Defending Texas Ports From Malicious Drones

Authority Gaps, Emerging Federal Pathways, and Operational Readiness After the FY26 NDAA

WRITTEN BY

Art Wolfskill

Michael Wolfskill

2026

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

Abstract

Unmanned aerial systems (UAS) have transformed the threat landscape for U.S. critical infrastructure, introducing low-cost, high-impact vulnerabilities that traditional security frameworks were not designed to manage. In this paper we examine the rapid evolution of drone misuse by terrorists, criminal organizations, cartels, and lone actors, tracing a trajectory from early military applications to contemporary weaponized, autonomous, and swarm-capable systems. It analyzes major global and domestic incidents to illustrate how commercially available drones are now used for reconnaissance, smuggling, disruption, and kinetic attacks, including attempts targeting power substations, airports, government officials, and high-value petrochemical assets. Particular emphasis is placed on U.S. ports, especially Texas maritime facilities, where unauthorized drone activity has surged and where Area Maritime Security Committees report persistent surveillance flights, potential smuggling operations, and operational interference.

The paper evaluates the complex legal environment governing counter-UAS measures in the United States, detailing the severe limitations imposed on state and local law enforcement, private port operators, and critical infrastructure owners by federal aviation and communications statutes. Although emerging federal authorities permit DHS and DOJ to detect, track, and mitigate malicious drones at designated sites, those powers have not been extended to the local responders who are most likely to encounter imminent threats. Case studies from Texas ports, including documented UAS incursions at Houston, Brownsville, and Galveston, demonstrate the operational consequences of these regulatory gaps.

The legal and regulatory framework governing counter-uncrewed aircraft systems (C-UAS) is undergoing rapid transformation. December 2025 represents a pivotal inflection point in United States drone legislation, marked by the expansion of statutory authorities permitting state and local law enforcement agencies to engage in defensive actions against malicious or unauthorized UAS operations. In this paper we critically examine the historical evolution of UAS-related policies and legal constraints, analyze recent

legislative developments, and evaluate their implications for maritime and port security governance.

Building on the above analysis, the study proposes a set of actionable, legally defensible preparedness measures that port authorities should implement prior to a UAS-related incident in order to mitigate risk, ensure compliance, and enhance resilience against the escalating threat posed by hostile drone activity.

Ultimately, we conclude that ports represent a uniquely exposed sector of critical infrastructure and that effective defense will require both practical operational frameworks and proper implementation of allowances granted by recently expanded legal authorities. For instance, through potential deputization or formal delegation of authority to act, trained local responders can be empowered to interdict malicious drones before federal support can arrive.

Table of Contents

Introduction

Unmanned aerial systems (UAS), or drones, have rapidly expanded the threat landscape for critical infrastructure protection (CIP), particularly in high-value environments such as ports, transportation hubs, and energy facilities. Their small size, low cost, and ease of acquisition allow hostile actors, criminal organizations, and negligent operators to bypass traditional perimeter security and conduct surveillance, smuggling, disruption, and even targeted attacks. To aid in understanding the current risks, we begin with a backgrounder on the development of drones for hostile uses. Appendix I develops specific occurrences in more detail for those who desire further information on historical events.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) warns that drones "can be exploited for pernicious purposes" by terrorists, criminals, or lone actors, underscoring their growing utility as tools for espionage and physical harm (Cybersecurity and Infrastructure Security Agency 2026). This paper focuses exclusively on the risks posed by malicious or unauthorized drone activity and the evolving legal authorities that govern how law enforcement agencies, port authorities, and private infrastructure operators may detect, track, disrupt, or interdict such threats. It examines the current capabilities of commercially available drones, emerging trends such as autonomous navigation and swarming, plausible attack scenarios against ports and other critical assets, and the constraints imposed by federal aviation and communications law. The analysis further evaluates the recently expanded, yet still narrow set of counter-UAS permissions granted under federal statutes, the limitations facing state and local police, and the legal exposure private entities may face when attempting to defend their property. Together, these elements provide a comprehensive understanding of the drone-based threat environment and the regulatory gaps that continue to shape U.S. critical infrastructure vulnerability.

Over time, the capabilities of drones used in attacks have evolved significantly. As drone capabilities continue to advance, law enforcement's counter-drone technologies

must evolve in parallel, creating an ongoing “cat-and-mouse” dynamic between emerging threats and defensive measures.

Improvised vs. Commercial Drones: Earlier terrorist drone attempts (such as the 2011 Ferdaus plot on Washington, DC or Hezbollah’s 2006 drone bombing attempt against Israel) relied on improvised or military-grade UAVs that were hard to obtain and fly. See Appendix I for an abridged history of drone attacks. By contrast, today’s attackers often repurpose readily available commercial drones, like DJI Phantoms, Mavics, or racing drones, which are GPS-stabilized, easy to fly, and inexpensive. These drones can be bought online for a few hundred to a few thousand dollars and modified to carry grenades or small bombs (Dulligan et al., 2025). The widespread availability of high-performance hobby drones since 2015 has truly enabled the “democratization” of airstrike capabilities. For example, ISIS’s favorite models included DJI Phantom quadcopters (for dropping 1-2 lb. munitions) and larger Skywalker X8 foam drones (a model airplane), which they turned into kamikaze bombs. Hezbollah and Houthis, on the other hand, received more sophisticated Iranian drones like the Qasef-1, a variant of Iran’s Ababil UAV that could travel long distances and hit targets with larger warheads (Crino & Dreby, 2020). As a result, terrorists now have access to a spectrum of drones, from small quadcopters for close-range harassment to larger fixed-wing drones for strategic strikes. This capability allows them to choose their tactics accordingly.

Drop, Crash, and Swarm Attack Methods: The main ways drones are used in attacks are: (1) bomb-drop drones, which release payloads from above; (2) suicide drones, which dive into the target and explode; and (3) coordinated swarm attacks involving multiple drones. ISIS excelled at bomb-dropping tactics by adding release mechanisms to hobby drones and dropping mortar shells or grenades onto troops. This method effectively turns a drone into a mini bomber. Conversely, Houthis and some ISIS innovations turned drones into one-way explosive “cruise missiles” that crash and detonate on impact. The 2019 Saudi oil attack and 2021 Iraq PM attack used such loitering munitions (Reuters, 2021). Swarm attacks are still rare but expected to grow. A swarm can be a mix of drop and crash tactics to overwhelm defenses (Read, 2018). Notably, the 2018 Russian base swarm and a 2021 Hamas attempt to launch multiple

drones simultaneously at Israel hint at swarm strategy. Terror groups have also toyed with simultaneous multi-drone strikes from different angles (as in the Maduro attempt with two drones). The swarming trend could escalate with autonomous drone coordination, which is a nightmare scenario for security agencies.

Range and Payload Improvements: Early off-the-shelf drones had short ranges (a few hundred meters) and tiny payload capacity, limiting their attack usefulness. However, newer drones can fly miles and carry heavier loads. Commercial drones like DJI's M600 (such as used in the Maduro attempt detailed in Appendix I) can lift 5-6 kg. Custom DIY drones can be built larger for even more range or payload. For instance, the drone built by Al-Bared in the UK was modeled after a Tomahawk cruise missile shape to maximize range; it could likely travel a few kilometers with a small chemical warhead (Loh, 2023). Houthi rebels have fielded long-range drones (possibly with Iranian assistance) that flew nearly 900 km to hit targets in Saudi Arabia (Crino & Dreby, 2020). As GPS navigation and autopilot technology have become ubiquitous, even semi-skilled militants can program drones to fly precise routes ("waypoint navigation") and hit targets from afar. The effect is that drones can be launched from a safe hideout and travel dozens of miles to a target, evading traditional security perimeters. Critical sites like ports, airports, power plants, and government buildings must now consider threats from above and outside their immediate vicinity.

Evasion and Stealth: Attackers have adapted techniques to make drones harder to detect or stop. They often remove drone LED lights and identifying markings, fly at low altitudes or among buildings to avoid radar, and use timed or pre-programmed flights that require no active radio control, thus preventing control signal jamming. Some have even used fixed-wire control (a spool of fine fiber-optic cable) to guide drones, defeating radio-frequency jammers. Drones are generally small and have a low radar cross-section, making them difficult to spot until it's too late. In the Pennsylvania substation attempt (Details in Appendix I), the drone was painted black and had its camera and memory card removed to hinder investigators (Winks et al., 2024). These methods show increasing sophistication in terrorist tradecraft, essentially using low-tech stealth to counter high-tech defenses.

A Persistent and Evolving Threat

Over the past two decades, the use of drones in attacks has evolved from a novelty to a core tactic for both state militaries and non-state terrorists. What began with U.S. Predators hunting Al-Qaeda has morphed into a worldwide phenomenon of DIY aerial weapons. Terrorist and insurgent groups have embraced drones because they are relatively cheap, accessible, and can confer a sort of air power to those who lack traditional aircraft. Drones have been used to assassinate, to spread fear, to disrupt economies, and to target critical infrastructure. Incidents near the U.S., from power grid plots to cartel drone bombs just across the border, underscore that the homeland is very much in the crosshairs of this trend. And while we have yet to see a full-fledged biological or chemical attack via drone, the documented plots and interest in such capabilities mean we cannot dismiss the possibility.

For the Department of Homeland Security and its partners, the rise of drone threats demands new defenses. Efforts are underway to deploy counter-UAS systems around sensitive sites, from jamming guns and net-launching interceptors to high-tech lasers. Intelligence and law enforcement are paying close attention to chatter about drones in terror plots.

In summary, drones have transformed the playbook of attacks and assassinations. They have been used in war zones to deadly effect and are increasingly employed by terrorists and criminals worldwide. We have seen landmark attacks from the Middle East to Latin America, and foiled attempts on U.S. soil that read like thriller novel plots. The common thread is the attackers' focus on *how* to carry out their mission with drones, exploiting the UAVs' remote reach, surprise angle of attack (from the sky), and technological features. Whether by dropping a grenade, slamming into a target as a flying bomb, or potentially spreading dangerous agents, drones offer malicious actors a versatile weapon. The threat has steadily grown, and it calls for equally creative countermeasures to protect people and critical infrastructure from the skies. The evolution of drone attacks is still unfolding, and staying ahead of it remains a pressing challenge for agencies in the U.S. and around the world. Appendix II reviews legal allowances and efforts by Western allies to combat malicious UAVs.

Drones continue to advance in sophistication while becoming increasingly affordable, expanding their accessibility to a wide range of users. The absence of a major drone-related incident in the United States should not be interpreted as evidence of low risk; rather, it underscores the urgency for proactive preparedness. Law enforcement agencies and critical infrastructure operators must assume that a serious event is plausible and develop the operational, technical, and policy capacities necessary to respond effectively. Moreover, not all harmful outcomes stem from malicious actors. Negligent or uninformed drone use can cause significant disruptions, including damage to power lines and other essential systems, resulting in costly operational setbacks. Man of these incidents are avoidable if the proper precautions are implanted.

Protecting Against Malicious Drones: Legal Frameworks in the U.S. and Abroad

U.S. Federal Law: Prohibitions and Limited Counter-Drone Authority

Under U.S. federal law, private individuals have very limited legal means to directly counteract a “bad guy” drone. The Federal Aviation Administration (FAA) classifies drones as aircraft, meaning that damaging or destroying a drone is a federal crime. For example, an official Oklahoma state memo in 2024 emphasized the following.

Federal law generally prohibits disabling or destroying any UAS because federal rules consider drones to be a form of aircraft. This prevents even state and local law enforcement from any activity that would interfere with the flight of a drone, including shooting it down (Office of Governor J. Kevin Stitt, 2024).

In fact, under 18 U.S.C. §32 it is a felony to shoot down or otherwise harm an aircraft, which includes unmanned aircraft. Similarly, federal communications laws prohibit signal jamming or hacking; using devices to interfere with a drone’s GPS or radio link is generally illegal for civilians. Even state or local law enforcement have been barred by federal preemption from disabling drones in most cases until recently. In short, a private person who tries to shoot, physically disable, or jam a suspicious drone risks serious criminal penalties, including up to 20 years in prison in some cases (Sea-Tac Noise Advisory Council, n.d.).

