AEGEAN INTELLIGENCE GROUP

PUBLISHABLE MARKET RESEARCH · 2026

CLASSIFICATION
PUBLIC

PRODUCT ID
PMR-2026-0619-USA-003

TIMELINESS
CURRENT

DATE
2026-06-19

The Authority Gap

The Drone Threat Outran the Authority to Stop It. A New Law Cracks the Door, the Rulebook Is Late, and a Market Is Forming in the Space Between.

~350

DRONE INCURSIONS OVER 100+ US MILITARY BASES IN 2024

479

DRONE INCIDENTS AT FEDERAL PRISONS IN 2024, UP 20X FROM 2018

$3.2-8.4B

2025 COUNTER-DRONE MARKET ESTIMATES, GROWING ~25% A YEAR

EXECUTIVE DASHBOARD

Drones now cross into the airspace over American military bases, prisons, airports, power plants, and stadiums as a matter of routine. The technology to detect them is mature and for sale. The authority to stop them, until December 2025, belonged to just four federal departments, and to no one else. This brief maps the threat, the legal gap that defined the US response, the new statute that begins to close it, and the market forming in between.

THESIS

The binding constraint on America's drone problem is not detection technology, which is mature and widely sold, but **legal authority to act**: until the December 2025 SAFER SKIES Act, only four federal agencies could lawfully bring a drone down, while every stadium, utility, data center, prison, and private estate could at most watch. The new law reauthorizes federal authority and, for the first time, opens a path for state and local agencies to mitigate, but it is **gated behind certification and a rulebook that is already late**. The threat is established and the capability exists; the market and the protection it enables will be decided by how fast authority catches up to both.

KEY STATISTICS

~350
drone incursions over 100+ US military installations in 2024 (NORTHCOM)[1]

479
federal-prison drone incidents in 2024, ~20x the 23 logged in 2018[7]

>100/mo
drone sightings near US airports; drones in ~2/3 of 2024 top-airport near-misses[5, 6]

2,845
unauthorized drones over NFL games in 2023, from ~12 in 2017[9]

0.05%
share of 240,000+ eligible events the FBI can actually cover for counter-drone[7]

$20B / $5B
Anduril and Raytheon US Army counter-drone contract ceilings[14, 15]

Oct 2025
federal counter-drone mitigation authority lapsed entirely during the shutdown[23]

Dec 2025
SAFER SKIES Act: first state/local mitigation path; rules due ~June 2026[24, 25]

Scope & method. Open-source intelligence verified against allowlisted Tier 1 to 3 sources per AEIG source policy. Incursion counts are detection events reported by government officials and agencies, not confirmed hostile drones; unverified sighting clusters are flagged as such. Criminal matters are drawn from charges and are noted as unproven, with defendants presumed innocent. Market-size estimates diverge widely across vendors and are presented as a range; contract figures are multi-year ceilings unless stated. Battlefield casualty and strike-share figures are self-reported by combatants and flagged. Geographic focus is the United States, with foreign incidents where they establish a pattern. Timeliness: CURRENT, with the legal framework moving on the cadence of the 2026 rulemaking.

KEY JUDGMENTS

Six judgments anchor this assessment. Each is tied to cited evidence in the sections that follow and carries an explicit confidence level.

1 High — Drone incursions over US bases, prisons, airports, and stadiums are now routine and measured, not anomalous: roughly 350 over military installations, 479 at federal prisons, and 2,845 over NFL games in a single season.[1, 7, 9]

2 High — The December 2024 Northeast "drone wave" was, on a four-agency federal assessment, largely unverified sightings with no foreign nexus, yet it forced a runway closure and a governor's plea for authority. The real exposure it revealed is an authorities-and-capacity vacuum, not an invasion.[3, 4]

3 High — Until December 2025, only four federal departments could lawfully mitigate a drone. Shooting one is a felony and jamming one violates FCC law, with no exemption for police, venues, or private owners, so the most exposed parties could only detect.[19, 20, 21, 22]

