Utilizing Lessons from Foreign UAS Threats to Inform Domestic Counter-UAS

Brice A. Ott
Program Executive Office Simulation, Training, and Instrumentation (PEO STRI)
Threat Systems Management Office (TSMO)
Huntsville, AL
brice.a.ott.civ@army.mil

ABSTRACT

The rapid proliferation and technological advancement of Unmanned Aircraft Systems (UAS) is reshaping modern warfare, with adversaries using these systems for disruption, reconnaissance, and strikes against U.S. forces abroad. As these technologies become more accessible, there is an increased risk to domestic targets such as military bases, critical infrastructure, and special events. The U.S. urgently needs cohesive policies, effective Counter-UAS (C-UAS) testing, training, and defense strategies, informed by lessons from foreign threat encounters, to ensure domestic security from UAS threats.

This paper examines integrating C-UAS solutions into domestic defense, specifically focusing on leveraging insights from UAS threats overseas to enhance preparedness against domestic risks through advanced training capabilities. It highlights the growing incidents of clueless, careless, and criminal UAS uses and underscores the urgent need for the Department of Defense (DoD), Department of Justice (DOJ), Department of Homeland Security (DHS), and other agencies to enhance training programs, including simulation-based exercises and live red teaming, alongside testing and policy alignment, to defeat UAS threats.

This analysis identifies areas for policy improvement, such as fragmented authority, inconsistent response and detection standards, and airspace management constraints across federal, state, and local levels, while balancing ethical, legal, civil liberties, and logistical considerations of expanding domestic UAS countermeasures. Additionally, it proposes innovative frameworks to enhance information-sharing, interagency collaboration, and domestic C-UAS testing and training capabilities, incorporating embedded training and testing within the Live, Virtual, Constructive (LVC) domain to ensure national security through a robust, exercisable capability for collective training and combat readiness.

ABOUT THE AUTHOR

Mr. Brice A. Ott is a Project Director within the Program Executive Office Simulation, Training, and Instrumentation's (PEO STRI) Threat Systems Management Office (TSMO). His professional experience includes a proven track record of Department of Defense acquisition and systems engineering of military modeling and simulation, and training systems. In his career, he was the leading director in standing up the U.S. Army's current Threat UAS training program. His focus includes technology modernization, testing and training UAS capabilities, live threat, wireless technologies, and networking infrastructure.

Utilizing Lessons from Foreign UAS Threats to Inform Domestic Counter-UAS

Brice A. Ott
Program Executive Office Simulation, Training, and Instrumentation (PEO STRI)
Threat Systems Management Office (TSMO)
Huntsville, AL
brice.a.ott.civ@army.mil

INTRODUCTION

The rapid proliferation of Unmanned Aircraft Systems (UAS), also known as "drones", has upended both global warfare and domestic security, delivering game-changing capabilities while introducing a host of complex, fast-moving threats. Whether it is budget-friendly quadcopters or advanced military-grade drones, these devices are now in the hands of everyone from nation-states and proxy forces to criminal networks and lone individuals, and they are being employed for surveillance, disruption, and precision strikes. UAS technology keeps evolving by becoming cheaper, smarter, and more far-reaching, while traditional defense frameworks are being outpaced by the speed and scale of the threat.

Recent international conflicts, particularly in Ukraine, Syria, and Israel, have put the transformative power of drones on full display. These engagements have featured everything from coordinated swarm attacks and Artificial Intelligence (AI)-guided navigation to the use of civilian supply chains for covert drone launches. These tactics have laid bare the weaknesses in sophisticated military defenses. Just as critically, these foreign UAS use cases highlight how easily similar methods could be adapted for use against domestic U.S. targets.

Domestically, the threat is no longer theoretical. Federal reports show a steady climb in drone-related incidents each year, ranging from negligent intrusions near airports to suspicious overflights of military installations and critical infrastructure. Although federal and local agencies are working to develop Counter-UAS (C-UAS) responses, progress is constrained by fragmented authority, inconsistent detection and response standards, limitations in airspace management, and legal policies. When drone attacks happen, they happen fast, often leaving security personnel without the authority or tools to act in time.

To address these gaps, the United States must urgently rethink its approach. There is an urgent need for clear, unified policies, cutting-edge testing environments, and rigorous training programs rooted in the hard-earned lessons of foreign conflicts. Leveraging simulation-based exercises, live red teaming, and embedded C-UAS scenarios within the Live, Virtual, Constructive (LVC) domain are critical components of a ready defense posture.

This paper utilizes publicly available intelligence and interviews with Subject Matter Experts (SMEs) to highlight how insights from foreign UAS operations can guide domestic defenses. It offers practical strategies in areas like training, policy reform, and interagency coordination steps aimed at helping national security, law enforcement, and homeland defense entities stay one step ahead in these high-stakes and fast-evolving arenas.

BACKGROUND

UAS Threats in Foreign and Military Contexts

Over the last ten years, drones have moved from being fringe tech curiosities to essential tools of modern warfare. Once the exclusive domain of state-funded programs, UAS are now used by traditional militaries and asymmetric actors alike. This shift is not only technological but strategic. Drones now actively shape how wars are fought, often tipping the scales in surprising ways. Examining global UAS employment offers sobering lessons for the U.S. as it seeks to secure its own skies (CSIS, 2025; Reuters, 2019).