Traditionally, the federal government began carving out narrow exceptions for counter-drone defense, but these applied only to specific federal agencies, not to private individuals nor local law enforcement. In 2018, Congress passed the *Preventing Emerging Threats Act,* a separate legal act included as a part of the FAA Reauthorization Act of 2018. This law grants certain agencies, notably the Department of Homeland Security (DHS) and Department of Justice (DOJ), authority to detect, track, disrupt, seize, or even destroy drones that pose a “credible threat” to designated sensitive sites (AirSight, 2018). Under this authority, DHS and DOJ personnel (in

coordination with the DOT/FAA) can use techniques like radio jamming, intercepting control signals, or “kinetic” measures (e.g., shooting down) to neutralize a rogue drone. However, these powers were originally limited to protecting “covered facilities or assets” such as military bases, DHS facilities, National Special Security Events, prisons, major sporting events, etc., as defined by the statute. Private citizens and most local authorities are not covered by this law, meaning they *cannot* legally deploy counter-drone technologies on their own. Drone defense in the U.S. remains largely a federal monopoly. The imbalance has been noted in security forums; there are currently “significant gaps” in authority, where neither local police nor private owners can act against a malicious drone. This highlights the need for clearer laws (Deeks & Rinder, 2025). Only recently have federal agencies started officially deputizing local law enforcement as a measure to bridge this gap.

Case law so far reinforces these legal barriers. Perhaps the most famous incident is the 2015 “Drone Slayer” case in Kentucky, where a homeowner shot down a drone hovering over his yard. A local judge dismissed charges against the homeowner for discharging a firearm, accepting his argument that the drone was trespassing and invading privacy (witnesses said it flew low over his property) (National Agricultural Law Center, 2015). However, the drone’s owner produced video evidence that it was flying at about 200 feet altitude and pursued a federal lawsuit for damages. The federal court ultimately dismissed that lawsuit on procedural grounds in 2017, leaving the legal question unresolved. No clear precedent was set on whether landowners have a right to shoot drones over their property. In fact, the only definitive legal guidance dates back to a 1946 Supreme Court case (*United States v. Causby*), which recognized landowner airspace rights at least up to 83 feet but acknowledged navigable airspace above 500 feet is public domain. Drones operate in the hazy zone below 400 feet, and it remains a gray area as to how traditional property rights or self-defense doctrines apply to them. What is clear is that federal aviation law preempts private self-help: regardless of trespass, you cannot take the law into your own hands by destroying a drone. Indeed, when an angry homeowner or even a gun-toting felon has shot at drones, they have faced prosecution under federal law, often via related charges like firearms offenses, since shooting at a drone is itself illegal (Daily Commercial, 2023; Lancaster, 2024).

Bottom line: Under current U.S. federal law, a private individual's options for actively stopping a malicious drone are extremely limited. One must rely on authorized authorities to intervene or pursue the drone operator through legal channels after the fact. This sets the stage for examining what, if anything, state laws can provide to fill this gap.

U.S. State Laws: Privacy, Trespass, and Critical Infrastructure Protections

While states cannot override federal aircraft laws, many have enacted their own drone-related statutes to protect both privacy and critical infrastructure. These laws mainly do two things: restrict or punish malicious drone use (creating penalties for "bad guy" drone operators) and, in a few cases, empower certain responders (like police or first responders) to act defensively. It's important to note that no state law openly permits an average private citizen to shoot down or disable a drone; however, some states give limited immunity or authority to officials in special situations, and many create civil or criminal remedies against drone intrusions.

Privacy and Trespass Laws: California has been a pioneer in drone privacy legislation. In 2015 it expanded its civil invasion of privacy laws to cover drones: knowingly flying into someone's airspace to take photos or recordings of them on private property is now explicitly illegal and makes the operator liable for damages (Glaser, 2015). This law was originally aimed at paparazzi drones stalking celebrities, but it applies to anyone, giving private individuals a cause of action (and hefty statutory fines for the perpetrator) if a drone invades their private space.

The California law AB-856 states:

A person is liable for physical invasion of privacy when the person knowingly enters onto the land or into the airspace above the land of another person without permission or otherwise commits a trespass in order to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a private, personal, or

familial activity and the invasion occurs in a manner that is offensive to a reasonable person. (California Legislature, 2015)

Other states have similar “peeping Tom” laws adapted to drones. For example, in 2021 Oklahoma made it a misdemeanor to use a drone to surveil someone where they have an expectation of privacy or to trespass by hovering over private property without consent (Wirth Law Office, 2023). These laws don’t allow the offended person to knock the drone out of the sky, but they criminalize the drone pilot’s conduct and potentially allow one to sue the pilot for harassment or trespass. In practice, however, identifying and catching the operator is often the hardest part, which is why remote identification requirements (federal rules requiring drones broadcast an ID signal) are being implemented to help enforce such laws.

Critical Infrastructure No-Fly Zones: To protect farms, ranches, ports, power stations and other sensitive facilities, many states have enacted no-fly zone laws. As of mid-2025, at least 10 states prohibit drones from flying near or over certain critical facilities (typically with some altitude or distance buffer).

Currently, ten states have enacted specific laws that prohibit the flying of drones near or over critical facilities or infrastructure. These states include Arkansas, Arizona, Delaware, Florida, Louisiana, Nevada, Oklahoma, Oregon, Tennessee, and Texas. A few of these states specifically define critical infrastructures to include ports. Delaware, Oklahoma, Tennessee, and Texas specifically include “port” in their definition of a critical infrastructure (AirSight, n.d.). In those states, flying a drone over a shipping port or maritime facility without permission is a crime. For instance, Texas law makes it unlawful to intentionally hover within 400 feet of critical infrastructure facilities (ports, pipelines, chemical plants, etc.) and allows law enforcement to charge violators (National Conference of State Legislatures, 2023). New Jersey similarly lets operators of critical sites apply to the FAA for temporary flight restrictions and makes it an offense to endanger life or property with a drone or to surveil a critical facility without consent. These state laws essentially give teeth to “No Drone Zone” signs, providing grounds for police to arrest or fine a malicious drone operator who is snooping on (or endangering)

key infrastructure or private property. Each state defines “critical infrastructure” broadly. Oil refineries, power plants, rail yards, water treatment facilities, and agricultural feedlots have all been covered in various state laws (National Conference of State Legislatures, 2023).

Allowances for Defense by Authorities: A few states have gone a step further by authorizing certain officials to counter-attack drones in emergent situations (though seemingly bumping up against federal limits until recently). Utah was an early example: in 2016, facing drones that interfered with wildfire fighting, Utah passed an emergency law permitting the state highway patrol and National Guard to jam or even shoot down drones that violate wildfire no-fly zones (Grossman, 2016). The law targeted hobby drones that repeatedly grounded fire-fighting aircraft. It authorized signal jamming around wildfires and “good old-fashioned shooting” if necessary. Louisiana has recently pushed the envelope even further. In June 2025, Louisiana enacted the “We Will Act” law, the first state law granting *state and local law enforcement* explicit counter-UAS authority. Under this law, specially trained officers in Louisiana can intercept and disable drones (using both “kinetic and non-kinetic” methods) if the drone poses a credible threat to public safety near high-risk areas like schools, public events, or critical infrastructure. This effectively lets Louisiana police use anti-drone jamming guns or even shoot down a drone, a power previously reserved only for federal agencies. Drone operators violating this law face up to $5,000 fines, a year in jail, and forfeiture of their equipment. Important caveat: Such state laws tread into murky legal territory, because federal law still says only federal authorities can shoot down aircraft. Louisiana’s move is unprecedented, as it “marks the first time a state has granted its law enforcement agencies direct drone mitigation authority” (Office of Governor Jeff Landry, 2025). We can expect federal regulators or courts to scrutinize this. Louisiana’s law may have been a catalyst for new federal regulations and extended allowances for local law enforcement through federal deputization.

Another type of allowance is immunity for accidental drone damage. Recognizing that drones can impede emergency responders, California passed a law giving first responders immunity from liability if they damage a drone that is interfering with their

emergency operations, e.g., a firefighter's water stream that knocks out a nearby drone (National Conference of State Legislatures, 2023). This doesn't give firefighters a license to hunt drones, but it protects them if a drone gets in the way and is collateral damage.

Overall, state measures primarily focus on deterrence and punishment of rogue drone operators, rather than empowering private drone vigilantes. No state currently allows a private farmer or facility owner to personally shoot down a drone. Instead, a private citizen's legal tools are: call the police and have them enforce current drone trespass or no-fly laws or later sue the drone operator under privacy/trespass statutes if they can manage to identify them. States like Oklahoma have even considered laws to explicitly give property owners civil immunity if they shoot down a drone over their land (effectively legalizing drone shootdowns on one's own property), but those proposals (e.g., Oklahoma SB 660 in 2017) failed to pass (LegiScan, 2017). In fact, Oklahoma's governor in 2024 instead directed investment in drone detection systems, explicitly acknowledging that shooting or disabling drones is off-limits even for police under current federal rules.

The National Defense Authorization Act for Fiscal Year 2026 (FY26 NDAA) constitutes a structural inflection point in U.S. domestic counter-UAS governance because it begins to close a long-recognized mismatch between the operational reality of rapidly proliferating small UAS threats and the historically narrow set of entities legally empowered to detect and mitigate those threats. Prior to the FY26 NDAA's reforms, U.S. law concentrated most counter-UAS authority to select federal departments, notably DHS and DOJ, under statutory frameworks that emphasized narrowly defined "credible threats," controlled operational circumstances, and strict compliance safeguards (U.S. Department of Homeland Security, 2025). The FY26 NDAA establishes a more explicit federal pathway through which State, Local, Tribal, and Territorial (SLTT) law-enforcement and corrections agencies may, once certain federal prerequisites are satisfied, participate in counter-UAS operations at sensitive sites and events while preserving federal primacy through interagency oversight, approved technologies, and mandated accountability.

Substantive counter-UAS shift: “empowerment” bounded by federal control

The FY26 NDAA’s domestic counter-UAS provisions (as identified as the SAFER SKIES Act embedded in the larger Act) expand the practical perimeter of public-safety defense against malicious or reckless drones, but do so through a federal delegation model rather than a broad decentralization of powers. Emphasis was placed on coordination, standardization, and a compliance architecture intended to prevent unsafe interference with the National Airspace System and to reduce civil-liberties risk (McNabb, 2025). In effect, the legislation recognizes that frontline public-safety entities are frequently the first and only actors with realistic response time during a fast-moving UAS incident, especially near crowded venues or sensitive infrastructure. However, the Act still conditions any operational empowerment on centralized standards, approved tools, and reporting obligations.

Implementation: How real operational capability rolls out progressively in 2026

The FY26 NDAA’s SLTT counter-UAS framework is implementation-dependent. The authorizing language written in the bill does not generate immediate field capabilities. To be effective, the statute requires follow-on DOJ and DHS regulations, interagency coordination (including an aviation-safety interface with DOT/FAA), establishment of training/certification, and operational constraints on what technologies and tactics are permissible (U.S. Congress, 2025). The Act essentially just creates a legal and administrative pathway from federal authority to qualified SLTT execution, rather than an immediate nationwide operational switch in who can do what. In practical terms, “time to capability” is driven by the speed of regulatory rulemaking, procurement lead times for detection and mitigation systems that comply with the specs, ability to set up credentialing methodology, and the development of local concepts of operations (CONOPS) compatible with federal constraints and the FAA’s airspace-safety imperatives.

As it stands, U.S. state laws can help protect private citizens on paper by making the drone's actions illegal, which can lead to the drone pilot's arrest or provide grounds to sue for invasion of privacy. States can also set up geofences and no-drone zones (e.g., around ports, utilities, and farms) that add layers of legal protection for critical infrastructure. But they do not generally empower private individuals, including critical infrastructure managers, to take immediate offensive action against a drone. The burden is always on law enforcement (local or federal) to actually counter the drone. This limitation leads to the practical question: *what can be done in the heat of the moment* when a malicious drone is overhead?