4 Moderate — Battlefield proliferation has made cheap, capable attack drones a homeland and VIP threat: documented cartel weaponized-drone use, ~1,000 monthly border incursions, and a drone strike on the Israeli prime minister's residence. US-soil weaponization has not yet occurred, but the vector is open.[27, 30, 32]

5 Moderate

The SAFER SKIES Act (December 2025) reauthorizes federal authority to 2031 and creates a first state and local mitigation pathway, but it is gated behind training, certification, and implementing rules due around June 2026. The door is open; the rulebook is late.[24, 25]

6 Moderate

The counter-drone market is real and fast-growing but poorly bounded, with 2025 estimates ranging $3.2 to $8.4 billion at roughly 25 percent annual growth. The durable signal is the contract spine and a forming commercial segment that cannot yet lawfully self-mitigate.[11, 13, 14, 33]

SECTION 01 · THREAT

The Sky Filled Up

Incursions over sensitive American airspace are now a measured, recurring fact across military, carceral, aviation, energy, and event domains, even after the most famous episode turned out to be mostly misperception.

In 2024 the US military detected roughly 350 drone incursions over more than 100 installations, the NORAD and Northern Command commander told the Senate; unidentified drones flew over Langley Air Force Base for 17 consecutive days beginning in December 2023, and officials have logged more than 600 incursions over military sites since 2022, with about half of bases assessed as lacking adequate tracking.[1, 2]

The pattern repeats across civilian infrastructure. Federal prisons logged 479 drone incidents in 2024, roughly twentyfold the 23 reported in 2018, with detection installed at only 64 of 121 facilities; one drone intercepted over a South Carolina prison carried 464 grams of fentanyl.[7, 35] The FAA receives more than 100 drone sightings near airports every month, and drones featured in nearly two-thirds of reported near-midair collisions at the 30 busiest US airports in 2024, while nuclear plants reported a sharp rise in sightings under a new mandatory-reporting rule.[5, 6, 8]

Mass events are the most exposed soft target. The NFL recorded 2,845 unauthorized drone incursions over its stadiums during the 2023 season, up from about a dozen in 2017, a drone paused the January 2024 AFC Championship mid-game, and during the 2026 FIFA World Cup federal officials recorded 145 incursions across eight venues in a single week.[9, 10] The most-publicized episode, the December 2024 wave of sightings across New Jersey and the Northeast, generated about 5,000 tips but, on a four-agency federal assessment, no foreign nexus and no confirmed threat; even so, Stewart

International Airport briefly closed its runways and New York's governor demanded counter-drone authority for the states.[3, 4]

ASSESSMENT · HIGH CONFIDENCE

The drone-incursion problem is now structural and quantified across bases, prisons, airports, nuclear sites, and stadiums, not a passing anomaly. The strategic point is that the December 2024 Northeast wave was, on the evidence, mostly misperception, yet it still produced runway closures and a call for emergency authority. That reveals the true exposure: not a confirmed attack wave but an authorities-and-capacity vacuum into which both real incursions and public alarm rush. Reading the threat as either an invasion or a hoax misses it; the constant is that the airspace over sensitive sites is contested and largely undefended.

Rationale: NORTHCOM, Bureau of Prisons, FAA, and NFL counts establish routine incursion; the four-agency joint statement establishes the perception gap; the Stewart closure shows the operational consequence regardless of attribution.

SECTION 02 · PROLIFERATION

The Battlefield Came Home

The threat is cheap because war made it cheap, and the tactics are already migrating from Ukraine and the Middle East to cartels, smugglers, and attacks on principals and infrastructure.

Russia has launched more than 14,700 one-way attack drones at Ukraine; a leading think tank calculated a cost of roughly $350,000 per target struck even at a failure rate near 90 percent, far below the price of a cruise missile.[27] Ukraine reported some 819,737 video-confirmed drone hits in 2025 and its president claimed more than 80 percent of battlefield strikes are now drone-delivered, a self-reported figure but a directional one, while planning to field up to 4.5 million first-person-view drones in a single year.[28]

