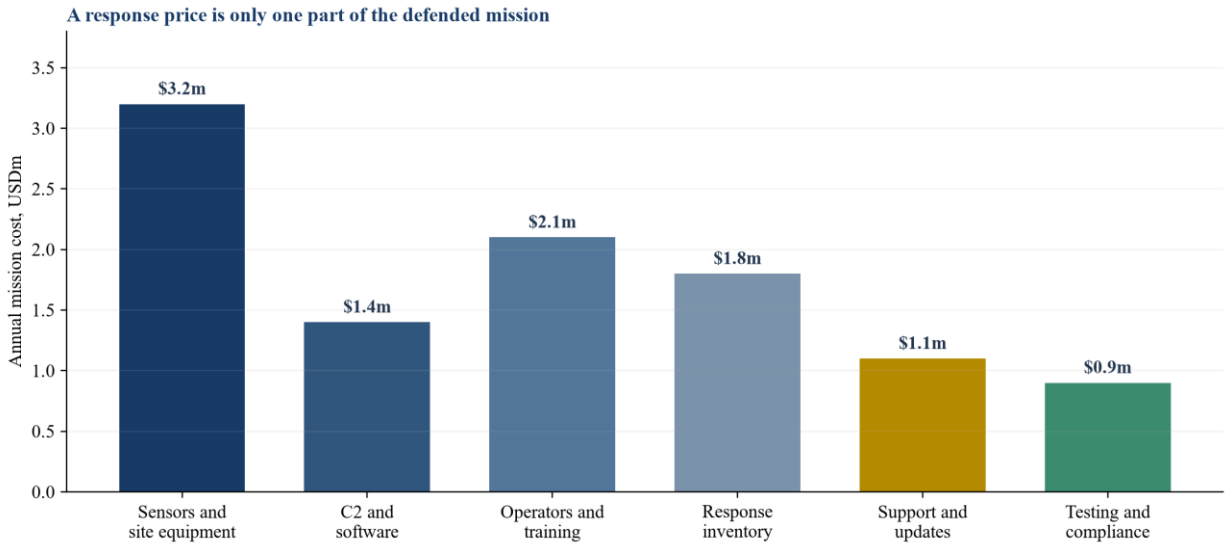

Figure 1. Hypothetical annual counter-drone mission cost stack

Values in USD millions are illustrative management assumptions, not observed company or programme data.

5. DESIGN THE DETECTION ARCHITECTURE

Detection can combine radar, radio-frequency sensing, electro-optical and infrared cameras, acoustics, cooperative identification and external intelligence. Each source has strengths, blind spots and legal or operational constraints. Coverage depends on terrain, buildings, clutter, weather, spectrum, target characteristics and placement.

The FAA distinguishes detection from mitigation and notes that radar, radio-frequency, electro-optical and acoustic sources can be used alone or together. Its airport guidance also states that detection systems do not determine intent or threat level. That distinction is essential for pricing: a track is an input to a decision, not a completed defence.

The buyer should obtain site surveys, sensor models, calibration records, coverage maps and test data. Claimed range should be tied to target class and probability under defined conditions. Redundant sensors can improve confidence when their failure modes differ. Redundancy provides little benefit when sensors share the same obstruction, network, power or classification error.

6. MEASURE PROBABILITY OF DETECTION AND FALSE ALARMS

Detection performance should state the denominator. A percentage without the number and mix of trials, target classes, conditions, distances and missed detections is not decision-grade evidence. The system should also report false tracks, nuisance alerts, track continuity and time to first reliable indication.

False alarms create operator load, interrupt operations and can encourage alert fatigue. Low false-alarm claims can be produced by high thresholds that miss difficult targets. The correct operating

point depends on consequence, traffic and response authority. Receiver-operating curves or equivalent threshold analysis can reveal the trade-off.

Diligence should reproduce performance from raw event logs for representative periods. It should include quiet days, busy airspace, birds, vehicles, weather and electromagnetic interference. Results should be separated by sensor and fused system. Pricing should reflect the operating point that the customer can actually sustain.

7. ESTABLISH TRACK QUALITY AND CONTINUITY

A detection becomes useful when the system maintains a sufficiently accurate track for identification and response. Track quality includes position, velocity, confidence, update rate, continuity, identity and uncertainty. Fragmented tracks can overstate the number of objects or cause a response system to lose custody.

The target should document association logic, handover between sensors, latency and behaviour during loss. Multiple drones and manoeuvring objects should be tested. Track confidence should not conceal stale or extrapolated data. Operators need to know when a picture is measured, fused or predicted.