Drone Defense for Texas Ports

Current Drone Threat Environment in Maritime Ports

Unmanned aircraft systems (UAS), have rapidly become a security concern for U.S. maritime ports. Port facilities in Texas, such as Port Houston, Port of Corpus Christi, and Port of Brownsville, are seeing a surge in unauthorized drone activity. A recent homeland security assessment found that security breaches involving drones around ports and other critical infrastructure "are becoming a common occurrence" (Johnson, 2023). Area Maritime Security Committees (AMSCs) across the country report frequent unauthorized UAS flights over restricted port facilities, raising concerns about espionage, smuggling, and potential attacks on the Marine Transportation System. In Texas, port authorities and law enforcement have observed drones hovering over petrochemical complexes, ship channels, and even near strategic assets like oil reserves and refineries, illustrating the breadth of the drone threat. For example, in late 2024 dozens of mysterious drones were spotted flying for hours at night around the Galveston Bay area, near Port Houston, the Bolivar Peninsula, and critical energy infrastructure, prompting an FBI and DHS investigation. While federal officials stated that they could not tie the sightings to foreign or terrorist groups, the incident highlighted how unidentified drones can spark alarm in port communities (Garcia, 2024).

At Texas ports, small commercially available drones are viewed as the most pressing current threat. In a 2023 study at the Port of Brownsville (near the Texas-Mexico border), stakeholders rated small aerial drones as a “High” *threat* (7.0 on a 10-point scale), higher than uncrewed ground vehicles or waterborne drones. Over a 13-month monitoring period, at least 7,948 drone flights were detected in the airspace around Brownsville’s harbor (Sullivan, 2023), all of them small commercial-off-the-shelf drones and typically manufactured by DJI. This reflects a significant baseline of drone activity near port terminals. Many of these incursions may be hobbyists or legitimate operators, but the sheer volume creates a daunting security challenge. Port personnel worry about drones being used for surveillance of port operations, smuggling contraband, or even as weapons (e.g., carrying explosives). These fears are not unfounded; drug cartels have already weaponized aerial drones in Mexico and used them to smuggle narcotics across the border, and overseas conflict zones have seen explosive-laden drones attack oil tankers and port facilities. In Texas, a drone was flown illicitly over Port Houston in 2019 to photograph cargo infrastructure, revealing how easily even a small drone can access sensitive areas (Port Houston, 2019). In that case, the drone literally fell from the sky trailing smoke, prompting port police and firefighters to rush in, but not before it spent 30 minutes over the docks snapping photos of vessels, pipelines, and buildings. Such incidents highlight a growing reconnaissance threat from curious or malicious operators.

U.S. Coast Guard officials have warned that the drone threat is evolving faster than current defenses. In its 2022 annual report, the Coast Guard noted that existing federal counter-UAS laws have been “largely ineffective” at the local port level (Johnson, 2023), leaving authorities without the tools or legal authority to interdict suspicious drones. All levels of law enforcement, from port police up to state and federal agencies, *“lack the authority, policies, and equipment to identify and safely interdict unauthorized UASs”* under today’s framework. In other words, drones are appearing over ports with increasing frequency, but port security has limited or no legal or tangible means to stop them. This gap in both capabilities and policy sets the stage for urgent improvements in port drone defenses. Since the legal structures are being put into place, port authorities must now update their UAS defenses and policies in accordance with newly instituted

legal authority, to include budgeting for and purchasing approved counter-UAS hardware and training.

Defense Strategies and Technologies for Port Drone Threats

To protect harbors and waterfront facilities from rogue drones, U.S. ports are adopting a range of practical defense strategies. These defenses generally fall into three layers: early detection systems, active counter-drone measures, and comprehensive protocols and training to respond to drone incidents. A layered approach is critical since no single gadget or rule will solve the drone problem. Therefore, ports are building “defense-in-depth” against UAS intrusions.

Drone Detection Systems and Situational Awareness

Detecting a drone as early as possible is the first step in any port’s defensive plan. A variety of sensor technologies are being deployed to achieve 360-degree drone awareness around ports:

- **Radar:** Specialized micro-radars can pick up the small radar cross-section of a drone and track it in flight. Radars are effective for all-weather, day/night detection and can cover broad airspace. Ports must account for clutter (waves, birds) and need FCC licensing to operate surveillance radars. When tuned properly, radar can provide range and elevation of a drone target.
- **RF (Radio-Frequency) Sensors:** Many drones communicate via radio link (control signals or video feed). RF sensor systems passively scan the spectrum for these signals, allowing detection and even identification of drone make/model or pilot location. RF detection is powerful but raises legal considerations. Monitoring drone frequencies can potentially run afoul of FCC regulations or federal wiretap laws if not carefully managed. Still, with proper use, RF sensing can pinpoint a drone and its operator’s controller by triangulating signal sources.
- **Electro-Optical/Infrared (EO/IR) Cameras:** High-zoom daylight cameras and thermal infrared cameras can visually confirm a drone once cued by radar or RF. Optical systems provide important visual identification (e.g., is the drone carrying a payload, what type is it), and can track drones in real time. They are generally

limited to line-of-sight but are invaluable for evidentiary footage and situational awareness, especially at night using IR.

- **Acoustic Sensors:** Arrays of microphones can detect the distinctive buzzing sound of drone rotors. Acoustic detection is shorter-range and can be fooled by background noise, but it adds another layer to catch drones that might slip past radar and RF (e.g., non-communicating or pre-programmed, autonomous drones). Acoustic systems are generally allowed for port use, since listening for motor noises doesn't violate communications laws.

Modern port drone defenses tend to use a fusion of these sensors. No single sensor is foolproof, for example, radar might pick up a drone but can't tell if it's friend or foe; RF sensors might miss drones not using common frequencies. By combining radar, RF, EO/IR, etc., security teams get a more reliable and comprehensive "air picture." Multi-sensor systems were highlighted in new federal guidance as the recommended approach, tailored to each port's environment (Inside Unmanned Systems, 2025). For instance, a port surrounded by tall structures and radio interference, such as Port Houston's busy ship channel and petrochemical corridor, might lean more on radar and optical tracking, whereas a more open port might utilize longer-range RF scanning. The Cybersecurity and Infrastructure Security Agency (CISA) in November 2025 released its official Unmanned Aircraft System Detection Technology Guidance for Critical Infrastructure (Cybersecurity and Infrastructure Security Agency 2025b), which walks operators through assessing their site's risk profile and selecting appropriate detection technologies (radar, RF, EO/IR, acoustic) based on terrain, RF clutter, and mission need. Importantly, CISA urges port operators to integrate drone detection feeds into their existing Security Operations Centers and incident workflows, rather than watching a separate "drone screen" in a silo. In practice, this means that if a drone is detected, an alert would pop up in the port's central alarm system or video management console, ensuring rapid awareness by security personnel.

Real-world examples

The Port of Galveston in Texas was an early adopter of drone detection. In 2017 it launched a pilot project with the private technology partner TelaForce to deploy a drone

detection system that could *“accurately detect, identify, track and protect against unauthorized drones”* in the vicinity of the port (Port of Galveston, 2017). That system not only tracked drones in protected airspace, but uniquely could locate the ground controller’s position, enabling law enforcement to respond to the pilot. The Port of Brownsville’s 2022-2023 drone risk study similarly used a network of sensors (provided by Aerial Armor, a Dedrone company) to log nearly eight thousand drone flights around the port. These tools gave Brownsville authorities a detailed picture of hotspots and flight patterns, data that is now guiding security investments. Many ports are now exploring detection-as-a-service solutions or portable kits that can be set up during special operations.

Indeed, Texas has seen innovation from its public safety agencies. The Texas Department of Public Safety (DPS) has tested an *Airborne Counter-UAS System (ACUS)* mounted on helicopters to detect and track drones from the air. This system uses advanced RF sensing and geolocation to alert DPS officers of any drone threats in real time (Shaw, 2025). Such capabilities could be leveraged to support port security during large events or high threat periods. Overall, establishing a robust “drone radar” around ports is now considered essential, so that any intruding UAS can be detected as early as possible and continuously monitored.

As a real-time example, the Port of Brownsville has a tenant that specializes in breaking older ships that have outlived their usefulness. It has recently concluded a successful dismantling of the aircraft carrier USS Kitty Hawk (CV-63). During that time, a particular drone operator made regular fly-bys recording the progress of the breakdown, posting the videos on YouTube. On February 2, 2025 the USS John F. Kennedy (CV-67) arrived for its end-of-life dismantling. It is unique in that, while not a nuclear-powered ship, it was originally designed for nuclear propulsion. Its internal workings, which will be exposed to the air during the dismantling process, are considered sensitive. The Port of Brownsville, ISL (the breaker company), and the US Navy are all concerned with the potential for unauthorized drone flights and photography.

Counter-Drone Measures (Jamming, Interception, and Mitigation)

Once a rogue drone is detected encroaching on a port, the next question is how to neutralize or redirect it. A variety of counter-UAS technologies exist, from radio jamming guns to interceptor drones, but as discussed in the legal section, their practical use at U.S. ports is heavily constrained by law. Nevertheless, it is important for port authorities to understand the tools available (and who can use them) as they develop response plans:

- **Radio-Frequency Jamming and Protocol Exploitation:** Many counter-UAS systems work by severing the link between a drone and its operator or GPS. Jammers transmit strong signals on the control frequencies or satellite bands, causing the drone to lose connection. This can trigger the drone's fail-safe (typically to either hover, land immediately, or return to its takeoff point). More advanced systems use protocol exploitation to send *"spoof"* commands, effectively hijacking control of the drone and forcing it to land in a safe area. Jamming/spoofing can be effective against most off-the-shelf drones, but it carries risks of interference with other communications and is strictly regulated (generally prohibited for civilian use). Under current U.S. law, port police or security staff are *not* authorized to deploy RF jammers on their own without federal training and oversight. Only certain federal agencies (e.g., DHS or DOJ teams with special authority) can legally employ these tools. Thus, while jamming tech exists, such as handheld "drone guns" used by the military and some federal law enforcement, a port would need federal support to utilize them in an incident. The FCC has strict regulations on who can transmit on certain parts of the frequency spectrum, and even how information derived from passively listening in on the spectrum can be used.
- **Kinetic Interceptors:** These are physical methods to directly disable or destroy a drone. They range from anti-drone projectiles and shotguns to sophisticated interceptor drones that launch nets. For example, some security companies field net guns (Wagstaff, 2015) or net-carrying drones (Groupe assmann, 2015) that can entangle a rogue drone's propellers, causing it to fall. There are also

emerging high-tech solutions like laser weapons (Tom's Hardware, 2025) or high-power microwave devices that can shoot down drones at short range. However, deploying any kinetic force in a busy port environment is risky, as projectiles or debris could injure people or damage assets. More importantly, destroying a drone in flight is considered "aircraft destruction" under U.S. law, which is illegal for anyone except a few federal agencies, although the Trump administration has recently given more leeway to defensive operators. As recently as late 2025, state and local authorities (and private critical infrastructure operators) did not have clear legal permission to shoot down or disable drones, even if they are trespassing or acting in a threatening manner. Because of this, ports had to rely on federal counter-UAS teams for any active drone takedown. One example occurred in 2022 at a petrochemical facility in Louisiana. After dozens of suspicious night-time drone incursions, the Coast Guard's Maritime Security Response Team (MSRT), a specialized federal unit, was deployed with counter-UAS capabilities to assist Louisiana State Police in countering the threat (Johnson, 2023). It was the first time the Coast Guard's drone mitigation assets were used in an urgent port scenario, operating over the course of 84 hours and providing lessons for future incidents. In Texas, a similar federal response could be called in if, say, a swarm of drones was endangering the Houston Ship Channel. It is crucial that port security operators know what can be done in the new legal environment and what cannot, and also have relationships in place with federal authorities prior to their necessity.

- **Drone "Kill Zones" and Geofencing:** Some ports are exploring passive measures like geofencing and exclusion zones. The idea is to prevent drones from entering sensitive areas in the first place. Geofencing is a software limitation in many commercial drones that prevents them from flying in designated restricted zones (such as near airports or critical sites listed in firmware). Ports can coordinate with the FAA to establish Temporary Flight Restrictions (TFRs) during special events or request to be added to drone manufacturers' no-fly databases. However, geofences are not foolproof; they can be overridden by savvy operators or simply not honored by custom-built drones. Therefore,

geofencing is seen as a supplementary measure. It may deter casual hobbyists (who get a warning on their app), but determined intruders won't be stopped by software. Physical barriers like port perimeter fencing and netting can help against ground or waterborne drones, but they do little against aerial intrusions beyond keeping trespassers out of restricted ground areas.