Those tactics are migrating. A federally funded study documented 221 weaponized-drone incidents attributed to Mexican cartels between 2021 and 2025, 27 of them fatal; US Northern Command reports roughly 1,000 drone incursions a month across the southern border, overwhelmingly for smuggling and surveillance, though cartels have not yet weaponized drones on US soil.[30, 31] Drones have also become an instrument against principals: in October 2024 three drones were flown at the Israeli prime minister's private residence, one of which struck the home roughly 70 kilometers from the border without triggering sirens.[32]

The newest frontier is commercial infrastructure. In March 2026, drone strikes damaged three Amazon Web Services data centers in the Gulf, the first widely reported physical drone attacks on commercial cloud infrastructure, an overseas event but a clear signal of trajectory.[34] The throughline, as a leading defense research institute put it, is that cheap drones have democratized precision strike and ended the era in which distance kept the homeland a sanctuary.[29]

ASSESSMENT · MODERATE CONFIDENCE

Battlefield drone proliferation has converted a military problem into a homeland and personal-security one, and the migration path, through cartels, smugglers, and lone actors, is visible rather than hypothetical. Confidence is moderate on US-soil weaponization specifically, which has not yet occurred, but the trajectory is firm: the technology, tactics, and intent are documented abroad, and the border-incursion volume shows the vector is open. The planning implication is that estate, event, and infrastructure security can no longer treat aerial attack as a state-only threat.

Rationale: Cost-effectiveness math and Ukraine scale establish proliferation; the cartel dataset and border-incursion volume establish migration; the residence strike and data-center hits establish the VIP and infrastructure vector; the US-soil weaponization caveat is stated explicitly.

SECTION 03 · AUTHORITY

Cleared to Watch, Not to Act

The defining feature of the US drone response is legal, not technical. For years only four federal agencies could mitigate a drone; the authority then lapsed entirely, and a new statute now begins to widen it.

Until late 2025, only four federal departments, Defense, Energy, Homeland Security, and Justice, held statutory authority to mitigate a drone, that is, to jam, seize, or down one, under the 2018 Preventing Emerging Threats Act.[19, 20] Everyone else, state and local police, airport and stadium operators, utilities, and private owners, was limited to detection. Shooting a drone is a federal felony under the aircraft-sabotage statute, punishable by up to twenty years, and jamming its signal independently violates FCC law, with no exemption for police or private parties.[21, 22]

That framework proved fragile. The federal authority ran on a chain of short-term extensions and then lapsed entirely on October 1, 2025, during the longest government shutdown in US history, leaving even federal agencies able to detect but not mitigate for several weeks before a stopgap restored it.[23] The episode made the structural weakness impossible to ignore on the eve of a year of mega-events.

The fix arrived in December 2025. The SAFER SKIES Act, enacted within the FY2026 defense authorization, reauthorized federal counter-drone authority through 2031, gave the Energy Department explicit authority over nuclear sites, and, for the first time, created a pathway for certified state, local, tribal, and territorial police and corrections agencies to mitigate drones.[24, 25] But the authority is gated: agencies may act only after federal training and certification, the implementing regulations were due roughly 180 days after enactment, around June 2026 and timed to the FIFA World Cup, and unauthorized counter-drone action carries penalties up to $100,000. A permanent DHS program office to coordinate it stood up in January 2026.[26]

ASSESSMENT · HIGH CONFIDENCE

The binding constraint on US drone defense is authority, not capability, and the SAFER SKIES Act has changed the legal frame without yet changing the operational reality. The implication is twofold: the universe of entities that may lawfully act is expanding from four federal agencies toward thousands of police and corrections departments, which is the single largest driver of future counter-drone demand; but until the rulemaking publishes and certification scales, almost every stadium, utility, data center, and estate remains legally able only to detect. Capability bought ahead of authority sits idle; authority granted ahead of rules sits unused.

Rationale: The 2018 statute, the aircraft-sabotage felony, and the FCC jamming bar establish the pre-2025 lock; the October 2025 lapse shows the fragility; SAFER SKIES plus the pending mid-2026 rulemaking and certification gating establish the open-but-unrealized state.

SECTION 04 · MARKET

A Market Forming in the Gap

Counter-drone is real, fast-growing, and badly measured. The defensible evidence is not the headline market size but the contract flow and the structural expansion of who is allowed to buy mitigation.