The buyer should compare displayed tracks with independent ground truth. It should inspect missed handovers and identity swaps, not only successful runs. Integration with an external air picture or command system needs separate evidence because data formats, timing and classification can alter performance.

8. SEPARATE IDENTIFICATION FROM INTENT

Identification can use physical characteristics, radio-frequency signatures, remote identification, flight behaviour and operator investigation. None alone necessarily proves intent. A compliant drone near a site, a lost link, a malfunction and a hostile operation can produce overlapping observations.

The decision system should state confidence and source. Cooperative identification can reduce uncertainty for known traffic, while non-cooperative sensing remains necessary for other objects. Databases should be current and governed. A classification model trained on one geography or device population may degrade as equipment changes.

Procurement should measure correct classification, unknown rates and escalation time. The cost model should include human review and external coordination. A product that identifies fewer objects accurately may create more value than one that applies precise labels without calibrated evidence.

9. GOVERN COMMAND, CONTROL AND DECISION LATENCY

Command-and-control software should present evidence, uncertainty, rules and available actions to an authorised user. The timeline from first detection to decision must fit the protected geometry and threat speed. Latency should be measured end to end, including network, fusion, display, human review, approval and effector cueing.

The system should log recommendations, decisions, changes and outcomes. Interface design should reduce ambiguity under stress. Automated prioritisation can support attention while remaining subject to defined authority and validation. A graphical demonstration does not establish that the workflow performs under load.

The buyer should test degraded networks, sensor loss, multiple tracks and shift changes. It should map who can approve each action and how authority transfers. The acquisition model should include integration effort for the customer's command environment and the cost of maintaining each interface version.

10. CONFIRM LEGAL AUTHORITY BEFORE VALUING RESPONSE

Detection, monitoring and mitigation can engage aviation, spectrum, surveillance, computer, criminal, defence, safety and property law. Authority differs by country, agency, site and technology. The FAA's current airport guidance states that only specified U.S. federal departments have explicit statutory authority to operate mitigation systems in the circumstances described by that guidance.

The 2020 U.S. interagency legal advisory explains that radio-frequency monitoring and mitigation can implicate federal laws and that radar, electro-optical and acoustic sensing present different considerations. These sources do not determine another jurisdiction's position. They demonstrate why addressable market and product capability must be separated from lawful operation.

The vendor should maintain jurisdiction-specific analysis prepared by qualified advisers. Contracts should identify the customer's authority and responsibilities without transferring an unsupported assurance. Diligence should value detection-only, decision-support and mitigation markets separately where permissions differ.

11. BUILD A LAYERED RESPONSE ARCHITECTURE

Response options can include alerting, operational procedures, airspace coordination, locating an operator, physical security, electronic measures, takeover, capture, directed energy and kinetic systems. Suitability depends on authority, environment, threat, range, collateral risk and available time.

A layered architecture can preserve expensive or scarce effectors for threats that require them. It can also add integration, training and command complexity. The buyer should model which layer covers each threat and what happens after failure. A list of available effectors is not a defensive design.

The target should provide test and safety evidence for each response path. The effect of a countermeasure on other systems, friendly aircraft, communications and people should be assessed. Recovery of a disabled aircraft and preservation of evidence can create additional cost and responsibility.

12. COMPARE MARGINAL FIRING COST WITH MISSION COST

UK Ministry of Defence publications have described low stated firing costs for developmental radio-frequency and laser directed-energy systems. These public figures illustrate the potential benefit of

reusable or electrically powered effectors. They do not establish total ownership cost, availability, range, weather performance, acquisition price or fitness for a specific mission.

Cost comparison should include acquisition amortisation, sensors, tracking, power, cooling, maintenance, crew, training, infrastructure, consumables, reload, failed attempts and recovery. It should also include the probability that the option is authorised and effective in the relevant window. A nominally cheap firing can be expensive when many attempts or a separate fallback system are required.

The board should see both cost per attempt and expected cost per successful mission outcome. The latter divides the full relevant cost by evidence-weighted completion. It should be calculated by threat and condition, with public claims retained as context rather than substituted for company evidence.

13. TEST MAGAZINE DEPTH AND SATURATION

Capacity is the number of threats that can be detected, tracked, decided upon and addressed within time. Sensors, networks, operators, effectors, power, cooling, reload and command authority can each become the bottleneck. Magazine depth therefore extends beyond physical ammunition.

The target should test simultaneous tracks, close spacing, mixed classes, repeated waves and decoys within safe and authorised conditions. It should report queueing, dropped tracks, re-engagement and recovery. Demonstrating one successful engagement says little about a sustained defence.