Given the constraints on kinetic or electronic engagement, most U.S. ports emphasize robust detection and tracking, to monitor a rogue drone until it leaves or until law enforcement can intervene at the ground control station. In an extreme emergency (e.g., a drone clearly threatening a loaded LNG tanker), port authorities would likely call in specialized federal teams immediately. The reality is that, for now, ports cannot independently deploy "hard-kill" countermeasures. This is a point of active discussion and legislative effort, as previously described.

Port Security Protocols and Response Plans for Drone Incidents

Technology alone is not enough; operational protocols and training are crucial for transforming drone detections into effective defense. Texas ports are working on integrating drone scenarios into their emergency response plans and security procedures. Key elements of these protocols include:

- **Defined Response Levels:** Ports are adopting a tiered response model for drone sightings. Not every drone is hostile, so security teams establish criteria for what is merely *"benign"* (e.g., a news photographer with permission) versus *"suspicious"* (unknown drone loitering near a pipeline) versus *"critical threat"* (drone appears weaponized or on a collision course). CISA's recent *Suspicious UAS Activity Guidance* recommends exactly this approach, normalizing expected drone activity and flagging the truly unusual behaviors (Inside Unmanned Systems, 2025). For example, a port might classify a drone hovering high over a parking lot in daylight as low concern (log it, but just observe), whereas multiple

drones swarming near a dock at night with no lights would trigger high alert and law enforcement notification. By defining these thresholds in advance, ports aim to avoid both under-reacting and over-reacting to drones. A clear decision tree must be established: at what point do we call the Coast Guard or FBI? When do we halt vessel movements or close a terminal as a precaution? These decisions are now being incorporated into port security plans and playbooks.

- **Rapid Interagency Notification:** As soon as a threatening drone is identified, communication is critical. Most major Texas ports have their own police or security force on-site (for instance, Port of Brownsville has a Port Police department and on-site U.S. Coast Guard detachment). Standard Operating Procedures (SOPs) typically instruct port security to immediately notify the Coast Guard Captain of the Port and local law enforcement when a drone incident occurs. The Coast Guard, as the lead federal agency for port security, can help coordinate airspace control measures or request specialized counter-UAS units. In the 2022 Louisiana incident mentioned, the Coast Guard, state police, state homeland security office, and industry partners all coordinated within two weeks to deploy a counter-drone operation. Texas ports likewise work through their AMSCs to build tight communication links with DHS, FBI, FAA air traffic control, and others. Some ports have MOUs allowing direct radio contact between port security and nearby police aviation units or military bases if a drone incursion overlaps their jurisdictions. Since drones typically move fast and have limited time on station, time is of the essence in the response. As a result, these relationships and protocols must be developed and rehearsed in advance.
- **Training and Drills:** Incorporating drone threat scenarios into training exercises is an emerging priority. The U.S. Coast Guard has urged ports to include UAS incidents in their regular security drills and Area Maritime Security Training exercises (Johnson, 2023). Several ports have already done so. For example, the Port of Hueneme, the only deep-water port between Los Angeles and the San Francisco Bay area in California, recently hosted a multi-agency exercise focusing on a hostile drone targeting a harbor facility (PortStrategy, 2025). In Texas, port security officials participate in the statewide Texas Fusion Center

network and Infrastructure Liaison Officer (ILO) programs to share drone threat intelligence and best practices. These information-sharing efforts help ports learn from each other's experiences (e.g., if Port X had a drone repeatedly mapping their facility, how did they respond?). Tabletop exercises have been conducted where port managers must decide how to respond to a hypothetical drone dropping a suspicious package on a wharf, who secures the device, how to safeguard personnel, and what notifications go out. Such drills reveal gaps and build confidence in a coordinated response.

- **Public Awareness and Reporting:** Many ports are also engaging the surrounding community and port workers to be part of the solution. Port Houston, for instance, has outreach reminding drone hobbyists that the harbor area is a "No Drone Zone" without prior authorization (Port Houston, 2019). Signs and website FAQs (such as Port Freeport's) warn that flying a drone over port property is illegal and violators can face arrest, charges, and confiscation of drones (Port Freeport, n.d.). Including links to the appropriate chapter in the Texas Government Code, e.g., Title 4, Subtitle B, Chapter 423 Use of Unmanned Aircraft (Texas Government Code, n.d.) may aid in getting recreational drone pilots to become aware of the legal implications of unauthorized drone flights. Meanwhile, ports encourage workers, mariners, and residents to report any drone sightings near restricted areas. A quick phone report could cue security to a potential intrusion that their sensors didn't catch. By increasing awareness that drones pose a serious security risk around ports and are not just toys or photography tools, authorities hope to deter casual misuse and gain early warning of suspicious activity. Additionally, establishing designated Drone Fly Areas will encourage sanctioned drone usage near ports and discourage hobbyists from operating in restricted areas.

Finally, an often overlooked but crucial part of the protocol is what to do *after* a drone is neutralized or crashes on port property. CISA's 2025 guidance includes a *Safe Handling of Downed Drones* component, emphasizing that any unknown drone should be treated as a potential bomb or data device (Cybersecurity and Infrastructure Security Agency 2025a). Port police and fire departments are being trained on bomb-squad procedures

for securing a downed drone: keep people at a distance, use protective equipment, and preserve the drone and any payload for evidence. The guidance stresses documenting the scene and maintaining chain-of-custody, since the recovered drone (and its onboard camera or memory card) could be invaluable for criminal investigation or intelligence analysis. For example, once a drone is recovered the FBI could analyze its flight path and data to find the operator or assess whether it was conducting hostile reconnaissance. Port authorities are therefore integrating drone recovery into their incident response plans, often in partnership with local bomb squads or federal agents. By moving from an ad-hoc “just grab the drone” approach to a structured protocol outlined in an SOP, ports can better protect themselves from hidden hazards and help build a legal case against the perpetrators.

Case Studies: Texas Ports Implementing Drone Defense

Several Texas ports have taken notable steps to address drone threats, providing case studies and lessons learned for the broader maritime community:

1. **Port Houston (Harris County, TX):** The busiest port in the U.S. Gulf, Port Houston has encountered unauthorized drones and responded proactively. In one 2019 incident, a drone overflew the Turning Basin terminal and crashed on site, leading to an immediate mobilization of port security forces (Port Houston, 2019). Within minutes, Port Houston Police and firefighters were on scene, and an investigation revealed a freelance photographer had been operating the drone to take pictures of ships and infrastructure. The case was turned over for potential prosecution. Under Texas law, the operator faced a Class B misdemeanor for flying over a critical infrastructure facility without permission. This incident prompted Port Houston to tighten its drone policies. The port now requires any drone operator to obtain prior authorization and abide by all FAA rules. At the time, FAA regulations required all drones flying within five miles of a towered airport to contact air traffic control prior to the flight (that requirement has since been eliminated with the advent of the FAA’s LAANC system). Port

Houston's website and publications regularly remind the public of the ban on unapproved drones near the ship channel. On the technological side, while specific systems have not been identified to the public, Port Houston has been working with industry partners on enhancing surveillance. They emphasize a multi-layered security posture ("*eyes in the sky*" are as important as boots on the ground) and coordinate closely with the U.S. Coast Guard Sector Houston-Galveston on airspace monitoring. Port Houston's security chief has also indicated that they are integrating cyber defense with physical drone defense, recognizing that some drone incursions could be precursors to or combined with cyber-attacks on port IT systems (PortStrategy, 2025). The port's inclusion of drone scenarios in emergency drills, and its active engagement in the local AMSC, have made it a leading example of a big port grappling with the drone age.

2. **Port of Brownsville (Cameron County, TX):** The Port of Brownsville conducted a comprehensive drone threat assessment in 2023 with researchers from Sam Houston State University (Sullivan, 2023). This case is notable because Brownsville is the only U.S. deepwater port directly on the Mexican border, making it a potential hotspot for cartel-related drone activity. The assessment confirmed significant drone traffic near the port (nearly 8k flights in a year) and identified particular concerns such as drones spying on oil storage sites or being used to drop contraband onto ships. In response, the Port of Brownsville is now implementing recommendations from the study. These include acquiring dedicated drone detection gear, improving training for Port Police in UAS response, and establishing formal standard operating procedures for when a drone is spotted. Brownsville has also been exploring information-sharing agreements so that when they detect drones, that intel can feed into state and federal systems (e.g., notifying the Texas Fusion Center). An interesting aspect of Brownsville's approach is the attention to maritime (waterborne) drones as well. They rated uncrewed surface and underwater vehicles a moderate emerging threat. This port is expanding its security focus beyond just the air domain, recognizing that a coordinated multi-domain drone attack (air and water) could be

a future tactic. Brownsville's efforts serve as a model for smaller ports that still have high-value assets and international exposure.

3. **Port of Galveston (Galveston County, TX):** A major cruise and cargo port, Galveston was one of the first in Texas to publicly pilot a drone detection system project. In 2017, partnering with the private company TelaForce, the Port of Galveston tested an integrated platform that could continuously monitor the airspace for UAS and locate both the drones and their operators. The pilot project demonstrated the ability to track drone incursions in real time, day or night and in all weather, and provided valuable data on what kind of drone activity was happening around the port's perimeter. While details of the long-term deployment are limited, Galveston's interim port director at the time stated that he welcomed advancing the industry's ability to *"mitigate port security threats"* (Port of Galveston, 2017) from drones. This early initiative has been built upon by other ports in the region. Galveston, like other ports, enforces the state ban on unauthorized drones over its facilities and coordinates closely with the Coast Guard's local units. During large events (Galveston hosts major cruise departures and special events), the port increases vigilance for drones, sometimes deploying additional spotters or temporary detection gear. The Galveston case underscores the value of public-private collaboration in trialing new security tech. The 2017 pilot project no doubt has informed other ports (and DHS) on how to deploy drone detection in a maritime setting.
4. **Port of Corpus Christi (Nueces / San Patricio Counties, TX):** The Port of Corpus Christi is one of the nation's largest energy ports, and though specific public information on its drone defense measures is scarce (likely due to security sensitivities), it has signaled a strong posture against drone threats. The port has its own state-certified police department, which in 2020 submitted UAS-related use-of-force policies to Texas authorities, indicating they are training officers on how to handle drones. Port of Corpus Christi is known to engage in innovation partnerships, e.g., working with Texas A&M University-Corpus Christi on drone traffic management research (Texas A&M University-Corpus Christi, 2019). While that research is about enabling drones, it also gives the port exposure to cutting-

edge UAS detection and communication systems that could be repurposed for security. Like other Texas ports, Corpus Christi prohibits drone overflights of its property without advance permission. The port is adjacent to critical oil refineries and military installations, so there is a collaborative security environment. Although no major drone incursions at Corpus Christi have been publicly reported, the port likely took note when in December 2024 the flurry of drones on the Gulf Coast were spotted not far up the coast near Houston (Garcia, 2024). One can reasonably assume Port Corpus Christi increased its surveillance and perhaps tapped state or federal resources to ensure those mysterious drones did not encroach on Corpus facilities. This port also stands to benefit from new federal initiatives like the FEMA counter-UAS grant program, which is also available for other critical infrastructure operators in Texas to apply for funding for drone detection systems. In summary, Port Corpus Christi's case shows a port with significant energy infrastructure taking a cautious but proactive stance: establishing internal policies and keeping engaged with broader UAS security efforts, even if it hasn't had a known drone incident to date.

Actionable rollout steps for Texas port authorities (implementable now)

Texas ports should treat FY26 NDAA rollout as a program build, not a technology purchase. The near-term objective is to be "certification-ready" when DOJ/DHS implementation guidance and training pipelines mature. What follows is a process-oriented timeline to build procedures and capacity over a relatively short period of time.