Nowhere is this transformation more vivid than in Ukraine. Since Russia's 2022 invasion, both Ukrainian and Russian forces have leaned heavily on drones, turning the airspace over the battlefield into a proving ground for aerial autonomy, innovation, and adaptation (CSIS, 2025). Ukraine has embraced the art of using inexpensive, first-person view (FPV) drones for everything from intelligence gathering to kamikaze-style strikes on tanks and bunkers (CEPA, 2023; War on the Rocks, 2024). Many of these devices are assembled from commercial parts and controlled with off-

the-shelf controllers and headsets, costing as little as $400 a unit (McGee, 2024). Yet they deliver an outsized strategic impact. As one U.S. defense contractor put it, “Ukraine has demonstrated hyper evolution...presenting a nearly impossible challenge for industry” (Anonymous industry expert, SME #3, personal communication, June 5, 2025).

A defining moment came on June 1, 2025, during Operation Spiderweb. In a meticulously coordinated attack, Ukrainian forces launched a barrage of 117 FPV drones, concealed in civilian trucks and launched from within Russian territory, targeting Russian strategic air bases stretching from Olenya to Belaya. By the end of the operation, more than 40 aircraft had been hit, including strategic bombers and airborne early warning aircraft, causing an estimated $7 billion worth of damage. Russia lost about a third of its cruise missile bomber fleet to drones that cost a fraction of their targets' value (Reuters, 2025; CSIS, 2025; Guardian, 2025). Perhaps most revealing was the inability of Russian air defenses to respond to a dispersed, low-signature, multi-axis threat.

In the Middle East, drones have helped non-state actors sidestep billion-dollar defense systems. Back in 2019, Houthi rebels in Yemen claimed responsibility for a coordinated drone and cruise missile attack on Saudi oil facilities at Abqaiq and Khurais. The strike temporarily knocked out half of Saudi Arabia’s oil output, highlighting how traditional air defenses struggle against low-flying, small-profile threats (Reuters, 2019). More recently, in 2023 and 2024, Iranian proxy forces used similar tactics in Iraq and Syria, targeting U.S. installations with one-way attack drones. In January 2024, a drone strike on Tower 22 in Jordan killed three American soldiers and injured dozens more, highlighting the lethality of low-cost drone attacks when paired with accurate targeting intelligence and delayed attribution (Associated Press, 2024).

Israel, long experienced in drone warfare, faced a different type of challenge during the October 7, 2023, Hamas attack. Small drones were used to drop explosives on lookout towers and disrupt surveillance, effectively blinding defenses just before a coordinated ground assault (Washington Post, 2023). While these attacks were basic in execution compared to full-fledged swarming tactics, they underscored their value in shaping the battlefield and undermining enemy awareness.

China presents a more complex and long-term concern. As both a military power and the world’s top drone exporter, China influences the UAS space through sheer commercial and industrial reach (CSIS, 2025). Da-Jiang Innovations (DJI), a dominant player in the civilian drone market, produces devices that regularly turn up in global conflict zones, whether or not they are supplied directly by the Chinese state (Harrell & Moran, 2023). Meanwhile, the People’s Liberation Army (PLA) is rapidly advancing its drone capabilities, developing everything from stealth UAS and autonomous swarms to high-altitude endurance platforms. Military exercises in regions like Taiwan and the South China Sea now feature drones integrated with cyber and electronic warfare units, clear signs that UAS are a central part of China’s anti-access/area denial (A2/AD) strategy (Trévithick & Rogoway, 2025). U.S. officials have also voiced concerns about Chinese drones operating domestically, especially near critical infrastructure, where they could be used for espionage or to cause disruption during a crisis (Harrell & Moran, 2023).

Collectively, these conflicts highlight several trends that are directly relevant to U.S. domestic defense. First, adversaries are blending drones with civilian logistics to get them closer to high-value targets, a tactic that could easily be used against U.S. bases or infrastructure. Second, swarming attacks and sheer volume can overwhelm conventional defense systems, which are not built to fend off dozens of simultaneous, low-altitude threats. Third, the pace of innovation in everything from navigation to autonomy means that threat actors can adapt far faster than our current acquisition and development cycles can accommodate.

Most critically, the threat is not confined to distant battlefields anymore. Drones are mobile, scalable, and increasingly difficult to attribute. As Major General David Stewart, head of the Joint Counter-Small UAS Office, noted, “Conflicts in the Middle East and Ukraine have demonstrated how advances in hardware, software, and tactics have enhanced speed and range while making drones more autonomous, more easily acquired, and deadlier” (Stewart, 2025). The U.S. cannot afford to be reactive. It must study these global engagements carefully, internalize their lessons, and prepare accordingly before the wrong drone slips through American airspace either unnoticed or allowed to proceed unchallenged.