The buyer should model demand as scenarios, not a single average. It should value modular expansion only where interfaces, supply and site design permit it. Capacity claims that depend on future software or uncontracted inventory belong in milestones rather than signing value.

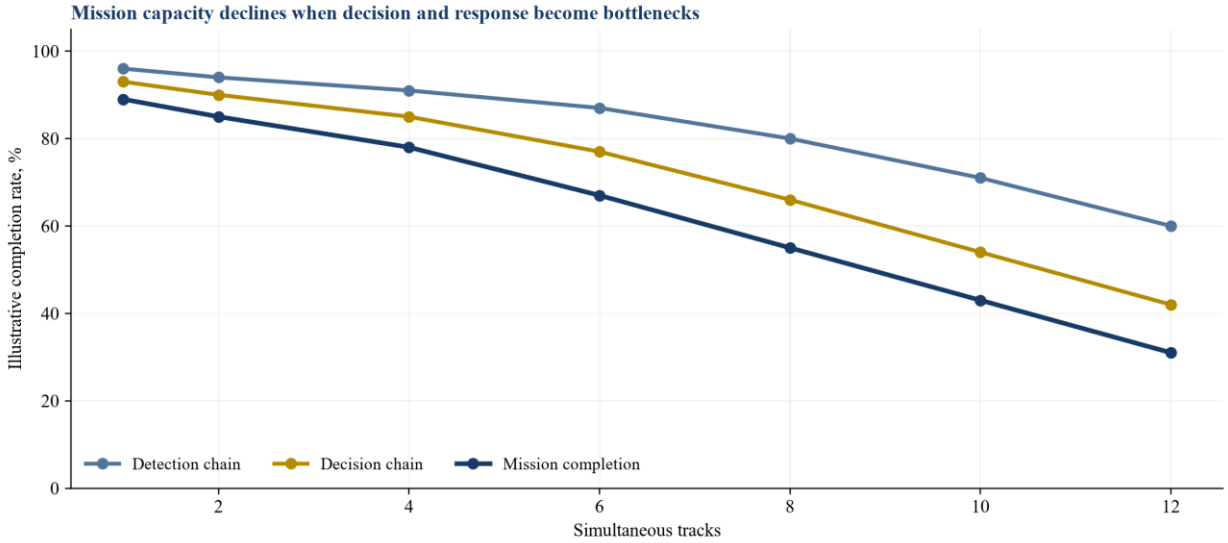

Figure 2. Hypothetical evidence-weighted mission capacity under increasing simultaneous tracks

Percentages are illustrative management assumptions and do not represent a real system.

14. MEASURE COST PER PROTECTED HOUR

Cost per protected hour allocates site equipment, software, operators, support and readiness across the hours in which the service is required. It reveals differences between a permanent installation, a mobile team, an event deployment and an on-call arrangement. It should state the coverage area and service level.

High consequence sites may require continuous redundancy even when incidents are rare. Event protection may concentrate cost into a short window. A customer can reduce cost by narrowing coverage or operating hours, but that choice changes the mission. Pricing should show the trade-off explicitly.

The supplier should reconcile protected hours with availability and outages. Planned maintenance, calibration, weather exclusions and unavailable effectors should reduce service hours where appropriate. Revenue described as recurring should be supported by enforceable service obligations and customer acceptance.

15. MEASURE COST PER CREDIBLE TRACK AND RESPONSE

Cost per credible track divides detection and decision costs by tracks that meet an agreed confidence threshold. It helps distinguish a quiet site with reliable sensing from an environment that consumes substantial operator time. The metric should not reward a system for suppressing difficult detections.

Cost per authorised response includes confirmation, approval, effector preparation, action, outcome assessment and recovery. Responses that stop before mitigation, such as operator location or operational rerouting, should be categorised separately. The customer's objective can be achieved without an interception in some cases.

The buyer should use a metric tree rather than one blended number. Protected hours measure readiness, credible tracks measure awareness, authorised responses measure workflow and successful outcomes measure mission effect. Each denominator should reconcile to logs and avoid double counting.

16. REQUIRE REPRESENTATIVE TESTING AND INTEROPERABILITY

NATO's counter-UAS technical interoperability exercises test sensors, effectors, jammers and command applications in controlled live scenarios. NATO reported more than 60 systems and 40 command-and-control applications at its 2026 exercise. The scale demonstrates the integration problem and the importance of standards; it does not validate every participating product.

Tests should reflect site geometry, clutter, authorised traffic, weather, spectrum, operator workload, threat classes and response constraints. Laboratory and component tests remain useful for isolation. Site acceptance should confirm the whole mission chain. Adverse and incomplete results should remain in the evidence record.