1. **Stand up a port-wide Counter-UAS Governance Cell (30–45 days).** Assign an accountable executive owner (Port Security Director or equivalent) and create a joint working group with the port police, local sheriff/PD partners, and the Captain of the Port liaison. The output is a single CONOPS and decision matrix (who can do what, under what authorities, with what reporting).
2. **Conduct a UAS threat/risk assessment aligned to federal guidance (45–60 days).**

Use CISA's UAS resources to structure risk categories (suspicious activity reporting, detection considerations, and layered mitigations) and document the port's specific "crown jewels" e.g., LNG, petrochemical interfaces, container gates, cruise terminals, control rooms, radar and communications nodes (Casapulla, 2025).

3. **Design a detection-first architecture, with mitigation as a governed escalation (60–120 days).**
   Because mitigation is the most legally and operationally sensitive element, build the program around persistent detection, classification, and incident triage, then define escalation pathways to federally authorized partners until SLTT authorities are formally enabled via DOJ/DHS processes. (This sequencing also reduces safety risk to the National Airspace System.)
4. **Pre-negotiate coordination and evidence protocols (60–90 days).**
   Draft MOUs/SOPs for: incident notification, chain of custody for UAS-related evidence, data retention and privacy controls, and FAA interface during incidents. The goal is to avoid ad hoc decisions during a live event.
5. **Build a training pipeline and credential readiness plan (start immediately; iterate quarterly).**
   Create an inventory of which roles require what level of training (watchstanders, supervisors, tactical responders, investigators). When DOJ/DHS publish the required certification framework, ports that have already mapped roles and competencies will onboard faster.
6. **Embed UAS incidents into port exercises and MTSA-style drill rhythms (next 1–2 exercise cycles).**
   Run tabletop exercises for (a) unknown UAS over restricted waterside areas, (b) drone over a cruise embarkation crowd, (c) drone reconnaissance near gate/rail intermodal, and (d) multi-site distraction events. Capture metrics: time-to-detect, time-to-classify, time-to-notify, and time-to-establish unified command.
7. **Procurement discipline: require "compliance-by-design."**
   Even before mitigation authority is available, write procurement requirements that anticipate federal constraints: audit logs, exportable reporting, safety interlocks,

operator access controls, and documentation that supports DOJ/DHS/FAA governance expectations. CISA's detection-technology guidance is a useful baseline for defining selection criteria and documentation.

Conclusion and Directions for Future Research

This paper demonstrates that unmanned aerial systems have fundamentally altered the threat environment for U.S. critical infrastructure, and that maritime ports, especially in Texas, represent one of the most exposed and consequential sectors. The convergence of low-cost commercial access, increasing autonomy, and demonstrated malicious use by state and non-state actors has produced an "airborne" security problem that traditional perimeter-based and jurisdictionally fragmented frameworks were not designed to manage.

Across the threat evolution, legal analysis, and Texas port case evidence, the central finding is that the dominant constraint on effective counter-UAS defense has not been a lack of technology, but a mismatch between threat velocity and governance capacity. Historically, counter-UAS authority has been concentrated almost exclusively at the federal level, creating a persistent operational gap between the entities most likely to detect and manage an incursion and those legally empowered to mitigate it. While state laws have strengthened penalties and no-fly protections around critical infrastructure, they have generally stopped short of authorizing real-time interdiction.

The FY26 National Defense Authorization Act signals a pivotal shift by establishing a federally governed pathway for state, local, tribal, and territorial participation in counter-UAS operations. That shift, however, should be understood as conditional delegation rather than decentralization: federal primacy is preserved through training, certification, approved technologies, and reporting requirements, and operational capability will hinge on implementation pace and institutional uptake.

Accordingly, the practical implication is that effective port defense will depend less on any single statutory provision or technology stack than on institutional readiness. Ports that stand up clear governance, adopt detection-first architectures, formalize interagency coordination and evidence protocols, and build training and exercise pipelines will be best positioned to operationalize expanding authorities as they mature. Conversely, ports that treat counter-UAS as an ad hoc or purely technological problem risk remaining reactive, legally constrained, and operationally exposed even under expanded statutory allowances.

Several research gaps merit priority attention. First, empirical study is needed on FY26 implementation outcomes: timelines, certification models, oversight mechanisms, and where bottlenecks emerge across DOJ/DHS rulemaking and FAA operational interfaces.

Second, the literature requires defensible standards for training, credentialing, and escalation governance appropriate for delegated counter-UAS roles in complex civilian environments, including accountability models and civil-liberties safeguards.

Third, more maritime-specific testing is needed to validate detection and sensor-fusion performance under port conditions such as RF congestion, reflective surfaces, dense infrastructure, and mixed civilian–industrial clutter.

Finally, future work should evaluate coordinated multi-domain disruption risks involving aerial, surface, and cyber components within the Marine Transportation System.

In sum, the absence of a catastrophic drone incident at U.S. ports should be treated as an opportunity, not reassurance. The legal landscape is beginning to align with operational reality, but law alone does not confer resilience. The preparedness window is finite. Texas ports can lead nationally by building lawful, interoperable readiness now: governance first, detection and reporting as the backbone, and mitigation as a tightly controlled escalation as authority and competency standards come online so that future UAS events are contained as incidents rather than escalated into crises.

References

AirSight. (2018, October 9). *FAA Reauthorization Bill of 2018: UAS integration and countering drone threats*. https://www.airsight.com/en/news/faa-reauthorization-bill-of-2018-uas-integration-and-countering-drone-threats/

AirSight. (n.d.). *UAS risk assessment: Drone threats to ports of entry*. https://www.airsight.com/uas-risk-assessment-drone-threats-to-ports-of-entry-faa/

California Legislature. (2015). *Assembly Bill No. 856: Invasion of privacy* (Chapter 521, 2015-2016 Reg. Sess.). California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB856

Casapulla, S. (2025, November 19). CISA urges critical infrastructure to be air aware. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/news/cisa-urges-critical-infrastructure-be-air-aware

Cybersecurity and Infrastructure Security Agency. (2026). *Suspicious UAS activity guidance (508c V2)* [PDF]. https://www.cisa.gov/sites/default/files/2026-01/Suspicious_UAS_Activity_Guidance_508cV2.pdf

Cybersecurity and Infrastructure Security Agency. (2025a, November 19). *Safe handling considerations for downed unmanned aircraft systems*. https://www.cisa.gov/resources-tools/resources/safe-handling-considerations-downed-unmanned-aircraft-systems

Cybersecurity and Infrastructure Security Agency. (2025b, November 19). *Unmanned aircraft system detection technology guidance*. https://www.cisa.gov/resources-tools/resources/unmanned-aircraft-system-detection-technology-guidance

Crino, S., & Dreby, A. (2020, May). *Drone attacks against critical infrastructure: A real and present threat*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2020/05/DRONE-ATTACK-0420-WEB.pdf

Daily Commercial. (2023, October 10). *10-year prison sentence possible for shooting down sheriff's drone*.

https://www.dailycommercial.com/story/news/courts/2023/10/10/10-year-prison-sentence-possible-for-shooting-down-sheriffs-drone/71128325007/

Deeks, A. S., & Rinder, M. (2025, February 5). *Are domestic drone shoot-downs lawful?* Lawfare. https://www.lawfaremedia.org/article/are-domestic-drone-shoot-downs-lawful/

Dulligan, J., Freeman, L., Phoenix, A., & Davis, B. (2025, March 28). *The rising threat of non-state actor commercial drone use: Emerging capabilities and threats*. CTC Sentinel. https://ctc.westpoint.edu/the-rising-threat-of-non-state-actor-commercial-drone-use-emerging-capabilities-and-threats/

Garcia, A. (2024, December 13). *Texas Gulf Coast residents now spotting mysterious drones too*. Houston Chronicle. https://www.chron.com/news/houston-texas/article/drones-texas-new-jersey-19978116.php

Glaser, A. (2015, October 7). *CA governor approves limits on paparazzi drones*. DroneLife. https://dronelife.com/2015/10/07/ca-gov-approves-limits-on-paparazzi-drones/

Grossman, D. (2016, July 14). *Utah allows authorities to disable drones that are too close to wildfires*. Popular Mechanics. https://www.popularmechanics.com/technology/gadgets/a21845/utah-to-become-first-state-to-allow-jamming-drones-at-wildfires/

Groupe assmann. (2015, January 21). *drone antidrone intercepteur surveillance* [Video]. YouTube. https://www.youtube.com/watch?v=rMFBUZ8iLTw

Inside Unmanned Systems. (2025, November 20). *CISA rolls out new UAS security guides for critical infrastructure operators*. https://insideunmannedsystems.com/cisa-rolls-out-new-uas-security-guides-for-critical-infrastructure-operators/

Johnson, B. (2023, October 5). *Maritime infrastructure security breaches from drones 'becoming a common occurrence,' says report on port defense*. Homeland Security Today. https://www.hstoday.us/featured/maritime-infrastructure-security-breaches-from-drones-becoming-a-common-occurrence-says-report-on-port-defense/

Lancaster, J. (2024, March 1). *Florida man sentenced to 4 years in federal prison after shooting down a drone*. Reason. https://reason.com/2024/03/01/florida-man-sentenced-to-4-years-in-federal-prison-after-shooting-down-a-drone/

LegiScan. (2017). *Bill text: OK SB660 | 2017 | Regular Session | Amended*. https://legiscan.com/OK/text/SB660/id/1527781

Loh, M. (2023, September 29). *UK PhD student guilty of 3D-printing a chemical-weapon drone for ISIS*. Business Insider. https://www.businessinsider.com/mohamad-al-bared-3d-print-drone-isis-chemical-weapon-2023-9

McNabb, M. (2025, December 9). *NDAA FY 2026: Key counter-UAS provisions explained*. DroneLife. https://dronelife.com/2025/12/09/ndaa-fy-2026-key-counter-uas-provisions-explained/

National Agricultural Law Center. (2015, October 29). *Judge drops charges on man who shot down drone*. https://nationalaglawcenter.org/judge-drops-charges-on-man-who-shot-down-drone/

National Conference of State Legislatures. (2023, March 27). *Current unmanned aircraft state law landscape*. https://www.ncsl.org/transportation/current-unmanned-aircraft-state-law-landscape

Office of Governor J. Kevin Stitt. (2024, December 16). *Governor instructs Department of Public Safety to protect Oklahomans against potential aerial threats*. https://oklahoma.gov/governor/newsroom/newsroom/2024/nov2024/governor-instructs-department-of-public-safety-to-protect-oklaho.html

Office of Governor Jeff Landry. (2025, June 18). *Louisiana becomes first state to authorize local law enforcement to neutralize dangerous drones*. https://gov.louisiana.gov/news/4865/

Port Freeport. (n.d.). *Frequently asked questions*. https://www.portfreeport.com/about/faq

Port Houston. (2019, March 4). *Use of drones triggers security actions at Port Houston*. https://porthouston.com/use-of-drones-triggers-security-actions-at-port-houston/

Port of Galveston. (2017, July 19). *Port of Galveston selected for drone detection pilot project* [Press release]. https://aapa.files.cms-plus.com/Port%20of%20Galveston%20Selected%20for%20Drone%20Detection%20Pilot%20Project.pdf

PortStrategy. (2025, August 14). *Port exercise targets drone threats*. https://www.portstrategy.com/port-and-terminal-news/port-exercise-targets-drone-threats/1504133.article

Read, B. (2018, August 10). *Drone assassins - scifi becomes reality*. The Royal Aeronautical Society. https://www.aerosociety.com/news/drone-assassins-scifi-becomes-reality/

Reuters. (2021, November 7). *Drone attack targets Iraq PM - who escapes unhurt, Iraq military says*. Reuters. https://www.reuters.com/world/middle-east/drone-attack-targets-iraq-pm-who-escapes-unhurt-iraq-military-2021-11-07/

Sea-Tac Noise Advisory Council. (n.d.). *FAA: Shoot down a drone, go to jail (for up to 20 years!)*. Retrieved December 10, 2025, from https://seatacnoise.info/bookmark/faa-shoot-down-a-drone-go-to-jail-for-up-to-20-years/

Shaw, M. (2025, October 15). *Texas DPS helicopters can now detect drones and operators*. FOX 7 Austin. https://www.fox7austin.com/news/texas-dps-helicopters-can-now-detect-drones-operators/