The Domestic UAS Threat Environment

Just as drones have reshaped warfare abroad, they are becoming an increasingly disruptive presence within the U.S. homeland. While the scale of domestic drone threats has not yet reached the intensity of conflict zones, the increasing frequency, sophistication, and intent of UAS activity within the U.S. signals a critical vulnerability. The U.S. is seeing more drone incursions, many of them more sophisticated and deliberate than casual hobbyist missteps (D-Fend Solutions, n.d.). From airspace violations by recreational users to criminal operations involving smuggling and surveillance, the evolving drone landscape is exposing real vulnerabilities in America's defenses. Currently, U.S. policies, legal authorities, and response strategies are struggling to keep pace with the threat.

Take the AFC Wild Card game on January 11, 2025, for example. A drone breached restricted airspace during the event, triggering emergency protocols (Ruiz, 2025). A representative interviewed from the Federal Bureau of Investigation (FBI) stated, "Despite [Federal Aviation Administration] FAA flight restrictions and active surveillance, response teams were caught in a bind. They had neither the authority nor the technical capacity to immediately act" (Anonymous FBI special agent, SME #2, personal communication, May 10, 2025). In the end, the drones left before any mitigation could occur (Ruiz, 2025). The situation made one thing clear: even well-defended venues are vulnerable when responsibility for drone defense is spread too thin across multiple agencies.

Similarly, there is the case of Wright-Patterson Air Force Base, one of the most strategically important military sites in the country. In December 2024, drones were spotted hovering near sensitive infrastructure, behaving in a way that strongly suggested reconnaissance missions, with drones pausing, loitering, and navigating with deliberate precision (Wright-Patterson Air Force Base, 2024). Yet, once again, legal restrictions tied the hands of base personnel. They could not engage or even retrieve the drones, leaving open troubling questions about surveillance and adversary intent (Anonymous FBI special agent, SME #2, personal communication, May 10, 2025). It is not hard to imagine how such loopholes could be exploited on a broader scale.

Border areas present another persistent challenge. U.S. Customs and Border Protection (CBP) has documented a rise in drone activity linked to transnational criminal organizations. These are not clueless or careless overflights; these drones are autonomously navigating routes, guiding smugglers, or dropping contraband deep into U.S. territory (U.S. Customs and Border Protection, 2023). In one case, drones were even caught conducting pattern-of-life surveillance on border agents' movements, tactics more often associated with intelligence services than drug cartels (FedScoop, 2024). Yet despite the frequency of these incursions, effective responses are rare. Gaps in drone detection coverage and a shortage of authorized C-UAS personnel leave many of these flights unchallenged.

Even when the drones are spotted, the absence of clear interagency protocols, standardized response measures, and real-time intelligence sharing often results in miscommunication or delayed action. One telling example occurred in June 2023 when an unauthorized drone caused a 30-minute ground stop at Pittsburgh International Airport (U.S. Government Accountability Office, 2024). The agencies involved had overlapping responsibilities but conflicting guidance on engagement. Local police could see the drone but lacked engagement authority, and Federal officials with mitigation tools were not immediately on site. As one industry expert put it bluntly, "Authority to engage a drone is often not available to the person who detects it" (Anonymous industry expert, SME #3, personal communication, June 5, 2025).

Taken together, these incidents are not anomalies, and they are early indicators of a larger, systemic vulnerability that points to a disturbing truth: the U.S. does not yet have a cohesive, actionable strategy for dealing with domestic drone threats. What exists instead is a patchwork of jurisdictions, muddled communication lines, and bureaucratic red tape. While such gaps may be manageable when the threat is minimal, they become critical as tactics like coordinated surveillance and critical infrastructure probing become more common and the consequences of inaction grow sharper.

As with foreign conflicts, the core issue is not a lack of technology. The U.S. has advanced detection systems, electronic jamming tools, and trained personnel. What is missing is a clear legal framework, timely decision-making authority, and the interagency muscle to act quickly and decisively. The next section will take a closer look at the policy bottlenecks behind this gap: how legal ambiguity, privacy concerns, and an outdated regulatory mindset are leaving the country exposed to a threat that is moving faster than the laws meant to contain it.

Policy, Legal, and Ethical Constraints

Despite growing concern over UAS activity inside U.S. borders, domestic policies governing drone detection, mitigation, and agency response remain largely fragmented, inconsistent, and outdated. While Department of Transportation (DOT) agencies like the FAA have made strides through initiatives like Remote ID, there is still no clear, unified framework for dealing with hostile or negligent drone use. Instead, a patchwork of legal statutes, siloed jurisdictions, and overly cautious guidance has left the U.S. struggling to mount a timely or coordinated defense against an increasingly complex threat.

At the heart of this challenge lies 6 U.S.C. §124n, the statute governing which federal agencies may conduct C-UAS operations. Currently, a limited set of DOJ and DHS components are directly authorized under this law: The FBI, CBP, U.S. Secret Service (USSS), Federal Protective Service (FPS), and U.S. Coast Guard (USCG) (U.S. Congress, 2018). The Department of Defense (DoD) and the Department of Energy (DOE) also have some authority, but only under very specific circumstances. Strikingly also constrained to either specific limited frameworks or strict support roles are agencies like the Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Transportation Security Administration (TSA), Federal Emergency Management Agency (FEMA), and State, Local, Tribal, and Territorial (SLTT) law enforcement, all of whom are on the front lines when it comes to protecting airports, stadiums, and public gatherings.