Estimates of the 2025 global counter-drone market range from about $3.2 billion to $8.4 billion depending on whether the scope is detection-only or full mitigation, and defense-only or commercial, a spread of more than two to one, with most firms clustering the growth rate near 25 percent a year.[11, 12, 13] The honest read is a market expanding quickly off an uncertain base, not a precise figure.

The defensible signal is the contract spine. The US Army awarded Anduril a counter-drone-focused contract worth up to $20 billion in 2026 and RTX a roughly $5 billion Coyote-interceptor deal in 2025, both multi-year ceilings; the pure-play DroneShield reported 2025 revenue of about A$217 million, up nearly 280 percent; Axon acquired Dedrone; and Epirus, Fortem, and D-Fend drew fresh contracts and

capital for high-power-microwave, net-capture, and radio-frequency-takeover mitigation.[14, 15, 16, 17, 18] Detection still outweighs any single mitigation method in spend, but non-kinetic mitigation is the fastest-growing layer.

The commercial and private segment is the newest and least mature. Counter-drone systems for events and estates are quoted from under $100,000 for radio-frequency detection to $500,000 or more for radar, and named entrants are courting stadiums, data centers, and high-net-worth residences. Demand is being pulled by concrete incidents: law enforcement has tied drones to reconnaissance for burglaries of wealthy homes, and a professional sports league warned its teams that organized theft crews were using drones to surveil players' residences.[33]

ASSESSMENT · MODERATE CONFIDENCE

The counter-drone market's headline size is the weakest part of the story; the durable evidence is the contract flow and the structural expansion of who is allowed to buy and use mitigation. The distinction that matters for a buyer is between detection, which is lawful, available, and already being procured by venues and estates, and mitigation, which until certification remains effectively a federal-agency function. Confidence is moderate because market sizing is vendor-driven and the commercial segment is young, but the direction, toward a layered detection market now and a much larger mitigation market as state and local certification scales, is clear.

Rationale: The cross-vendor sizing divergence flags the soft number; the Anduril, Raytheon, and DroneShield figures and the detection-versus-mitigation split are the hard spine; the private-estate pricing and the burglary-reconnaissance incidents establish the emerging commercial demand.

SECTION 05 · EXPOSURE

The Buyer Cannot Yet Buy the Solution

For the parties most exposed, the threat is legal to detect and illegal to stop. The near-term answer is an owned, layered airspace posture, not premature mitigation hardware that cannot be lawfully used.

The practical situation is paradoxical: a stadium can know a drone is overhead and cannot bring it down; a utility can map an incursion and must call a federal agency that can cover only a fraction of requests; a private estate can install radar and remains barred from jamming. The FBI itself testified it can provide counter-drone coverage for roughly 0.05 percent of the more than 240,000 events eligible for it.[7]

This is why the posture that matters now is layered and lawful: detection and airspace awareness, hardening and response planning, coordination with the agencies that hold mitigation authority, and

readiness to adopt mitigation the moment certification allows it. The SAFER SKIES pathway will, over time, let qualified police and corrections agencies act, reshaping the protective model for events and corrections first and private venues later, but only after training, certification, and the reconciliation of the new authority with the standing prohibitions on jamming and downing.[24, 25]

The exposure also converges with the personal-security and infrastructure problems mapped elsewhere. A drone is simultaneously a surveillance platform that feeds physical targeting, a delivery system for contraband or explosives, and a tool of disruption against the data centers and grid nodes everything else depends on. Treating it as a niche aviation nuisance underprices it; treating airspace as a security domain to be owned, monitored, and integrated with physical and cyber posture is the adjustment the threat now demands.

ASSESSMENT · HIGH CONFIDENCE

The counter-drone problem is, for most buyers, currently unsolvable by procurement alone, because the law reserves the decisive action to federal agencies and, soon, to certified police, not to the venue or principal under threat. The near-term investment that pays is detection, awareness, and an integrated airspace-security posture coordinated with those who hold mitigation authority, not premature purchase of mitigation hardware that cannot be lawfully used. The organizations that win treat their airspace as part of an owned, converged security surface and are positioned to add mitigation the day certification permits it.