Sullivan, J. P. (2023, November 30). *Drones and port security in Brownsville: A case study on the Gulf*. Homeland Security Today. https://www.hstoday.us/featured/drones-and-port-security-in-brownsville-a-case-study-on-the-gulf/

Texas A&M University-Corpus Christi. (2019, February 19). *NASA selects Texas A&M University-Corpus Christi to test drones in urban traffic management*. https://www.tamucc.edu/news/2019/02/021919_lsuasc_nasa.php

Texas Government Code Ch. 423. (n.d.). *Use of Unmanned Aircraft*. https://statutes.capitol.texas.gov/?tab=1&code=GV&chapter=GV.423&artSec=

Tom's Hardware. (2025, November 23). DragonFire laser shoots down high-speed drones traveling at 400 mph, costs £10 ($13) per shot - UK Navy to begin deploying system on destroyers. https://www.tomshardware.com/tech-industry/uk-dragonfire-laser-downs-high-speed-drones

U.S. Congress. (2025). *S. 1071: National Defense Authorization Act for Fiscal Year 2026* (Engrossed as Handed text). Congress.gov. https://www.congress.gov/bill/119th-congress/senate-bill/1071/text/eah

U.S. Department of Homeland Security. (2025, April 10). *Counter Unmanned Aircraft Systems legal authorities fact sheet*. https://www.dhs.gov/publication/st-counter-unmanned-aircraft-systems-legal-authorities-fact-sheet

Wagstaff, K. (2015, December 11). *Tokyo police hope to snare rogue drones with net-carrying interceptor*. Time. https://time.com/4146372/tokyo-police-drone-nets/

Winks, D., Chill, S., Ferrer, F., Lovell, M. J., Swearingen, M., & Lasky, M. (2024, December 4). *Protecting critical infrastructure from weaponized drones*. Domestic Preparedness. https://www.domprep.com/articles/protecting-critical-infrastructure-from-weaponized-drones/

Wirth Law Office. (2023, July). *New law makes it a misdemeanor to spy with a drone in Oklahoma*. https://www.wirthlawoffice.com/tulsa-attorney-blog/2023/07/new-law-makes-it-a-misdemeanor-to-spy-with-a-drone-in-oklahoma/

Appendix I:

Evolution of Drone Attacks: From Military Tools to Terrorist Weapons, a Selective History.

Early Military Use of Drones in Warfare

Unmanned aerial vehicles (UAVs), commonly called drones, have been used in warfare for decades, but the modern era of drone attacks began in the early 2000s. The United States pioneered armed drones for counterterrorism: in November 2002, the CIA used a Predator drone in Yemen to carry out the first known targeted killing by UAV, eliminating an Al-Qaeda leader involved in the USS Cole bombing[1]. Throughout the 2000s, U.S. forces increasingly relied on drones like the MQ-1 Predator and MQ-9 Reaper for strikes in Afghanistan, Iraq, Pakistan, and elsewhere. These military drones, remotely piloted and equipped with missiles, demonstrated how UAVs could precisely hunt and strike high-value targets from afar. This state-level use of drones in warfare set the stage for non-state actors to adopt similar tactics on a smaller scale. By the 2010s, dozens of countries and militant groups had acquired drones, ushering in a new era of asymmetrical threats.

Militant and Terrorist Adoption of Weaponized Drones

In the 2010s, terrorist organizations and insurgent groups began to weaponize commercially available drones and DIY remote-controlled aircraft. This evolution greatly expanded their attack capabilities. Violent non-state actors (VNSAs) such as ISIS, Al-Qaeda affiliates, Hamas, Hezbollah, and Yemen's Houthi rebels all experimented with drones for offensive operations[2]. Early instances included Hezbollah's use of Iranian-supplied UAVs against Israel in the mid-2000s, and reports that Al-Qaeda plotted as

---

[1] Costs of War. (n.d.). About Costs of War. Retrieved November 14, 2025, from https://costsofwar.watson.brown.edu/about

[2] Dulligan, J., Freeman, L., Phoenix, A., & Davis, B. (2025, March). The rising threat of non-state actor commercial drone use: Emerging capabilities and threats. CTC Sentinel. Retrieved November 30, 2025, from https://ctc.westpoint.edu/the-rising-threat-of-non-state-actor-commercial-drone-use-emerging-capabilities-and-threats/

early as 2001 to attack the G8 summit in Italy with explosives-laden model airplanes[3]. In 2002, a terrorist plan in London even aimed to hit the British Parliament with a drone carrying an anthrax poison device, an ominous sign of interest in drones for chemical/biological attack, although this plot was thwarted.

By the mid-2010s, battlefields in the Middle East saw routine terrorist drone attacks. The Islamic State (ISIS) became notorious for its "drone air force" during the wars in Iraq and Syria. ISIS modified off-the-shelf quadcopters to drop grenades and small bombs on troops and civilians. In one 24-hour period in early 2017 during the Battle of Mosul, coalition forces reported up to 70 ISIS drones in the air, some armed as "killer bees" dropping 40mm munitions. That year saw a peak of over 250 ISIS drone attack incidents in Iraq and Syria. These were mostly small hobbyist drones adapted to carry explosives, demonstrating how easily terrorist groups could acquire and deploy aerial weapons. Although crude, ISIS drones caused significant disruption and some casualties. For example, in October 2016 ISIS fighters rigged quadcopters to drop mortar shells and managed to kill two Kurdish fighters and when a downed, booby-trapped drone exploded upon inspection, injured French special forces troops. Other militant groups followed suit: Hamas and other Palestinian militants have flown drones or DIY gliders with explosives towards Israel, and Hezbollah has used one-way explosive UAVs (essentially kamikaze drones) against Israeli targets since the 2000s. In one notable case, Hezbollah sent an Iranian-made drone packed with explosives into Israeli airspace in 2006. It was shot down before reaching its target.

Outside the Middle East, Mexican drug cartels also began adopting drone tactics. Cartels initially used drones for smuggling but soon weaponized them. By the late 2010s and early 2020s, cartels were dropping grenades or IEDs from drones on rival gangs and security forces. This trend accelerated dramatically: in 2023, over 260 drone bomb attacks were documented in Mexico[4]. In one 2025 incident, a cartel used three

---

[3] Read, B. (2018, August 10). Drone assassins – sci-fi becomes reality. Aerospace (The Society for Aerospace Professionals). https://www.aerosociety.com/news/drone-assassins-scifi-becomes-reality/

[4] Fletcher, Z. B. (2025, November 14). How cartels are adopting drone tactics from Ukraine. Defense News. https://www.defensenews.com/unmanned/2025/11/14/how-cartels-are-adopting-drone-tactics-from-ukraine/

first-person-view (FPV) racing drones rigged with C4 to bombard the state prosecutor's office in Tijuana and the drones exploded and showered the parking lot with nails, ball bearings, and shrapnel. Cartel drone strikes have injured police and soldiers, and have even been followed by ground assaults. These developments show that capabilities once limited to nations are now in the hands of cartels and terrorists, who use cheap drones to mimic military tactics. Drones give such groups a kind of "air force" on the cheap, enabling them to target enemies from above while staying out of direct combat.

Drone use by VNSAs poses a significant threat as it provides these groups with a versatile platform with capabilities to achieve several operations. Drones provide VNSAs with an additional tool to accomplish their strategic, ideological, and psychological goals. Drones enable VNSAs to gain a presence within the air, granting them a 'miniature' air force, at extremely low costs. Moreover, the cost barrier to entry for recreational 'hobbyist' drones continues to decrease, even as drones continue to see significant performance increases in their capabilities. Commercial and hobbyist drones also require minimum training by operators. COTS drones typically require no training to learn how to fly, and there are numerous instructional videos and forums that operators can learn from online.

Landmark Drone Attacks and Assassination Attempts

In the last decade, a number of high-profile drone attacks and assassination attempts have grabbed global attention; many of which occurred when drones were used against prominent targets or critical infrastructure:

Attempted Assassination of Venezuelan President (2018): In August 2018, two drones loaded with C-4 explosives were flown toward a military parade where President Nicolás Maduro was speaking. The attackers used high-end commercial DJI Matrice 600 hexacopter drones carrying about 1 kg of C-4 each[5]. One drone was apparently intended to explode above the president's podium and the other in front of him,

[5] Read, Bill. "Drone Assassins — Sci-Fi Becomes Reality." *Royal Aeronautical Society*, August 10, 2018. https://www.aerosociety.com/news/drone-assassins-scifi-becomes-reality/

potentially killing him with shrapnel. Fortunately for President Maduro, Venezuelan security forces jammed one drone and the other lost control, detonating early. The blast injured seven soldiers, but Maduro survived unharmed. This incident, the first known drone "assassination" attempt on a head of state, underscored the new threat of drones to VIP protection. It showed that even a relatively small hobby drone, if turned into a flying bomb, could penetrate a secure zone and threaten a president.

Attack on Saudi Oil Facilities (2019): In September 2019, drones were used in a coordinated strike on Saudi Arabia's Abqaiq and Khurais oil processing facilities (attributed either to Houthi rebels or Iran). A swarm of drones and cruise missiles breached Saudi defenses, causing massive fires and halting about half of Saudi oil output temporarily. This was a landmark in drone warfare against infrastructure. The drones (reportedly Iranian-made kamikaze UAVs) demonstrated precision by slamming into critical equipment. This attack, though outside the U.S., alarmed American homeland security experts because it showed how drones could cripple critical energy infrastructure. It prompted U.S. authorities to consider similar threats to power plants and refineries at home[6].

Wars in Ukraine and Israel have shown how drones can be used to destroy civilian infrastructure[7]. In a similar fashion, transnational crime organizations embrace weaponized drones to combat rivals and police, as the use of weaponized drones is spreading beyond warzones[8]. In 2020, a drone was used in an attempt to disrupt the US power grid[9] by attacking a substation in Pennsylvania by dropping a metal cable

---

[6] Winks, D., Chill, S., Ferrer, F., Lovell, M. J. "Apollo", Swearingen, M., & Lasky, M. (2024, December 4). *Protecting critical infrastructure from weaponized drones*. Domestic Preparedness. https://domesticpreparedness.com/articles/protecting-critical-infrastructure-from-weaponized-drones/

[7] Kanal13. (n.d.). "Kyiv takes revenge"-Ukraine launches massive drone attacks targeting Russia's energy infrastructure [Video]. YouTube. https://www.youtube.com/watch?v=vD7fZ_0J4GM

[8] Bunker, R. J., & Sullivan, J. P. (2021, November 11). Mexican cartels are embracing aerial drones and they're spreading. War on the Rocks. https://warontherocks.com/2021/11/mexican-cartels-are-embracing-aerial-drones-and-theyre-spreading/

[9] Barrett, B. (2021, November 5). A drone tried to disrupt the power grid. It won't be the last. WIRED. https://www.wired.com/story/drone-attack-power-substation-threat/

across high-voltage lines. Fortunately, the attack was unsuccessful. However, it is only a matter of time[10] before a drone attack disables or destroys critical infrastructure.

Drone Swarm Attack on Russian Base (2018): In January 2018, a Syrian insurgent group (unconfirmed, possibly ISIS or an Al-Qaeda affiliate) launched a coordinated swarm of thirteen armed drones at Russia's Khmeimim Air Base in Syria. The small DIY fixed-wing drones carried improvised explosives. Russian defenses managed to shoot down or jam most of them, but the incident proved that non-state actors could deploy swarm tactics previously seen only in military R&D labs. A swarm attack could overwhelm a target's defenses by sheer numbers. This was one of the first recorded instances of a large drone swarm attack by militants, hinting at future "saturation" attacks that have security officials concerned.

Assassination Attempt on Iraq's Prime Minister (2021): On November 7, 2021, attackers launched three explosive-laden drones at the residence of Iraqi Prime Minister Mustafa al-Kadhimi in Baghdad. Two drones were shot down by security, but one drone managed to hit Kadhimi's house, exploding on impact[11]. The PM was unharmed, but several of his bodyguards were injured and the blast damaged the building. This attack, described by Iraqi and U.S. officials as a "heinous act of terrorism", highlighted how armed drones can strike even in heavily fortified zones (e.g., the Green Zone). The drones used were relatively small, likely modified quadcopters or DIY drones carrying explosives, yet they nearly succeeded in killing a national leader. No group claimed responsibility, but suspicion fell on Iran-backed militia factions angered by election results. The incident underscored the growing reliance on drones for targeted political violence.