The TSA is a prime example of these statutory challenges. Despite being tasked with securing airports, which are among the most vulnerable to drone threats, the TSA currently lacks direct statutory authority to detect or mitigate UAS. Similar concerns apply to owners of critical infrastructure like power plants, ports, and stadiums. They cannot take defensive measures, even when drones are spotted flying overhead. As a DHS security expert put it, “It is alarming that our commercial airports remain unprotected from the threat of drones” (Anonymous senior DHS official, SME #1, personal communication, May 15, 2025). That disconnect between statutory authority and operational need is putting high-value targets at unnecessary risk.

Another particularly complex policy challenge arises when a UAS crosses from public or civilian-controlled airspace into restricted military airspace. While the FAA governs most national airspace, military installations are often surrounded by overlapping jurisdictional boundaries, including controlled airspace, special use airspace, and base-restricted zones, each with distinct rules for engagement and response. When a drone transitions between these zones, the authority to detect, track, or mitigate it can become unclear. For example, a drone loitering near a military base perimeter may initially fall under FAA or local law enforcement oversight. Once it crosses into a restricted military airspace, response responsibility shifts to the DoD, yet mitigation may still be constrained by legal, technical, or policy barriers, particularly if the system has not been formally declared hostile. This gray zone can delay action during time-sensitive incidents, especially when no pre-established protocols exist between DoD, DOT, and SLTT agencies for shared surveillance, threat assessment, or coordinated response. In practical terms, this means a drone could surveil or probe sensitive military infrastructure with little to no immediate consequence, simply by exploiting jurisdictional seams.

The problem does not stop at legal gaps. There is also a lack of standard operating procedures and interagency coordination. Unlike areas like counterterrorism or cybersecurity, C-UAS efforts still lack a central federal doctrine. Some DHS units engage in advanced training, including red team simulations, while others have virtually no UAS preparedness. SLTT agencies are in a similar bind. Budget constraints have limited federal support, and a lack of access to technology or intelligence has led to a patchy and inconsistent national response.

Civil liberties and privacy protections, while essential, also contribute to operational delays. The DHS often requires Secretary-level approval before deploying C-UAS tools, and a Privacy Impact Assessment (PIA) in many cases must be completed first. While these measures safeguard important rights, they also slow down responses, leaving room for bad actors to exploit the lag. Concerns over Fourth Amendment violations, data misuse, and liability often deter agencies from acting, even when the confirmed threat is present.

The FAA’s 2021 Remote ID rule aimed to bring some accountability by requiring most drones to broadcast their identity and location, but the system has gaps (U.S. Federal Aviation Administration, 2021). Drones lighter than 0.55 pounds are exempt, broadcast signals can be spoofed or shut off, and Remote ID offers awareness, not authority. Agencies still cannot act unless they are already authorized to do so. One expert summed it up: “If we are not fully

aware of everything in the airspace, we cannot effectively fulfill our roles as security partners" (Anonymous senior DHS official, SME #1, personal communication, May 15, 2025).

Tensions between law enforcement and homeland security objectives only add to the complexity. DHS might want to immediately neutralize a drone that appears threatening, while the DOJ may prefer to monitor it as part of an ongoing investigation. Without pre-agreed rules or shared legal frameworks, these differing priorities can delay action, often when there is no time to spare.

In the absence of a national C-UAS policy, some states have tried to fill the void, but this has led to a patchwork of state laws and local protocols that do not always align with federal standards (Anonymous senior DHS official, SME #1, personal communication, May 15, 2025). Without consistency, joint operations suffer. Agencies are often left guessing at risk thresholds and struggling to navigate conflicting regulations.

Adding to the mix is a general lack of enforcement. Many drone operators fail to comply with registration requirements, Remote ID broadcasting, or airspace rules, and rarely face consequences. One industry expert stated, "There are rarely repercussions for not following drone regulations" (Anonymous industry expert, SME #3, personal communication, June 5, 2025). That kind of environment only emboldens those looking to exploit the system.

At the end of the day, the issue is not a lack of technology or talent. The U.S. has both. The problem lies in legal barriers, institutional inertia, and a reactive mindset. If the country wants to stay ahead of the rapidly evolving UAS threat, it needs a national strategy that grants appropriate authorities, aligns agency goals, supports shared training and intelligence, and balances civil liberties with urgent operational needs. Without that, we risk falling further behind a threat that is not waiting for the law to catch up.

RECOMMENDATIONS

Improving Interagency Coordination and Information Sharing

As domestic drone threats become more frequent and sophisticated, it is increasingly clear that no single agency, military or civilian, can handle the challenge alone. This paper has already outlined how fragmented authorities and jurisdictional mismatches are hampering our collective ability to respond. Now, the focus shifts to solutions: how the U.S. can improve interagency coordination and information sharing by borrowing from the very playbook that is proven effective in foreign threat environments.

In active conflict zones, drone tactics can shift week to week. Staying ahead requires real-time coordination among services, commands, and international partners. There must be speedy intelligence flows, clearly defined roles, and the rapid conversion of threat observations into actionable training and doctrine. These principles can and should be scaled for domestic drone defense, with proper legal and policy safeguards in place.

Right now, the domestic C-UAS environment is reactive, fragmented, and heavily siloed. While there are federal working groups and some interagency coordination, there is no centralized system for managing UAS threat data, harmonizing response protocols, or designing joint mitigation strategies. That means similar drone incidents, such as a surveillance drone over a military base or energy facility, can yield entirely different responses depending on where they happen. Lessons learned in one city may never reach others in time to matter. Here is how we can start closing that gap:

1. Build Standardized, Threat-Informed Playbooks

One major hurdle in joint drone response is the lack of a shared playbook. Agencies often operate with different vocabularies, escalation protocols, and timelines, creating delays and confusion. Overseas, C-UAS units use structured response frameworks with risk escalation ladders, decision-making templates, and legal review processes all updated continuously based on threat intelligence.

Domestically, we should do the same. By creating civilian-adapted C-UAS response guides customized for DHS, DOT, DOJ, and SLTT partners, we could establish a shared lexicon, common detection thresholds, and clear rules of engagement. This guide would ensure faster, more consistent action, even when responses cross agency lines.

2. Expand Joint Training and Multi-Agency Exercises

Drone threats do not respect jurisdictional maps, and our training should not either. Using red teams and LVC simulations, we should conduct routine cross-agency exercises. These exercises should feature realistic threat profiles, multi-drone swarms, Global Positioning System (GPS) denial, Intelligence, Surveillance, and Reconnaissance (ISR) over infrastructure, and be designed to test communication, legal decision-making, and situational awareness under pressure.

3. Formalize Drone Threat Intelligence Sharing

Timely intelligence is the backbone of foreign drone defense, and a similar model could significantly strengthen domestic readiness. A formal civil and military UAS intelligence sharing system would:

- Consolidate incident reports from federal, state, and local agencies
- Identify patterns such as recurring flyovers, modified commercial drones, and platforms of foreign origin
- Distribute unclassified briefings to infrastructure operators and first responders
- Connect domestic incidents to broader geopolitical trends

This kind of system would not just support better decision-making; it would provide early warnings of gray-zone tactics that blur the lines between espionage, sabotage, and surveillance.

4. Invest in Interoperable Systems and Shared Technology Platforms

Coordination is only as good as the tools behind it. If agencies cannot share data or operate on compatible detection platforms, coordination breaks down. Interoperability has been a recurring challenge even in overseas operations, but when solutions are found, they should include both coalition partners and domestic counterparts. Sharing lessons learned in sensor fusion, network design, and platform integration will strengthen the entire national C-UAS architecture.

As the distinction between foreign and domestic drone activity continues to fade, our response must become more unified, agile, and anticipatory. The goal is not for the military to take over the domestic problem; it is to be a willing partner in building a national response capability that works across agencies, domains, and geographies.

By investing in coordination hubs, shared training events, standard response protocols, and real-time threat intel systems, we can make sure the next drone sighting, whether near a base, a refinery, or a concert, is not met with bureaucratic confusion, but with decisive, coordinated action.

Policy Improvements

The spread of UAS has introduced a fast-moving, asymmetric threat to national security that no longer respects the traditional lines between foreign combat zones and domestic airspace. As outlined throughout this paper, adversaries are increasingly using drones for surveillance, precision strikes, and infrastructure probing. While the DoD has made substantial progress in countering these threats abroad, the domestic landscape remains a patchwork. Domestic policies are outdated, authorities are limited, and operational readiness is uneven.

The task now is to bring the lessons learned overseas back home, not by copying military frameworks wholesale, but by strengthening an interagency network that is better prepared, more tightly connected, and adequately resourced to meet the evolving threat. To address the most urgent capability and coordination gaps, the following policy steps are recommended:

1. Expand Statutory C-UAS Authority

Congress should revise 6 U.S.C. §124n to extend C-UAS authorities beyond the current components. Key players like the TSA and vetted SLTT law enforcement agencies should be granted conditional powers to detect, track, and, where legally appropriate, neutralize drone threats. New authorities must come with strong oversight, clearly defined limits, and built-in privacy protections to maintain public trust.

A concrete example of how this could be accomplished includes adding a new subsection that authorizes additional federal and qualified SLTT entities to conduct limited C-UAS operations under a tiered authorization model. This model would establish three clear tiers of operational authority, subject to DHS and DOJ oversight:

- Tier 1 - Core Federal Entities (Full Authority):
  Retain full C-UAS detection and mitigation authority for the original components, plus explicitly include TSA. These agencies would operate under existing coordination and oversight mechanisms, with added reporting requirements to Congress.
- Tier 2 - SLTT Agencies (Conditional Authority):
  Grant qualified SLTT law enforcement agencies conditional C-UAS authority under DHS certifications. To qualify, agencies must:
  - Complete approved training and legal review
  - Operate under predefined airspace zones such as stadiums, government buildings, and special events
  - Use only approved and federally tested equipment
  - Submit incident reports to a central oversight body
- Tier 3 - Critical Infrastructure Partners (Passive Detection Only):
  Permit certified critical infrastructure operators to deploy passive detection technologies to detect UAS activity over or near their property. These entities must report threats to the DHS or FBI and are prohibited from engaging in active mitigation. DHS would serve as the central coordinating agency for response.

The amendment could also mandate the following safeguards:

- All deployments must comply with Privacy Impact Assessments (PIAs) and civil liberties audits.
- DHS, in consultation with DOJ and the Privacy and Civil Liberties Oversight Board (PCLOB), must issue implementation guidance detailing approved technologies, required training, data retention limits, and redress procedures.
- DHS would submit an annual report to Congress summarizing data, incident reviews, and policy violations.

2. Stand Up a National C-UAS Coordination Center

A dedicated national hub for C-UAS operations and planning is overdue. Modeled on proven examples like the National Counterterrorism Center (NCTC) or the National Cybersecurity and Communications Integration Center (NCCIC), this center would:

- Coordinate real-time incident responses
- Standardize training and doctrine
- Analyze threat intelligence
- Facilitate engagement across federal agencies, SLTT partners, and private sector stakeholders

By placing representatives from DoD, DHS, DOJ, DOT, and others under one roof, the U.S. can move toward a truly unified national strategy.

3. Invest in Regional C-UAS Test and Training Ranges

Congress and DHS should support the creation of regional test sites where agencies and infrastructure operators can conduct hands-on drone mitigation training. These facilities would enable:

- Live-fire and red team drills
- Technology integration testing under realistic conditions
- Iterative validation of protocols and communications

The DoD's experience in setting up such ranges at places like White Sands Missile Range (WSMR) and Yuma Proving Ground (YPG) can serve as a guide. Sharing red team tactics, scenario design, and lessons learned would multiply the value of each site.

4. Make Joint Training and Simulation Exercises Mandatory

Any federal agency receiving C-UAS related funding should be required to participate in multi-agency training exercises. These drills should include both live and virtual components and be designed to test legal coordination, threat recognition, and time-sensitive response under pressure. The DoD should assist by making available opposing force (OPFOR) resources, templates to keep scenarios relevant, and adversary behaviors authentic.

5. Establish a National Drone Intelligence Fusion System

To keep pace with fast-evolving drone tactics, the U.S. should stand up a civil and military intelligence fusion cell dedicated to UAS. This system would:

- Aggregate domestic and foreign drone threat reports
- Spot patterns in platform types, flight behaviors, or geographic targeting
- Push real-time alerts to SLTT agencies and infrastructure owners
- Feed into broader intelligence assessments, including gray-zone activity indicators

The goal is to detect and anticipate threats, not just react to them.

6. Define Interoperability and Detection Standards

Interagency cooperation will not work without shared technical ground. DHS and DoD, in collaboration with the National Institute of Standards and Technology (NIST), should define core standards for detection and mitigation systems. These should include:

- Minimum performance thresholds
- Data formatting and sharing protocols
- Unified communication alerts

Such standards would ensure that local investments in tech can plug seamlessly into national networks, improving coordination and overall situational awareness.

7. Prioritize Base Defense for Domestic Installations

While overseas bases benefit from layered C-UAS defenses, many U.S. installations on the home front remain exposed. This discrepancy needs to change. DoD, in partnership with Congress, should accelerate efforts to:

- Install advanced drone detection and countermeasures at high-risk domestic bases
- Incorporate drone threats into regular force protection exercises
- Foster direct coordination with local law enforcement for off-base incident tracking
- Ensure that base commanders have timely access to up-to-date intelligence on evolving drone tactics

Enhancing Domestic C-UAS Testing and Training Through the Threat Lens

Over the past decade, the DoD has learned how to confront the rising threat posed by drones on the battlefield. What began as a scattered nuisance has quickly evolved into a strategically potent challenge, employed by both peer competitors and rogue actors across the globe. In combat zones ranging from Ukraine and Iraq to the Indo-Pacific, DoD has built a responsive framework: one that combines real-time threat intelligence with evolving doctrine, hands-on training, and a cycle of field experimentation. These lessons, hard won in dynamic conflict environments, now offer a roadmap for strengthening the nation’s domestic C-UAS posture.

Crucially, this is not about militarizing civil defense. Rather, it is about national security partners, civilian and military, collaborating to confront a fast-moving threat that does not respect geographic or institutional boundaries.

One of DoD's most powerful tools is its ability to translate battlefield intelligence into operational readiness, almost in real time. Units facing drone threats abroad, ranging from surveillance overflights to loitering munitions and coordinated swarm attacks, feed their experiences back to strategic planners. That information fuels rapid updates to tactics, training protocols, and acquisition strategies. It also gets injected into live exercises, red-teaming efforts, and wargaming scenarios that do not just prepare for yesterday's fight but anticipate tomorrow's.

That same agility built on real-world data can and should be applied at home. Agencies like DHS, DOJ, and the DOT, along with state and local partners, are already seeing an uptick in drone activity near sensitive sites. While many of these encounters seem benign on the surface, patterns like low-observable routing, spoofed IDs, and autonomous navigation suggest more deliberate probing. These behaviors align with early indicators observed in foreign conflicts. If we want to stay ahead of the curve, the time to connect those dots is now. There are several practical ways the DoD should help bridge the training and readiness gap nationwide:

1. Share Threat-Informed Training Models

The DoD's use of LVC environments allows it to run sophisticated, repeatable scenarios simulating drone incursions, swarms, and electronic warfare. These stress tests could cover everything from communication breakdowns to legal ambiguity. By partnering with agencies like the ATF, FEMA, and TSA, the DoD could help tailor these LVC models to domestic security missions. Injecting drone response into existing fusion center training or emergency exercises would make an immediate impact without having to reinvent the training pipeline.

2. Expand Access to Test Ranges and Red Teaming

The military already maintains secure test sites, like WSMR and YPG, where drones can be tested and countered in realistic conditions. Opening these facilities even periodically to SLTT agencies would give civilian partners the rare chance to run live drills and validate defense strategies. Similarly, DoD's red teams, which mimic adversary drone behavior using both military and commercial gear, would play a crucial role in building out civilian training teams.

3. Assist in Keeping Pace with Technological Evolution

Adversaries are rapidly enhancing UAS capabilities using commercial off-the-shelf (COTS) components and open-source software, outpacing traditional technological cycles. Domestic agencies must counter a wide range of threats, from single hobbyist drones to coordinated swarms, yet current C-UAS efforts often target singular threats like DJI, leaving responders unprepared for complex scenarios. Inconsistent training curricula and limited access to realistic UAS environments further hinder preparedness. DoD and domestic agencies must share technologies and insights with little impediment to shift from static, one-size-fits-all training to dynamic, threat-informed programs that match adversary innovation.

4. Support Interagency Doctrine and Exercise Design

As drone threats become more complex, the lack of a standardized domestic C-UAS doctrine is becoming a liability. DoD's experience managing layered defenses, coordinating shared airspace, and navigating joint response frameworks can help guide this process. By contributing to national exercises like Eagle Horizon or Cyber Storm, DoD could inject realistic drone scenarios that test interagency coordination and reveal gaps in authority or readiness before a real incident occurs (U.S. Department of Transportation, 2009).

5. Promote Shared Threat Tracking and Lessons Learned

The DoD's rapid adaptation to drone threats stems from its centralized approach to monitoring and analyzing UAS activities. The Joint Counter-Small UAS Office (JCO) collects battlefield data and pushes insights back into training and procurement cycles. Creating a similar civil and military fusion node jointly run by DHS and intelligence agencies could allow early warning trends, platform sightings, and threat patterns to be shared across jurisdictions. This kind of insight is especially important as adversaries use commercial drones for both foreign and domestic operations.

6. Institutionalize LVC and Simulation Training for Homeland Agencies

Simulation-based training is a cost-effective, scalable way to prepare for drone threats, especially when live testing is not feasible. DoD should help build out modular simulation tools that allow agencies to practice swarm attacks, GPS denial, or airspace deconfliction in safe, repeatable environments. Smaller or resource-constrained jurisdictions could participate in national drills via virtual injects, fostering a shared understanding of threat dynamics and response tactics.

Nonetheless, the DoD is not merely a provider of support but also a beneficiary of domestic drone intelligence. The military can also derive strategic benefit from analyzing domestic drone incidents. When unknown UAS platforms hover over U.S. bases or loiter near critical energy infrastructure, those events may provide early clues about adversary reconnaissance strategies. Domestic intelligence on drone misuse, when properly integrated, can sharpen DoD's global threat picture. These relationships benefit from being two-way streets and demand a closer, real-time partnership. The drone threat is not just a military or law enforcement problem. It is a national challenge and meeting it will require more than new equipment or policies. It demands coordination, agility, and above all, a shared commitment to readiness.

By connecting battlefield insights with domestic preparedness, we can create a unified, forward-looking defense posture, one capable of neutralizing emerging drone threats with speed, precision, and collective resolve.

CONCLUSION

Future Outlook

Looking ahead, the domestic drone threat is not just here to stay; it is poised to get more complex. Both state-sponsored adversaries and independent actors are watching recent conflicts closely and adapting fast. They are learning to evade radar, operate in GPS-denied environments, and exploit legal and bureaucratic gaps in our national security posture. With the growing availability of long-range FPV drones, autonomous flight capabilities, and swarming software that can be bought off the shelf, the challenges we face will only deepen. At the same time, legitimate commercial and recreational drone use will continue to grow and underscore the importance of striking the right balance between protecting security and preserving civil liberties.

The DoD must take an active, supportive role in helping civilian agencies stay ahead of emerging threats. DoD brings decades of experience in red teaming, real-time threat simulation, and intelligence fusion capabilities that would be a force multiplier in the domestic space, without crossing jurisdictional lines. Its work in training, testing, and LVC-based preparation offers a proven model for scalable, scenario-rich exercises that could benefit partners across DHS, DOJ, DOT, and local jurisdictions.

What is needed now is a shift from reactive enforcement to proactive readiness. That means going beyond simply expanding legal authority. It means embedding a national cycle of preparedness in which detection systems are regularly tested, response timelines rehearsed, and threat data is disseminated securely and rapidly across all relevant agencies.

The good news is that we are not starting from scratch. The core components already exist, which are battle-tested tactics, next-generation sensors, powerful simulation platforms, live threat capabilities, and a community of dedicated stakeholders. What we need is the glue, a deliberate, well-funded, and coordinated effort to bring it all together into a truly national capability.

Congress, the DoD, DHS, DOT, and DOJ must unite with urgency, cooperation, and foresight to meet the domestic C-UAS challenge and prepare how we fight, or risk fighting unprepared.

ACKNOWLEDGEMENTS

The author would like to thank the FBI Hazardous Devices School, the DHS C-UAS Program Management Office, and the industry subject matter expert who generously contributed their time and insight. Their perspectives and operational experience were invaluable in shaping the analysis and recommendations presented in this paper.

DISCLAIMER

The views expressed in this paper are those of the author and do not necessarily reflect the official policy or position of the Department of Defense, the Department of Homeland Security, the Federal Bureau of Investigation, or any other U.S. government agency. Reference to any specific product, process, or service does not constitute or imply endorsement by the U.S. Government. Any interviews or personal communications cited are included with the permission of the individuals involved and reflect their personal opinions, not official agency positions.

REFERENCES

Associated Press. (2024, January 28). *Drone strike kills three U.S. soldiers in Jordan* [AP News]. https://apnews.com/article/us-jordan-drone-attack-iran-tower-22-israel-hamas-war-0265beed527e3009a966c0531c08838e

Center for Strategic and International Studies. (2025, May 28). *The Russia–Ukraine drone war: Innovation on the frontlines and beyond*. CSIS.

Center for European Policy Analysis. (2023). *Ukraine's secret weapon: Artificial Intelligence*. CEPA.

D-Fend Solutions. (n.d.). *Drone incident tracker*. https://d-fendsolutions.com/drone-incident-tracker/

FedScoop. (2024). *Federal law enforcement officials make the case for expanded drone laws*. Retrieved from https://fedscoop.com/fbi-doj-customs-border-drone-laws/

Guardian. (2025, June 2). *Operation Spiderweb: a visual guide to Ukraine's destruction of Russian aircraft*. Guardian.

Harrell, B., & Moran, T. (2023, March 23). *The pressing threat of Chinese-made drones flying above U.S. critical infrastructure*. CyberScoop.

McGee, L. (2024, February 28). *The future of warfare: A $400 army drone took out a $2M tank*. Politico. https://www.politico.eu/article/future-warfare-400-army-strike-drone-unit-2m-tank/

Reuters. (2019, September 14). *Attacks on Saudi oil facilities knock out half the Kingdom's supply*. Reuters.

Reuters. (2025, June 4). *How Ukraine pulled off an audacious drone attack deep inside Russia*. Reuters.

Ruiz, N. (2025, January 11). *Drone pauses Ravens-Steelers game*. The Baltimore Banner. https://www.thebaltimorebanner.com/sports/ravens-nfl/drone-pauses-ravens-steelers-game-MMBTODX2SBC4ZMNMEXGSA35SGQ/

Stewart, D. F. (2025, May 1). Statement before the Subcommittee on Tactical Air and Land Forces, Committee on Armed Services, U.S. House of Representatives, 119th Congress, 1st session.

Trévithick, J., & Rogoway, T. (2025, February 25). *China's massive WZ-9 'Divine Eagle' drone now operating from South China Sea base*. The War Zone.

U.S. Congress. (2018). *Preventing Emerging Threats Act of 2018, 6 U.S.C. §124n*. https://www.congress.gov

U.S. Customs and Border Protection. (2023, March 1). *Human smugglers now using drones to surveil USBP*. U.S. Department of Homeland Security. https://www.cbp.gov/newsroom/local-media-release/human-smugglers-now-using-drones-surveil-usbp

U.S. Department of Transportation. (2009). *Training and exercises, US – English*. https://www.transportation.gov/sites/dot.gov/files/docs/2%20-%20Training%20and%20Exercises%20US%20-%20English.pdf

U.S. Federal Aviation Administration. (2021). *Remote Identification of Unmanned Aircraft Rule. Federal Register, 2020-28948 (86 FR 4390)*. https://www.federalregister.gov/documents/2021/01/15/2020-28948/remote-identification-of-unmanned-aircraft

U.S. Government Accountability Office. (2024, June 27). *Drones take flight, so do concerns about safety*. https://www.gao.gov/blog/drones-take-flight-so-do-concerns-about-safety

War on the Rocks. (2024). *Drones are transforming the battlefield in Ukraine but in an evolutionary fashion*. War on the Rocks.

Washington Post. (2023). *Small drone strikes during Hamas attack on Israel*. Washington Post.

Wright-Patterson Air Force Base. (2024, December 17). *Wright-Patt airspace experiences additional drone incursions*. https://www.wpafb.af.mil/News/Article-Display/Article/4015684/wright-patt-airspace-experiences-additional-drone-incursions/