Rationale: The FBI 0.05 percent coverage figure and the detection-versus-mitigation legal split establish the procurement paradox; the SAFER SKIES certification pathway establishes the forward path; the convergence with surveillance, contraband, and disruption establishes why airspace must be owned, not left to chance.

SECTION 06 · OUTLOOK

Three Scenarios, Twelve Months

Construction confidence reflects analytical quality, not probability. Each scenario carries a risk velocity and the signal that would confirm it.

Baseline · The rules slip, the gap persists

CONSTRUCTION CONFIDENCE: HIGH · VELOCITY: GRADUAL

The SAFER SKIES implementing rules publish late or as interim guidance; federal agencies retain practical mitigation authority while state and local certification rolls out slowly. Incursions continue at 2024 to 2025 levels across bases, prisons, airports, and events. Venues, utilities, and estates keep buying detection while mitigation stays a federal function, and the market grows on detection plus defense contracts rather than broad commercial mitigation.

SIGNAL TO WATCH: THE MID-2026 RULEMAKING DEADLINE SLIPS OR PUBLISHES AS INTERIM GUIDANCE; CERTIFIED STATE AND LOCAL AGENCIES NUMBER IN THE LOW SINGLE DIGITS

Deterioration · A successful soft-target strike

CONSTRUCTION CONFIDENCE: MODERATE · VELOCITY: RAPID

A weaponized or disruptive drone causes casualties or a major outage at a US event, airport, data center, or grid node. Political pressure forces emergency authority and spending; demand spikes into a market and a certification pipeline that cannot absorb it; liability and insurance for venues and operators reprice sharply. The threat narrative shifts from nuisance to national priority in days.

SIGNAL TO WATCH: A CONFIRMED WEAPONIZED-DRONE INCIDENT ON US SOIL; AN EMERGENCY EXPANSION OF MITIGATION AUTHORITY OR FUNDING

Stabilization · Layered defense normalizes

CONSTRUCTION CONFIDENCE: LOW-MOD · VELOCITY: STRUCTURAL

The rulemaking lands, state and local certification scales to police and corrections, the jamming and downing prohibitions are reconciled with the new authority, and layered detect-plus-mitigate becomes standard at events, prisons, and critical infrastructure, then private venues. The market matures toward mitigation, and airspace security becomes a normal security line item rather than a federal exception.

SIGNAL TO WATCH: PUBLISHED FINAL RULES PLUS A GROWING ROSTER OF CERTIFIED STATE AND LOCAL AGENCIES; INSURER OR VENUE STANDARDS THAT CITE A COUNTER-DRONE POSTURE

ASSESSMENT · MODERATE CONFIDENCE

Across all three paths the threat is established and the authority is the variable. Baseline, a slow rule-out with the gap intact, is the most probable twelve-month path; Deterioration is a fast, lower-probability, high-impact risk that a single successful strike would trigger; Stabilization is the slow structural endpoint that depends on rulemaking and certification rather than technology. For any exposed operator the planning constant is the same: invest in detection and an owned airspace posture now, and be positioned to add mitigation the moment it becomes lawful.

Rationale: Incursion data is settled; SAFER SKIES timing and certification are the swing factors; the procurement paradox makes a detection-first, mitigation-ready posture the dominant strategy under every scenario.

SOURCE REGISTRY

1. DefenseScoop, "NORAD commander says hundreds of drone incursions were detected at US military installations," 2025.
2. The Hill, "Pentagon confirms 'incursions' of unauthorized drones over Air Force base," 2024.
3. DHS / FBI / FAA / DoD, "Joint Statement on Ongoing Response to Reported Drone Sightings," 2024.
4. Office of Governor Kathy Hochul, "Statement by Governor Hochul on Additional Drone Activity (Stewart International Airport)," 2024.
5. U.S. Federal Aviation Administration, "Drone Sightings Near Airports," 2026.
6. CBS News / Associated Press, "Drones in near midair collisions with planes at major U.S. airports an increasing danger," 2025.
7. FBI / U.S. Department of Justice, "Securing the Skies, Statement to the Senate Judiciary Committee," 2025.
8. U.S. Nuclear Regulatory Commission / The War Zone, "Drones and Nuclear Power Plant Security; uptick in reported sightings," 2024.
9. U.S. House Committee on Homeland Security, "Statement of Cathy L. Lanier, Chief of Security, National Football League," 2024.
10. U.S. Department of Justice (USAO Western District of Missouri), "Drones Seized and Violation Notices Issued During FIFA World Cup Events," 2026.
11. MarketsandMarkets, "Counter-UAS Systems Industry worth $20.31 billion by 2030," 2025.
12. Grand View Research, "Anti-drone Market Size, Share, Growth, Industry Report," 2026.
13. Fortune Business Insights / Precedence Research, "Counter-UAS Market size estimates (divergent)," 2026.
14. DefenseScoop, "Army awards Anduril $20B contract with an eye toward counter-drone capabilities," 2026.
15. The Defense Post, "US Army Awards Raytheon $5 Billion Deal for Coyote Counter-UAS System," 2025.
16. Investing.com / DroneShield, "DroneShield FY2025 results: revenue up ~277%," 2026.
17. Axon / PR Newswire, "Axon to acquire Dedrone," 2024.

18. Epirus, "Epirus Receives $43.5 Million Contract from U.S. Army for IFPC-HPM Generation II Systems," 2025.
19. U.S. Code, "6 U.S.C. 124n (Preventing Emerging Threats Act of 2018)," 2018.
20. U.S. Department of Homeland Security, "Counter-Unmanned Aircraft Systems Legal Authorities Fact Sheet," 2019.
21. Legal Information Institute, Cornell Law School, "18 U.S.C. 32, Destruction of aircraft or aircraft facilities," 2024.
22. U.S. Federal Communications Commission, "Jamming Cell Phones and GPS Equipment is Against the Law," 2024.
23. DRONELIFE, "Counter-UAS Authority Expires Amid Government Shutdown," 2025.
24. U.S. Congress, "SAFER SKIES Act, FY2026 National Defense Authorization Act (Title LXXXVI)," 2025.
25. DRONELIFE, "NDAA FY 2026: Key Counter-UAS Provisions Explained," 2025.
26. U.S. Department of Homeland Security, "DHS Launches New Office to Advance Drone and Counter-Drone Technologies," 2026.
27. Center for Strategic and International Studies, "Calculating the Cost-Effectiveness of Russia's Drone Strikes," 2025.
28. Defense News, "Ukraine says more than 80% of enemy targets now destroyed by drones," 2026.
29. Center for a New American Security, "Countering the Swarm: Protecting the Joint Force in the Drone Age," 2025.
30. NCITE (Univ. of Nebraska Omaha) / Small Wars Journal, "Mapping Weaponized Drone Attacks Attributed to Mexican Drug Cartels," 2026.
31. Center for Strategic and International Studies, "The United States Needs a Southwest Drone Wall," 2025.
32. Associated Press, "A drone targets the Israeli prime minister's house," 2024.
33. The Hollywood Reporter, "Using Drones for Peeping, Burglaries on Rise," 2025.
34. DefenseScoop, "Commercial data centers emerge as targets in modern warfare after drones hit 3 AWS facilities," 2026.
35. Facilities Dive, "Prisons battle nightly drone drops of drugs, other contraband," 2026.

AEGEAN INTELLIGENCE GROUP

Publishable Market Research

Timeliness: CURRENT. The structural argument here, a routine drone threat met by a legal-authority gap that a new statute is only beginning to close, is current on a horizon of months. The decisive variable is the SAFER SKIES implementing rulemaking due around mid-2026 and the pace of state and local certification. An Update Addendum will follow on publication of the final rules, a material change in authority, or a significant homeland drone incident.

Classification: PUBLIC. Prepared on open-source intelligence verified against allowlisted sources. Government figures and statements are cited to their published sources; incursion counts are detection events, not confirmed hostile drones; criminal matters are unproven allegations and defendants are presumed innocent; analytic judgments are Aegean's.

contact@aegeanintel.com · aegeanintel.com