Disruption of Gatwick Airport (2018): In December 2018, London's Gatwick Airport was shut down for several days due to rogue drones repeatedly flying into its airspace.

---

[10] Crino, S., & Dreby, C. (2020). Drone attacks against critical infrastructure: A real and present threat (Issue brief). Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2020/05/DRONE-ATTACK-0420-WEB.pdf

[11] Reuters. (2021, November 7). Drone attack targets Iraq PM who escapes unhurt, Iraq military says. Reuters. https://www.reuters.com/world/middle-east/drone-attack-targets-iraq-pm-who-escapes-unhurt-iraq-military-2021-11-07/

While not an “attack” in the traditional sense, this was a landmark incident of drones disrupting critical infrastructure. Unknown operators flew drones near runways, forcing hundreds of flights to be diverted or canceled as a safety precaution. The Gatwick incident stranded tens of thousands of travelers and cost airlines and businesses millions of dollars. It demonstrated the chaos that a few small drones could inflict on a major airport without even carrying a weapon. This spurred airports worldwide (including many in the U.S.) to invest in counter-drone detection and jamming systems to prevent copycats. Gatwick proved that drones could be used as tools of economic disruption, not just direct destruction.

Drone Attacks and Plots in the United States

Within the United States, there have been few successful drone attacks to date, but several foiled plots and alarming incidents illustrate the threat:

Foiled Pentagon/Capitol Bomb Plot (2011): One early case was a 2011 plot by Rezwan Ferdaus, a Massachusetts man and Al-Qaeda supporter, to attack the U.S. Capitol and Pentagon with remote-controlled aircraft. Ferdaus planned to pack several large remote-controlled scale model hobby airplanes with C-4 explosives and crash them into these buildings[12]. He procured a small fleet of drones, some over 5 feet long, and even built improvised detonators. However, an FBI undercover operation intercepted him before he could obtain real explosives. Ferdaus was arrested in September 2011 when he tried to arm the drones. He later pled guilty. This case showed that jihadist terrorists had begun plotting drone attacks on U.S. soil over a decade ago. Although the public was never in actual danger (the explosives he received were inert, supplied by the FBI), the plot revealed the *intent* to use drones as flying bombs against iconic targets in America.

[12] Federal Bureau of Investigation. (2011, September 28). Massachusetts man charged with plotting attack on Pentagon and U.S. Capitol and attempting to provide material support to a foreign terrorist organization. FBI. https://archives.fbi.gov/archives/boston/press-releases/2011/massachusetts-man-charged-with-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-material-support-to-a-foreign-terrorist-organization

White House Drone Incidents (2015): In January 2015, an off-the-shelf DJI Phantom quadcopter famously crash-landed on the White House lawn. In this case, the pilot was an intoxicated hobbyist, not a malicious actor[13]. While not considered an attack, this high-profile breach underscored a security gap: a cheap drone had penetrated the heart of Washington, D.C.'s no-fly zone. The incident prompted a wave of concern about how easily a drone could carry a payload such as explosives or hazardous material to attack sensitive U.S. sites. Lawmakers held hearings on the worst-case scenarios, such as drones dispersing anthrax over a crowd. Around the same time, another individual in Connecticut posted YouTube videos of a hobby drone modified to fire a handgun; he was later investigated by the FAA. These events were a wake-up call that drones, even in the hands of pranksters or lone wolves, could breach secure areas. The Department of Homeland Security and Secret Service began testing counter-drone measures in response.

Power Grid Sabotage Attempts (2020 and 2024): Perhaps the most concerning U.S. incidents involve attempts to use drones to attack critical infrastructure. In July 2020, an unidentified perpetrator flew a modified drone toward a Pennsylvania power substation, likely intending to disrupt the electric grid. The small drone that was discovered on the premises had a trailing tethered wire; a makeshift conductive cable meant to short out high-voltage equipment by dropping across power lines[14]. The device crashed into the substation fence and did not cause an outage, but investigators called it the first known drone-based attack on U.S. critical infrastructure. The FBI noted that the drone was stripped of identifying markings and memory, indicating a somewhat sophisticated attempt at stealth.

In November 2024, the FBI foiled a plot to attack the Nashville power grid with an explosive-laden drone. In that case, a suspect had ordered C-4 explosives and planned

---

[13]Franzen, C. (2015, March 18). Anthrax-spraying drones are probably not something Congress should worry about. VICE. https://www.vice.com/en/article/anthrax-spraying-drones-are-probably-not-something-congress-should-worry-about/

[14] Domestic Preparedness. (2024, December 4). Protecting critical infrastructure from weaponized drones. https://www.domesticpreparedness.com/articles/protecting-critical-infrastructure-from-weaponized-drones/

to use a drone to bomb a substation transformer. Undercover agents intercepted the explosives and arrested the man before he could carry out the attack. These incidents highlight exactly the kind of scenario homeland security officials fear: terrorists or extremists using drones to knock out electricity grids or other utilities. A well-placed drone strike on a transformer substation or gas pipeline could cause cascading outages and industrial accidents. The U.S. Department of Homeland Security has warned that thousands of substations and power plants are vulnerable to such small aerial incursions, and hardening every site is impractical. As a result, efforts are underway to deploy counter-drone systems around key facilities and to update laws so that security teams can disable rogue drones legally.

Border and Domestic Surveillance by Criminals: Beyond direct attacks, DHS is also grappling with drones used for cross-border crime. Smuggling and surveillance drones are commonly operated by Mexican cartels across the U.S.-Mexico border, over 1,000 illicit drone flights per month, according to U.S. Northern Command in 2024[15]. These drones are used to ferry drugs, scout Border Patrol positions, or even attack rivals on the Mexican side. While not “terrorism,” their tactics could easily be adapted by terrorists to penetrate U.S. airspace. Small drones have also been spotted over U.S. chemical plants, ports, stadiums, and other sensitive locations, raising suspicions. In one mysterious 2019 episode, a swarm of drones flew nightly over rural Colorado and Nebraska for weeks, unnerving residents and prompting an FBI investigation, although no malicious activity was confirmed. All these episodes underscore that the U.S. homeland is not immune, and drones are a new dimension of the threat environment that DHS, FBI, and other agencies are racing to address.

WMD and Biological Attack Fears Involving Drones

One of the gravest concerns is the possibility of terrorists using drones to deliver chemical, biological, radiological, or nuclear (CBRN) weapons. While there have been

---

[15] Fletcher, Z. B. (2025, November 14). *How cartels are adopting drone tactics from Ukraine.* Defense News. https://www.defensenews.com/unmanned/2025/11/14/how-cartels-are-adopting-drone-tactics-from-ukraine/

no successful biological drone attacks to date, there are a few documented cases and plots that illustrate the intent and feasibility:

Aum Shinrikyo's Drone Experiment (1990s): The Japanese doomsday cult Aum Shinrikyo, infamous for the 1995 Tokyo subway sarin attack, explored using remote-controlled helicopters to disseminate chemical and biological agents. In 1995, Aum Shinrikyo members *planned* to use an RC helicopter to spray anthrax in Tokyo[16]. They had developed a crude drone capability and even conducted test runs (they released anthrax from a rooftop in 1993, though fortunately it was an inert strain that caused no harm). Aum's drone plans never came to full fruition due to technical failures and the group's crackdown by authorities. However, it stands as an early example of terrorists envisioning drones for bioweapons delivery.

Al-Qaeda's Anthrax and "Dirty Bomb" Ambitions: During the early 2000s, Al-Qaeda considered various WMD attack methods. British and U.S. intelligence revealed that in 2002 Al-Qaeda sympathizers discussed attacking the UK Parliament with a remote drone dispersing anthrax[17]. Around the same time, reports surfaced that Al-Qaeda was interested in using crop-dusting planes or drones to spread chemical/biological agents. In 2003, U.S. forces in Afghanistan found Al-Qaeda training manuals referring to aerial dispersion of pathogens. While these remained only plans, not executed attacks, they demonstrate that the idea of a drone-based bio-terror attack has been on terror groups' radar for decades.

ISIS and Chemical Drones: ISIS used chemical weapons such as chlorine gas and sulfur mustard in Syria and Iraq on a limited scale, mainly via ground-fired shells. There is some evidence that by 2017 ISIS was actively researching drone delivery of chemical and biological agents[18]. A U.S. Army analysis noted that ISIS showed interest in arming

---

[16] Armscontrol.ru. (n.d.). Media reports of terrorist attempts to use UAVs. https://www.armscontrol.ru/UAV/clips.htm

[17] Royal Aeronautical Society. (2018, August 10). Drone assassins – sci-fi becomes reality. The Royal Aeronautical Society. https://www.aerosociety.com/news/drone-assassins-scifi-becomes-reality/

[18] Lambert, C. A. (2020, October). The chemical and biological attack threat of commercial unmanned aircraft systems (Spotlight 20-5). Association of the United States Army.

drones with chemical payloads once they had mastered conventional grenade-dropping drones. For example, coalition forces found ISIS documents and conversations about using drones to spray toxins or as “dirty bomb” carriers. No confirmed instance of ISIS actually deploying a chemical warhead on a drone has been reported. However, the group’s routine drone attacks with explosives, combined with its known use of chlorine in roadside bombs, raises the concern that a small drone could similarly release chlorine gas or another toxic agent over troops or civilian areas.

The number of potential attacks using drones in this manner has also increased, although to date none have succeeded. As early as 2001, the terrorist group Al Queda plotted to attack the G8 Summit in Genoa, Italy with explosive devices attached to remote-controlled drones followed by a plot in 2002 to attack the British House of Commons with a drone equipped with an anthrax poison device. In 2016, a UK insurance company report warned of the use of weaponized drones by ISIS against ‘soft targets’ in the country while the terror organization has also been implicated in plans to use drones to spray ‘dirty bomb’ nuclear material over Western cities.

Security experts have warned that a few DJI Phantom drones with spray attachments could disperse chemicals over a crowd, potentially causing panic, if not mass casualties[19]. The psychological impact of such an attack could be enormous, even if the technical lethality is limited.

Radiological Drone Stunt (2015): A bizarre incident in April 2015 in Japan showed the real-world potential of a radiological drone scare. A Japanese citizen protesting nuclear energy flew a small drone onto the roof of the Prime Minister’s office in Tokyo, carrying a container of radioactive cesium (collected from a Fukushima site)[20]. The drone landed

---

https://www.ausa.org/sites/default/files/publications/SL-20-5-The-Chemical-and-Biological-Attack-Threat-of-Commercial-Unmanned-Aircraft-Systems.pdf

[19] Franzen, C. (2015, March 18). Anthrax-spraying drones are probably not something Congress should worry about. VICE. https://www.vice.com/en/article/anthrax-spraying-drones-are-probably-not-something-congress-should-worry-about/

[20] Lambert, C. A. (2020, October). *The chemical and biological attack threat of commercial unmanned aircraft systems* (Spotlight 20-5). Association of the United States Army.

harmlessly and the radiation was not enough to hurt anyone, but it caused a security alert. The drone had a biohazard symbol on it and could easily have been mistaken for a serious radiological attack device. This event proved that even a lone actor with a drone and hazardous material could spark panic and breach a high-security location. After this, Japanese authorities accelerated their counter-drone initiatives, especially for protecting government buildings and events like the 2020 Tokyo Olympics.

Recent Foiled Plots: In 2023, British counter-terrorism police arrested Mohamad al-Bared, a PhD engineering student in Coventry, who had built a custom drone intended to deliver chemical weapons for ISIS[21]. Al-Bared 3D-printed a large fixed-wing drone (roughly 6 feet long) designed to carry a warhead or toxic payload. He researched deadly poisons like ricin, sarin, and mustard gas to potentially fill the drone's payload compartment. The drone was essentially a DIY cruise missile: it could carry a thermos-sized container of chemicals or explosives and was meant to crash into a target, releasing the payload. Fortunately, he was caught before he could hand it off to any operatives. This case was a chilling reminder that technically educated lone actors can design drones specifically for WMD delivery. The drone Al-Bared built illustrates the kind of "homebrew" kamikaze UAV that terrorist groups may try to use.