The buyer should inspect interfaces, timestamps, track formats, identity semantics and failure behaviour. Open interfaces can support competition and upgrades when implementation rights and documentation are usable. An interface described as open can still depend on proprietary gateways, restricted data or supplier services.

17. BUILD THE MISSION-EVIDENCE REGISTER

The evidence register should link requirement, configuration, site, threat, test, ground truth, result, limitation, reviewer, decision and remediation. It should preserve software, model, sensor and effector versions. A result belongs to the tested configuration and should not automatically transfer after change.

Evidence should be graded by independence and representativeness. Vendor demonstrations, customer trials, independent tests and accepted operational deployments answer different questions. Protected information can be reviewed through controlled channels, with non-sensitive conclusions recorded for transaction governance.

Diligence should sample successful and failed events. It should reproduce claimed rates and reconcile missing data. The register becomes a commercial asset when it shortens customer acceptance, supports updates and enables the buyer to know which configurations can be sold and supported.

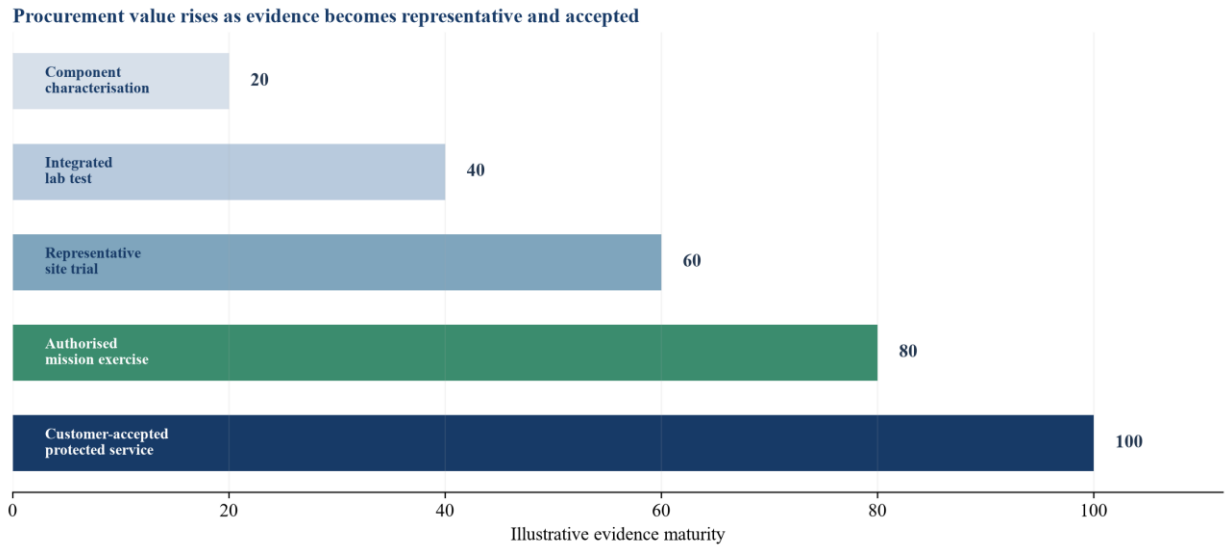

Figure 3. Counter-drone evidence ladder from component test to accepted protected service

The ladder shows decision relevance; higher levels require controlled configuration and authorised customer evidence.

18. VALIDATE ARTIFICIAL INTELLIGENCE AND DATA

Counter-drone systems may use machine learning for detection, classification, tracking, sensor fusion, prioritisation or anomaly recognition. Each use has distinct errors and consequences. The product should identify where machine output informs a human and where it initiates an automated function.

The target should document data provenance, labels, synthetic data, exclusions, train-test separation, geographic coverage, performance, calibration, drift and change approval. Metrics should be reported by relevant threat and condition. Aggregate accuracy can conceal weakness in rare but important cases.

The buyer should test false positives, false negatives and confidence calibration at operational thresholds. It should assess whether new threats can be incorporated without forgetting existing

performance. Data and model rights must support post-close operation, export, customer assurance and independent review.

19. TEST CYBERSECURITY AND SPECTRUM RESILIENCE

The defensive system can itself be disrupted through network attack, compromised updates, spoofed tracks, data poisoning, credential theft, component compromise or denial of service. Radio-frequency performance can change with congestion, jamming and new waveforms. Security belongs in mission availability.

The target should maintain threat models, secure development, component provenance, access control, cryptographic management, update integrity, vulnerability handling and incident response. Tests should include degraded networks and authorised adversarial assessment. External interfaces should have owners and monitored trust boundaries.

The buyer should inspect open vulnerabilities, exceptions, incidents and customer obligations. It should identify foreign-source components and remote support dependencies. Cyber and spectrum remediation can affect delivery, accreditation and export; these costs belong in the valuation model.

20. ESTABLISH PRODUCTION AND DEPLOYMENT READINESS

A successful prototype does not establish repeatable site deployment. The buyer should evaluate bills of materials, suppliers, tooling, test equipment, calibration, quality, yield, lead time, field installation and acceptance. Site surveys and civil works can control schedule even when equipment is available.

The target should reconcile forecast deployments with purchase commitments and trained teams. Configuration changes should flow through production, installation and support. Customer-specific hardware and software forks should be visible. The model should include spares and replacement cycles.

Diligence should stress schedules for component shortage, redesign, licence delay and failed acceptance. Working capital can rise before milestone payments. Backlog should be reduced for production, site and cash constraints rather than valued at contract face value.

21. TEST SOFTWARE UPDATE AND ADAPTATION ECONOMICS

Threats can evolve faster than traditional procurement cycles. Adaptation may require new signatures, models, rules, interfaces, sensors or response options. The supplier's update system can therefore be as valuable as the initial configuration.

The target should show release frequency, test coverage, regression evidence, security approval, customer acceptance and rollback. Emergency updates should not bypass safety and authority. A change that improves one threat class may increase false alarms or affect interoperability elsewhere.

The commercial model should identify which updates are included, licensed or separately funded. Recurring revenue should correspond to measurable service and rights. The acquirer should price the people, data and test infrastructure needed to maintain adaptation after key founders or programme experts leave.

22. CONTROL INTELLECTUAL PROPERTY, DATA AND TECHNICAL RIGHTS

The system may combine company software, government-funded development, third-party components, open-source code, sensor data, customer tracks and classified or controlled information. Ownership, access and export rights can differ. Possession of code does not establish an unrestricted right to use or transfer it.

The target should map inventions, funding, assignments, licences, markings, interfaces, training data and deployment data. It should identify customer rights and restrictions on reuse. Data retention and privacy obligations can differ by site.

The buyer should compare proprietary claims with deliverables and contracts. It should inspect escrow, source access and supplier continuity. Technical rights determine whether the acquirer can support installed systems, integrate its products and export the configuration.

23. MAP EXPORT CONTROLS AND MARKET ACCESS

Counter-drone hardware, software, technology, technical data and services can be controlled by jurisdiction, classification, destination, end user and end use. U.S. ITAR and EAR requirements and UK strategic export controls require configuration-specific analysis. Sanctions, retransfer and foreign-investment review can also affect a transaction.

The target should maintain written classifications and licence records prepared with appropriate expertise. Demonstrations, remote access, training and post-close integration should be included. A past licence does not establish permission for a new customer, investor or configuration.

The buyer should divide markets into currently supportable, approval-dependent and excluded categories. Revenue and synergy should follow current evidence. Pending permissions can support milestones or conditions precedent, with current professional advice obtained for each transaction.

24. TEST CONTRACTS, BACKLOG AND PROCUREMENT EVIDENCE

Counter-drone demand can appear as a funded contract, framework, trial, grant, memorandum, option or public announcement. These instruments have different commercial certainty. The backlog register should record authority, funding, configuration, site, deliverable, acceptance, schedule, cancellation, export condition, margin and cash milestone.

The buyer should trace each material claim to executed documents and customer records. It should separate contracted backlog from options and pipeline. Trials can create evidence and relationships while remaining distinct from recurring deployment.

Sampling should cover the largest, oldest, lowest-margin and most conditional awards. The model should include site readiness, customer dependencies and acceptance failures. Backlog earns value when it can be delivered, accepted, supported and collected.

25. ANALYSE SERVICE, SUPPORT AND AVAILABILITY ECONOMICS

Installed systems require monitoring, calibration, maintenance, spares, updates, training, incident support and reporting. Service obligations can create durable revenue and substantial cost. The target should allocate labour, travel, inventory, hosting and warranty by site and contract.

Availability should be measured against contractual service windows. Planned maintenance, customer-caused outages and force-majeure treatment should be transparent. Remote support can improve economics while creating security, sovereignty and staffing requirements.

The buyer should inspect ticket volumes, mean restoration time, repeat faults, spare consumption and service credits. It should determine whether margins include the cost of threat adaptation and test infrastructure. Revenue persistence should follow accepted service performance and renewal evidence.

26. SEGMENT CUSTOMERS BY MISSION AND AUTHORITY

Military users, airports, critical infrastructure operators, law-enforcement agencies, prisons, events and commercial facilities can have different needs and permissions. The same technical product can require different operating concepts and commercial models. A broad addressable-market slide should not be treated as executable demand.

The vendor should identify the buyer, operator, authority, beneficiary and budget for each segment. It should state whether the offering is detection, decision support, managed service, integration or authorised mitigation. Procurement cycles and evidence requirements should be mapped.

The acquirer should value segment expansion only where product, authority, channel and support evidence exist. Partnerships with authorised agencies or primes can create access while sharing economics and control. The customer map should show who accepts performance and who pays.

27. BUILD THE CUSTOMER-VALUE LEDGER

Customer value can include avoided interruption, reduced response time, improved situational awareness, more efficient deployment of authorised teams and better evidence after an incident. Each component requires a baseline, attribution method and time period. Avoided catastrophe should not be booked as recurring value without a governed scenario model.

The hypothetical target claims USD 18.4 million of annual customer value across 46 sites. Evidence review retains 31 sites and USD 7.2 million after coverage, false-alarm, authority, capacity and persistence adjustments. These numbers are illustrative management assumptions only.

The ledger should prevent duplication. Reduced downtime and avoided revenue loss can describe the same event. Operator savings should exclude staff retained for legal or resilience reasons. The customer should confirm which outcome supports purchase and renewal.

Table 2. Hypothetical annual customer-value ledger

Proposed value component	Management case	Evidence retained	Principal adjustment
Avoided operational interruption	USD 7.0m	USD 2.8m	Incident baseline and attribution
Faster detection and decision	USD 4.1m	USD 1.7m	Coverage, false alarms and authority
Efficient authorised response	USD 3.6m	USD 1.2m	Mission completion and saturation
Evidence, compliance and recovery	USD 3.7m	USD 1.5m	Process adoption and persistence
Total annual customer value	USD 18.4m	USD 7.2m	Governed evidence gates

Every number is an illustrative management assumption, not observed customer or programme data.

28. BUILD THE TRANSACTION VALUATION BRIDGE

The hypothetical target has 18 customers, 46 protected sites, USD 28.0 million of annual revenue, USD 96 million of management-reported backlog and a claimed 92 percent detection rate. Management proposes USD 12.6 million of buyer revenue and synergy. These figures are illustrative management assumptions.

Evidence gates retain 31 accepted or supportable sites, USD 41 million of funded and executable backlog and a 74 percent evidence-weighted mission-completion rate within defined test conditions. Revenue and synergy fall to USD 4.6 million after customer, authority, integration, production, support and cash adjustments.

The bridge does not produce a valuation opinion. It produces evidence-adjusted inputs that can enter the buyer's selected cash-flow, market or transaction method. IFRS 3, IFRS 13 and IAS 38 provide relevant accounting context for combinations, fair value and identifiable intangible assets; transaction-specific accounting judgement remains necessary.

Table 3. Hypothetical buyer revenue and synergy bridge

Component	Management case	Evidence-adjusted case	Evidence gate
Revenue retained	6.8	2.8	Funding, acceptance, support and cash
Cross-sell to existing sites	2.4	0.7	Authority, site fit and customer evidence
Integration and procurement synergy	2.0	0.7	Interfaces, capacity and delivery
Data and software synergy	1.4	0.4	Rights, security and model transferability
Total	12.6	4.6	No duplication with customer value

Values are illustrative management assumptions in USD millions.

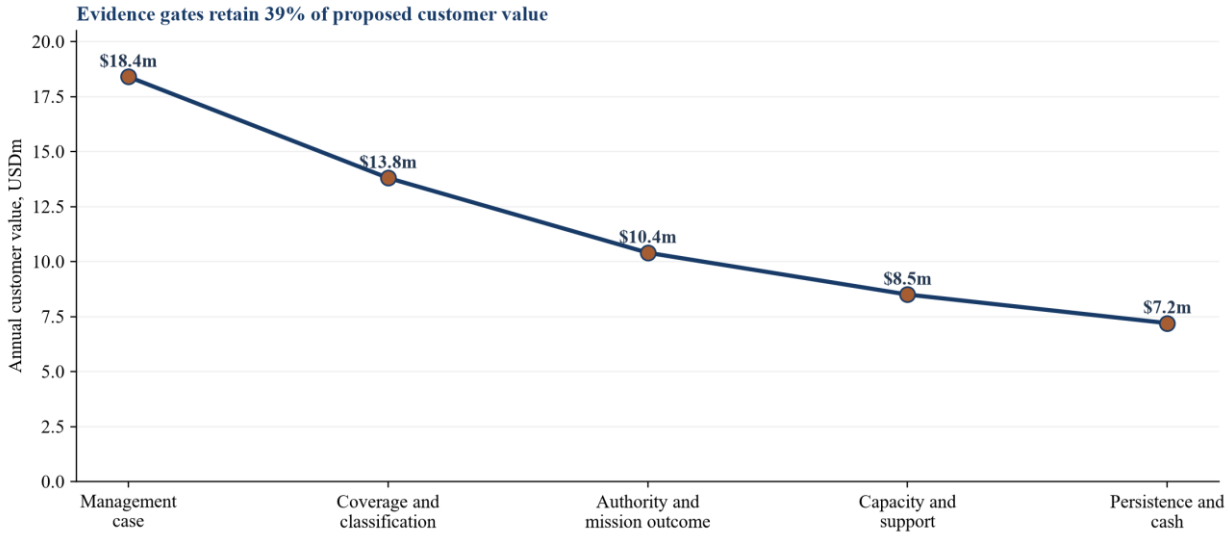

Figure 4. Hypothetical customer-value validation bridge

Values in USD millions are illustrative management assumptions.

29. TRANSLATE EVIDENCE INTO PRICE AND TRANSACTION TERMS

Accepted sites, funded backlog, controlled configurations and supportable rights can receive value at signing. Expansion into new threats, jurisdictions, customer segments and response methods can be funded through milestones. Each milestone should reference an observable outcome and responsible evidence owner.

Representations should cover contracts, test evidence, performance claims, legal authority statements, export controls, intellectual property, data rights, cybersecurity, incidents, production and service obligations. Holdbacks or targeted indemnities can address defined exposures. Integration budgets should include site, security, testing and support work.

Earn-outs require careful definitions. Government appropriations, customer authority and licence timing can sit partly outside management control. Revenue targets should state treatment of hardware pass-through, pilots, delayed acceptance, service credits, options and buyer-led cross-sell. Collected cash provides a stronger endpoint than an unsigned opportunity.

30. EXECUTE THE DILIGENCE WORKPLAN

The request list should include the threat register, protected-site inventory, configurations, coverage models, raw event logs, test plans, ground truth, model documentation, command workflows, authority analyses, safety cases, response records, interfaces, incidents, intellectual-property rights, export files, production records, service tickets, contracts and financial models.

Sampling should cover material customers, recent software, difficult environments, false alarms, missed detections, simultaneous tracks, failed responses and high-risk suppliers. Data access should respect security and legal controls. An authorised reviewer can record a transaction conclusion without copying protected content into an unrestricted data room.

The buyer should reconcile technical evidence with contracts and invoices. A site described as deployed may still be in trial, unavailable or awaiting acceptance. A recurring software fee may

include substantial operator or integration labour. Diligence should connect mission, obligation, cost and cash.

31. GOVERN THE FIRST ONE HUNDRED DAYS

The first thirty days should freeze inventories, confirm access, protect evidence and reconcile sites, contracts, versions and authorities. Days thirty-one to sixty should reproduce material metrics, close priority safety and security gaps and confirm customer acceptance. Days sixty-one to one hundred should harmonise testing, change, support, export and board reporting.

Integration should sequence identities, networks, source code, models, customer systems, licences and operational authority. Synergy should begin after lawful access and validated migration. Rapid technical consolidation can destroy configuration history or interrupt a protected service.

Board reporting should show protected hours, credible tracks, false alarms, decision latency, authorised responses, mission outcomes, simultaneous-track capacity, availability, open deficiencies, funded backlog, site margin, working capital and collected cash. One readiness score can conceal the source of risk.

Table 4. Diligence gates and first-one-hundred-day ownership

Workstream	Pre-close evidence	Day-one control	Day-one-hundred outcome
Mission and threat	Site and threat registers	Scope and version freeze	Governed mission estate
Detection and AI	Raw tests, models and limitations	Monitoring and change control	Reproduced performance baseline
Authority and response	Legal analysis, safety case and logs	Approval and escalation controls	Auditable authorised workflow
Delivery and support	Suppliers, acceptance and service data	Configuration and incident control	Validated availability plan
Commercial	Contracts, margin, working capital and cash	Backlog reconciliation	Evidence-adjusted integration case

Evidence owners should be named before close and remain accountable through integration.

32. RECOGNISE LIMITATIONS AND CONCLUDE

This framework does not validate a counter-drone product, legal authority, military mission, export classification, licence or transaction. Requirements vary by jurisdiction, customer, technology and fact. Current legal, safety, technical, export, security, accounting and procurement advice is required.

The hypothetical case does not estimate threat frequency, mission effectiveness, customer demand or transaction value. Public announcements about firing cost and trial success establish context. They do not establish total system economics or the status of a private company. Sensitive evidence should remain within authorised review channels.

The practical conclusion is that cost per interception is a governed outcome metric. The protected mission must be defined. Detection and identification must perform in representative conditions. Authority and safety must permit action. The response must complete the mission within capacity. Production and support must sustain the configuration. Contracts and cash must remain executable.

A low marginal response cost can be valuable. The strongest procurement and acquisition case connects threat, sensor, track, decision, authority, response, recovery, support and cash. That chain allows boards to compare architectures, price evidence and fund adaptation without treating one demonstration or headline cost as a complete defence.

REFERENCES

[1] U.S. Department of Defense. Fact Sheet: Department of Defense Strategy for Countering Unmanned Systems, December 2024. https://media.defense.gov/2024/Dec/05/2003599149/-1/-1/0/FACT-SHEET-STRATEGY-FOR-COUNTERING-UNMANNED-SYSTEMS.PDF

[2] U.S. Department of Defense. DoD Announces Strategy for Countering Unmanned Systems, December 2024. https://www.defense.gov/News/Releases/Release/Article/3986597/dod-announces-strategy-for-countering-unmanned-systems/

[3] U.S. Department of Defense. Counter-Small Unmanned Aircraft Systems Strategy, January 2021. https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF

[4] NATO Communications and Information Agency. Allies and industry test the latest counter-drone technology during NATO exercise, May 2026. https://www.ncia.nato.int/newsroom/news/allies-and-industry-test-the-latest-counterdrone-technology-during-nato-exercise

[5] NATO Communications and Information Agency. NATO tests counter drone technology during interoperability exercise, September 2024. https://www.ncia.nato.int/about-us/newsroom/nato-tests-counter-drone-technology-during-interoperability-exercise

[6] U.S. Government Accountability Office. Science and Technology Spotlight: Counter-Drone Technologies, GAO-22-105705, May 2022. https://www.gao.gov/products/gao-22-105705

[7] Federal Aviation Administration. UAS Detection, Mitigation, and Response on Airports, updated June 2025. https://www.faa.gov/airports/new_entrants/uas_detection_mitigation_response

[8] U.S. Department of Justice, FAA, DHS and FCC. Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems, August 2020. https://www.faa.gov/sites/faa.gov/files/uas/resources/c_uas/Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf

[9] Federal Aviation Administration. UAS Detection and Mitigation Systems Aviation Rulemaking Committee Final Report, 2024. https://www.faa.gov/regulations_policies/rulemaking/committees/documents/index.cfm/document/information/documentID/6104

[10] UK Ministry of Defence. Defence Drone Strategy: the UK's approach to Defence Uncrewed Systems, February 2024. https://www.gov.uk/government/publications/defence-drone-strategy-the-uks-approach-to-defence-uncrewed-systems

[11] UK Ministry of Defence and Defence Science and Technology Laboratory. Cutting-edge drone killer radio wave weapon developing at pace, May 2024. https://www.gov.uk/government/news/cutting-edge-drone-killer-radio-wave-weapon-developing-at-pace

[12] UK Ministry of Defence. Boost for Armed Forces as new laser weapon takes down high-speed drones, November 2025. https://www.gov.uk/government/news/boost-for-armed-forces-as-new-laser-weapon-takes-down-high-speed-drones

[13] UK Ministry of Defence and Defence Science and Technology Laboratory. British Army successfully tests new drone-destroying laser, December 2024. https://www.gov.uk/government/news/british-army-successfully-tests-new-drone-destroying-laser

[14] U.S. Department of State, Directorate of Defense Trade Controls. International Traffic in Arms Regulations. https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987

[15] Electronic Code of Federal Regulations. 22 CFR Part 121, United States Munitions List. https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-121

[16] U.S. Department of Commerce, Bureau of Industry and Security. Export Administration Regulations. https://www.bis.gov/ear

[17] UK Government. UK Strategic Export Controls. https://www.gov.uk/guidance/uk-strategic-export-controls

[18] UK Government. Export Controls: Military Goods, Software and Technology. https://www.gov.uk/guidance/export-controls-military-goods-software-and-technology

[19] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework. https://www.nist.gov/itl/ai-risk-management-framework

[20] IFRS Foundation. IFRS 3 Business Combinations. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

[21] IFRS Foundation. IFRS 13 Fair Value Measurement. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/

[22] 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/

[23] 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.