Despite these plots and experiments, no major biological or chemical drone attack has yet occurred in the West. However, officials caution that it's not for lack of intent, but rather technical hurdles; dispersing biological agents effectively is hard, and obtaining weaponized pathogens is even harder. Experts note that small drones can only carry limited payloads (a few pounds at most), so a widespread lethal bio-attack would likely require many drones or a very potent agent. Still, even a minor drone-delivered bio attack could sow widespread panic. For instance, a drone releasing *simulated* anthrax powder over a stadium could trigger mass fear and evacuation. Thus, homeland

---

https://www.ausa.org/sites/default/files/publications/SL-20-5-The-Chemical-and-Biological-Attack-Threat-of-Commercial-Unmanned-Aircraft-Systems.pdf

[21] Loh, M. (2023, September 29). *UK PhD student guilty of 3D-printing a chemical-weapon drone for ISIS.* Business Insider. https://www.businessinsider.com/mohamad-al-bared-3d-print-drone-isis-chemical-weapon-2023-9

security planners treat CBRN drone threats very seriously, running drills and developing sensors to detect any drone spraying mysterious substances[22].

[22] Kallenborn, Z. (2023, November 21). Why cheap drones pose a significant chemical terrorism threat. Bulletin of the Atomic Scientists. https://thebulletin.org/2023/11/why-cheap-drones-pose-a-significant-chemical-terrorism-threat/

Appendix II:

International Approaches: Anti-Drone Laws Abroad (Pros and Cons)

Around the world, governments are grappling with the drone threat to privacy and critical infrastructure. Some countries have enacted landmark laws that go beyond what the U.S. currently allows, giving a glimpse of what *"top performers"* in drone defense are doing. Here are a few notable examples and their pros and cons:

United Kingdom: The UK has developed a structured legal approach in response to high-profile incidents like the Gatwick Airport drone shutdown in 2018. They launched a Counter-Unmanned Aircraft Strategy in 2019, and in 2021 passed the Air Traffic Management and Unmanned Aircraft Act to bolster enforcement[23]. Police powers were greatly expanded - officers can require drone pilots to produce registration documents, stop and search people for drones, issue on-the-spot fines for drone offenses, and even seize drones or force them to land. Importantly, UK law also tackles the technical side: the government clarified that existing authority under the Wireless Telegraphy Act allows authorized personnel to jam or intercept drone radio signals when necessary for public safety. In practice, the UK has deployed military-grade anti-drone equipment (radar and RF jammers) at major airports and prisons.

Pros: Clear legal authority for police to act fast, and a national framework coordinating aviation regulators, law enforcement and even the military. The UK moved from reactive measures to a proactive stance, embedding counter-drone capabilities at sensitive sites.

Cons: Privacy advocates worry about police overreach, since broad powers to stop, search, and surveil drone users could implicate innocent hobbyists or put freedom of the press in peril. The UK approach also requires significant investment in technology at critical infrastructure sites, which is costly - but the payoff was seen when new incidents

[23] Kochavi, H. (2025, April 22). *Navigating the European skies: The push for a unified counter-drone regulatory framework.* Sentrycs Counter-Drone Blog. https://sentrycs.com/the-counter-drone-blog/navigating-the-european-skies-the-push-for-a-unified-counter-drone-regulatory-framework/

have been promptly contained. Overall, the UK is seen as leading in preparedness by giving officials both the legal toolkit and equipment to handle rogue drones.

Japan: Japan responded early to drone threats after a notorious 2015 incident (a protester landed a drone with trace radioactive material on the Prime Minister's roof). Japan swiftly amended its Civil Aeronautics Law to ban drone flights over densely populated urban areas, near airports, and over certain government or nuclear facilities[24]. Violators face heavy fines up to ¥500,000 (around $4,000). Tokyo's Metropolitan Police even formed a special Drone Interceptor squad equipped with large drones carrying nets to literally snare offending drones in mid-air. Police first issue a loudspeaker warning to the operator, and if ignored, they launch these net-drones to capture the rogue drone[25].

Pros: Japan's strict no-fly zones over cities mean a private citizen in Tokyo is *highly unlikely* to ever see a snooping drone out their window; it's flat-out illegal there. The net-wielding police drones are a non-lethal, controlled response that avoids stray bullets or signal jamming interference. It's a visually dramatic but effective technique, and similar net drones have been considered in France and other countries as well.

Cons: The blanket ban on drones in urban areas is a blunt tool. It stifles beneficial uses (like deliveries or hobby flying in cities) unless special permission is obtained. It trades innovation for security. Also, deploying police drones with nets is feasible in a controlled city environment, but may be less practical in wide open rural skies or if facing multiple drones or faster, more maneuverable UAVs. Still, Japan's approach does work in the sense that it has prevented a "Wild West" of drones in crowded areas and given law enforcement a clear mandate to remove threats.

Europe (General & EU): Many European countries are updating laws, though the approach is not uniform. Germany acknowledged their regulatory gap and in late 2024

---

[24] Mollman, S. (2015, December 10). *Tokyo police are deploying drones that use nets to capture drones.* Quartz**.** https://qz.com/571654/tokyo-police-are-deploying-drones-that-use-nets-to-capture-drones/
[25] Malou-Tech. (n.d.). *Drone antidrone interceptor surveillance* [Video]. YouTube. https://www.youtube.com/watch?v=rMFBUZ8iLTw

announced plans to explicitly empower both police and the military to counter drones. In 2025 the German government moved to amend its Aviation Security Act to allow the Bundeswehr (armed forces) to shoot down or neutralize drones over critical infrastructure during emergencies, stepping in when local police lack capabilities. A reform of the Federal Police Act is also underway to let German police use advanced counter-drone tools like electromagnetic pulse disruptors and radio jammers (currently such actions were legally unclear). France, facing drone issues and in preparing for events such as the 2024 Paris Olympics, updated its laws to strengthen drone defense as well. The top administrative court in France (Conseil d'État) recently approved the use of surveillance drones by police for public security, after privacy challenges. More relevant, France's 2024-2030 military funding law allocates €5 billion specifically for anti-drone and air defense technologies, including systems to detect and neutralize aerial threats. During the 2024 Olympics, France deployed a multi-layered C-UAS system (combining radar, radio-frequency jamming/cyber takeover tools, and some projectile interceptors) to protect venues.

Pros: Countries like Germany and France are creating explicit legal authority to act (so responders aren't paralyzed by legal doubts in a crisis) and backing it with serious investment in technology. This comprehensive strategy - *legal plus technical* - is considered a best practice. It acknowledges that drones can be both a safety hazard and a potential tool for terrorism, so countermeasures must be ready.

Cons: European nations face constraints from strict privacy and data laws (e.g. GDPR), which sometimes slow these efforts. For instance, using detection systems that record drone pilot signals or using police drones to surveil crowds has raised data protection issues in the EU. There is also fragmentation: until an EU-wide framework is harmonized, a drone could be illegal to down in one country but not in another, complicating cross-border threats. Europe is actively working on an EU-wide Counter-UAS framework to harmonize these rules.

In short, the "top performers" abroad blend law and technology: they legally empower authorities to act decisively *and* deploy counter-drone systems at critical sites. The U.S.

could take note by similarly updating laws to allow state and local responders (not just federal agents) to engage rogue drones and by investing in approved counter-drone tech for places like airports, power plants, and ports.

Other Notable Measures: A few creative tactics have been tried elsewhere. The Netherlands experimented with training eagles to grab drones from the sky (relying on natural instincts to intercept moving prey). This garnered viral attention around 2016 and was initially successful in tests as a low-tech interception method. However, Dutch police ended the program after finding that the eagles were *unpredictable and hard to train at scale* - a reminder that not every novel idea will pan out. Australia and Canada enforce strict drone regulations (such as requiring licensing, and imposing heavy fines for flying too close to people or restricted areas), but they, like the U.S., currently do not allow individuals to disable drones. Instead, they focus on registration and remote ID, hoping that clear identification of drones will deter misuse and aid in enforcement. Israel - facing hostile drones on its borders - has deployed advanced anti-drone weapons (from radio jamming to laser interceptors) and gives its military broad authority to shoot down suspicious UAVs. The Israeli approach is very security-driven (for obvious reasons) and shows high effectiveness in wartime scenarios, but applying such military-grade responses in civilian domestic airspace raises safety issues elsewhere.

Pros of these varied approaches include deterrence (would-be perpetrators know drones can be countered) and quick neutralization of threats.

Cons can include false positives (disabling a harmless hobby drone by mistake), the risk of falling drones causing damage, and the technical challenge that many counter-drone methods (jamming, lasers, intercept drones) have limited range or effectiveness against drone swarms. Each country's solution has trade-offs between security and freedom - e.g., outright bans and broad shoot-down powers maximize security but reduce the freedom to use drones commercially or recreationally; whereas hands-off approaches maximize innovation but leave gaps for "bad guy" exploitation.

In evaluating these, one can see a pattern: Leading nations empower their law enforcement (or even military) to act swiftly against drones and build out an

infrastructure of detection and interdiction. The United States can learn from these examples by developing a clearer legal framework that, for instance, could *authorize state or local authorities to use calibrated counter-drone measures in defined emergencies*, similar to the UK or German models. At the same time, U.S. policymakers must weigh constitutional rights - for example, broad drone interdiction powers might conflict with First Amendment interests (if a drone is used for newsgathering) or Fourth Amendment rights (if authorities misuse anti-drone tech for surveillance). The ACLU and civil liberties groups in the U.S. have raised concerns that some proposed counter-drone laws give government too much power to intercept private drones and data without oversight[26]. Thus, a balance is needed: other countries show it's possible to tighten security against drone threats, but each approach comes with pros and cons that the U.S. must carefully adapt to its legal context.

[26] AirSight. (2018, October 9). *FAA Reauthorization Bill of 2018: UAS integration and countering drone threats*. https://www.airsight.com/en/news/faa-reauthorization-bill-of-2018-uas-integration-and-countering-drone-threats/

Author Biographies

Dr. Art Wolfskill, Ph.D., is a Professor of Agribusiness at Sam Houston State University, where he specializes in finance, entrepreneurship, and the integration of unmanned aerial systems (UAS) within critical infrastructure and primary industries. A leading expert in aerial applications, he teaches Drone Applications in Agriculture and Industry, focusing on the dual-use nature of UAS technology for both economic efficiency and site security.

Dr. Wolfskill brings over eight years of experience flying drones, with FAA TRUST and Part 107 certifications, as well as a portfolio built upon a distinguished career as a U.S. Army helicopter pilot. During his military service, he was assigned to Air Cavalry units, where he developed a foundational understanding of aerial reconnaissance, threat detection, and airspace management in high-stakes environments.

His current research for the Institute for Homeland Security leverages this unique blend of tactical military aviation and academic rigor to address emerging vulnerabilities in maritime and industrial sectors. By combining operational experience with strategic policy analysis, Dr. Wolfskill provides actionable insights into defending Texas's ports and critical infrastructure against the evolving threat of drone incursions.

Michael A. Wolfskill is an independent researcher and operations specialist with over a decade of experience leading international, high-pressure teams in Latin America. A graduate of Sam Houston State University with a degree in Mass Communications, Michael has built a career at the intersection of technical infrastructure and strategic management. He possesses extensive experience in operations, sales, and marketing management, specializing in scaling complex operations, designing customer acquisition initiatives, and navigating the needs of cross-functional stakeholders.

As a technologist and drone enthusiast, Michael focuses his research on the evolving role of Unmanned Aerial Systems (UAS), matching their technological potential with modern-day use cases and practice. By leveraging his professional background in technology and global operations, he provides a unique perspective on the critical balance between national security, economic resilience, and civil liberties in the age of autonomous systems.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

Wolfskill, A. (2026). Defending Texas Ports from Malicious Drones: Authority Gaps, Emerging Federal Pathways, and Operational Readiness After the FY26 NDAA. (Report No. 2026 -1043). The Sam Houston State University Institute for Homeland Security.

https://doi.org/10.17605/OSF.IO/5TX48

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY