FPRI
FOREIGN POLICY RESEARCH INSTITUTE

SMALL DRONES, BIG PROBLEMS

Managing the Unmanned Threat to the Homeland

DR. AARON STEIN LTC (RET) TIM BALL

This publication was sponsored by the Homeland Defense Institute.
The views expressed in this publication do not necessarily represent the views of the United States Air Force Academy, North American Aerospace Defense Command and United States Northern Command, the Department of Defense, or the United States Government.

The views expressed in this report are those of the author alone and do not necessarily reflect the position of the Foreign Policy Research Institute, a non-partisan organization that seeks to publish well-argued, policy-oriented articles on American foreign policy and national security priorities.

May 2025

FPRI

FOREIGN POLICY RESEARCH INSTITUTE

Small Drones, Big Problems:

Managing the Unmanned Threat to the Homeland

Dr. Aaron Stein

LTC (Retired) Tim Ball

Table of Contents

About the Authors

Dr. Aaron Stein is the President of the Foreign Policy Research Institute (FPRI). Dr. Stein most recently served as the Chief Content Officer at War on the Rocks/Metamorphic Media, where he led the company's editorial strategy and hosted the War on the Rocks podcast. Previously he served as FPRI's Director of Research from 2020-2022, and Director of its Middle East Program from 2019-2022. Prior to joining FPRI, Dr. Stein was a resident senior fellow of the Atlantic Council and held fellowships at the Geneva Center for Security Policy (Switzerland), Royal United Services Institute (London), and the Center for Economics and Foreign Policy Studies (Istanbul). Dr. Stein holds a BA in politics from the University of San Francisco and an MA in international policy studies with a specialization in nonproliferation from the Middlebury Institute of International Studies at Monterey. Dr. Stein received his PhD in Middle East and Mediterranean studies at Kings College, London. He is the author of *The US War Against ISIS: How America and its Allies Defeated the Caliphate* (Bloomsbury, 2021) and *Turkey's New Foreign Policy: Davutoglu, the AKP, and the Pursuit of Regional Order* (Routledge, 2015). His commentary has been published in *Foreign Affairs, Survival, RUSI Journal, War on the Rocks*, and *The American Interest*. He also co-hosts the Arms Control Wonk podcast, a leading series on arms control, disarmament, and non-proliferation.

Tim Ball, Lieutenant Colonel, United States Army (Retired) is a Non-Resident Fellow in the National Security Program at the Foreign Policy Research Institute and a retired US Army Special Forces officer. He served as a detachment and company commander in 10th Special Forces Group (Airborne), with multiple tours in Iraq, and assignments throughout Europe, to include NATO Special Operations Headquarters. His research interests include the use of special operations forces and military advising. LTC Ball retired after serving as the Professor of Military Science at the University of Texas at San Antonio Army ROTC program. He holds a BA in Political Science from Texas A&M University and an MS in Defense Analysis (Irregular Warfare) from the Naval Postgraduate School in Monterey.

There is perhaps no better example of the rapidly evolving strategic environment than the emergence of small unmanned aerial systems (sUAS) as a threat to infrastructure and personnel in the homeland. The availability and utility of small drones has grown exponentially over the last decade, and some have repeatedly employed these systems for illicit purposes.

While US and coalition forces overseas have faced the threat of weaponized unmanned systems for years, small drones have emerged as a significant risk to infrastructure and safety in the United States in a relatively short period of time. The widespread availability of small drones, coupled with a complicated regulatory structure and limitations on UAS countermeasures based on concerns for flight safety and privacy, has created significant vulnerabilities that have been exploited by known and unknown actors.

— Gen. Gregory M. Guillot, Commander, United States Northern Command, Statement to Senate Armed Services

Executive Summary

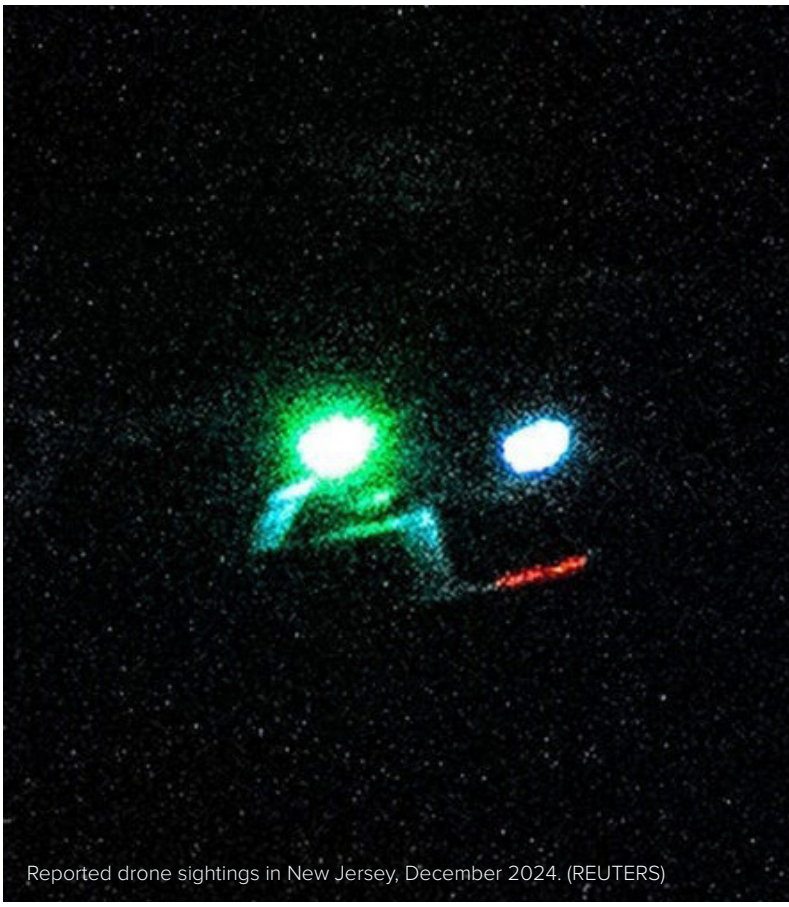
Drones are everywhere.

From the battlefields of Ukraine to the suburbs of New Jersey, it has become increasingly common to find small unmanned aerial systems (sUAS) in the sky. In the United States, there are now over one million lawfully registered sUAS platforms. The proliferation of sUAS in the civilian population has created a flood of reporting to law enforcement agencies across a variety of scenarios. Quite often, a civilian hobbyist simply flies their sUAS "too close to the sun" and encroaches upon restricted airspace around either civilian or military critical infrastructure. However, there have also been cases of foreign actors operating sUAS in an attempt to reconnoiter specific targets or locations.

There are now so many sUAS incidents occurring that it makes for an easily exploitable environment for malign activities by state or non-state actors. Making things even more dangerous, our research shows that quite often, no one knows who to call when a sUAS incident occurs. While officially the Federal Aviation Administration (FAA) has primacy over sUAS incidents, our research (and the FAA's own database) shows that local law enforcement is often contacted after sUAS incidents, and cases are often closed as soon as they are opened, without confirmed reporting to the FAA. As a result, Department of Defense (DoD) entities charged with homeland defense, such as US Northern Command (NORTHCOM), are often left without knowledge of sUAS incidents, and cannot observe and monitor trends adequately to support development of adequate countermeasures. They also do not have the authorities to counteract the threat, even when sUAS activity upends military training exercises. To mitigate this threat, the US government should consider:

- Establishing a Joint Interagency Task Force (JIATF)
- Maintaining a single, consolidated reporting database for any sUAS activity over critical infrastructure on an unclassified network.
- Mandating NORTHCOM to lead DoD efforts within this new JIATF and work with Congress on updated legislation to codify proper authorities for US agencies and the military to thwart UAS intrusions.

Introduction


Reported drone sightings in New Jersey, December 2024. (REUTERS)

Drones are everywhere.

From the battlefields of Ukraine to the suburbs of New Jersey[2], it has become increasingly common to find small unmanned aerial systems (sUAS) in the sky. In the United States, there are now over one million lawfully registered sUAS platforms.[3] The proliferation of sUAS in the civilian population has created a flood of reporting to law enforcement agencies across a variety of scenarios. Quite often, a civilian hobbyist simply flies their sUAS "too close to the sun" and encroaches upon restricted airspace around either civilian or military critical infrastructure. However, there have also been cases of foreign actors operating sUAS in an attempt to reconnoiter specific targets or locations.

This report conducted research into the number of reported sUAS incidents over or against both civilian and military critical infrastructure in the United States. While findings resulted primarily in reports from commercial airline pilots spotting sUAS around airports, they also point to a more complex vulnerability. There are now so many sUAS incidents occurring that it makes for an easily exploitable environment for malign activities by state or non-state actors. Making things even more dangerous, our research shows that quite often, no one knows who to call when a sUAS incident occurs. While officially the FAA has primacy over sUAS incidents, our research (and the FAA's own database[4]) shows that local law enforcement is often contacted after sUAS incidents, and cases are often closed as soon as they are opened, without confirmed reporting to the FAA.

As a result, DoD entities charged with homeland defense, such as NORTHCOM, are often left without knowledge of UAS incidents, and cannot observe and monitor trends adequately to support development of adequate countermeasures. The report notes these deficiencies and makes specific policy recommendations in order to increase support to NORTHCOM in its counter-sUAS efforts across the continental United States.

We believe that the following recommendations can help address the sUAS threat to civilian aviation, but also to empower the US government to counteract what appears to be a foreign-sponsored campaign to monitor military infrastructure and exercises:

1. Amidst ongoing cuts in both personnel and budgets at numerous federal agencies, interagency coordination efforts for counter-sUAS activities can be expected to get worse, not better.

2. In order to synchronize efforts across the whole of government, we recommend establishing a Joint Interagency Task Force (JIATF) tasked with not only recording sUAS incidents around critical infrastructure, but also developing a strategy for coordinated response between various government entities.

3. The JIATF should establish a single, consolidated reporting database for any sUAS activity over critical infrastructure. This database should be maintained on an unclassified network in order to maximize the opportunity for local, state, and federal entities to utilize the data.

4. NORTHCOM should lead DoD efforts within this new JIATF.

5. NORTHCOM should also leverage DoD congressional liaisons in order to codify DoD's role in countering sUAS activity in the continental United States. This role needs to be properly defined in context of what DoD is responsible for around non-DoD facilities and infrastructure, as well as updating DoD's authorities to counter sUAS activity near or over DoD facilities and infrastructure.

6. Specific operations like the southern border mission also require specific authorities. Congress needs to grant NORTHCOM expanded authorities to counter sUAS activity along the southern border.

Methodology

This study sought to examine the threat of sUAS to critical infrastructure within the continental United States (CONUS). To do so, the authors initially set out to assemble a database that captured sUAS incidents around critical infrastructure. In order to define critical infrastructure, the authors looked at multiple sources, to include Joint Publication 3-27's definition of defense critical infrastructure: "Department of Defense and non-Department of Defense networked assets and facilities essential to project, support, and sustain military forces and operations worldwide."[5] For the purpose of this study, the authors established four categories for critical infrastructure, while also acknowledging that these four categories do not capture every CONUS-based asset or facility that meets JP 3-27's definition. The four categories of critical infrastructure the authors utilized for this study included:

1. **Airports**
2. **Seaports**
3. **Key Rail Heads**
4. **DoD / Military Installations**

Five research questions were also established for this study:

1. **How have actors or governments used sUAS for attacks on critical infrastructure?**
2. **Do these attacks on infrastructure have similarities?**
3. **Do these attacks on infrastructure have critical differences?**
4. **What lessons can be learned?**
5. **What policy recommendations to protect infrastructure should be considered?**

While "attacks" is used in three of the research questions, it should be noted that this is not limited to kinetic actions against a target. The authors looked at incidents suspected of being used for close target reconnaissance of critical infrastructure, or even probing incidents meant to test response systems to the presence of sUAS near critical infrastructure.

To conduct our research into sUAS incidents around critical infrastructure, the authors began by utilizing open source media reporting platforms, such as Google Scholar and Lexis Nexis. Additionally, the authors looked at the FAA's own unclassified database of "drone sightings near airports," which proved to be even more thorough than open source media reporting. As research progressed, multiple issues emerged:

1. **Numerous examples of sUAS incidents reported but not recorded.**
2. **An average of nearly 400 sUAS incidents per fiscal quarter occurring around airports, captured in the FAA's database.**
3. **The majority of these FAA database entries have nothing beyond initial report and show that the incidents were often reported to a range of law enforcement agencies, with no**

continuity in who the reports went to within local, state, or federal government agencies.

4. **During discussions with the Force Protection division at US Army North, the authors were told a database for sUAS incidents around defense critical infrastructure already exists, but is maintained on a classified DoD network. This eliminated the authors' ability to cross-reference what is available through open source reporting and what DoD is actually tracking in their own database. It remains unclear to the authors as to whether interagency partners have access to this database, or if it is meant only for Force Protection planners.**

Reviewing available data allowed the authors to draw an easy conclusion: The overwhelming majority of incidents are accidents or innocuous events, with most incidents taking place near airports, and there is less reporting on sUAS incidents around other critical infrastructure.[6] This does not mean a lack of incidents occurring around DoD infrastructure, but because DoD maintains its data on classified networks, a thorough review of these incidents was not possible for the authors. Additionally, the overemphasis on airports is likely associated with the FAA serving as the primary agency tasked with the sUAS problem set. The news also tends to report more often on incidents around airports, less because they occurred at all and more because they typically cause significant disruptions in commercial air travel, especially when the incident occurs at a major "hub" like New Jersey, Atlanta, or Chicago.

Faced with these problems in the reporting and recording of sUAS incidents, the authors shifted focus of their research and attempted to analyze sUAS incidents that were attributable to a malign actor, or incidents in which a malign actor was suspected. This expanded some of the research to include sUAS incidents that occurred overseas around US military facilities or assets. This expansion allowed the authors to not only analyze sUAS incidents that were clearly conducted by a malign actor, but also to provide analysis on how the proliferation of sUAS platforms in the United States now provides an exploitable environment for malign actors seeking to conduct close target reconnaissance, or potentially even kinetic attacks against critical infrastructure.

Research and Findings

The data reveals two very straightforward trends. The first is that the majority of sUAS incidents are caused by hobbyists. The incidents are dangerous, especially when a sUAS overflies an airport, but the motive is innocuous. The frequency of these events does suggest more needs to be done to prevent overflight of airports. The FAA has definitive authority over these incidents and more efforts should be made to prevent the overflight of civilian airports to decrease the risk of a catastrophic accident.

The second, more ominous trend, is that there are clear indications that foreign actors are using sUAS — and even larger systems — to perform close target reconnaissance of US military platforms during small and large force exercises. This campaign is enabled by the lack of authorities to counteract flight operations and the "stove-piped" set of regulations and authorities that regulate sUAS flights in the United States.

ENTHUSIAST ACCIDENTS

The data the authors collected and reviewed reveals that the majority of all UAS incidents over the past year documented were accidents. The FAA's data begins in October 2019 and records every reported incident over each fiscal quarter. Reviewing this data showed that on average, there are between 375–400 sUAS incidents around airports each quarter. Recorded incidents generally follow the same pattern: A hobbyist flew a sUAS into an area, the DJI type drone[7] was spotted, and action was then taken to prevent an accident. The most common incident took place near an airport, where the risk of a sUAS colliding with a passenger jet was considerable. The findings reveal that there is no set procedure for how to deal with these overflights and how to deal with both the sUAS and the sUAS operator.[8]

The FAA's primary mechanism to prevent this overflight is with legislation allowing for the sUAS to be tracked via registration and to regulate where and how they fly.[9] For example, after a series of sUAS sightings in New Jersey and New York in late 2024,

Drone ready for flight at the New York UAS Test Site, Griffiss International Airport. (NUAIR).

the FAA and Gov. Kathy Hochul imposed temporary flight restrictions.[10] The sightings caused mild panic amongst the general public, underscoring how a state actor could use simple tools to upend civilian flights and cause local panic about the origin and nature of sUAS flights in populated areas.

The issue, of course, is how to enforce no-flight restrictions. The enforcement of such a ban is often split between federal, state, and local governments, each with a different set of tools and experience to deal with the issue. The inability to enforce such a ban is a particular problem for flights near and over military installations. Our data revealed a separate — and more troubling — set of incidents that point to a sustained foreign-actor led campaign to monitor US military exercises. The incidents underscore the vulnerability of US military facilities to espionage, given the lack of legal authorities given to halt these overflights.

THE CAMPAIGN

The more concerning trend are the events that we coded as linked to foreign actors, or where reporting clearly suggests a foreign actor is involved in sUAS-related events. It is increasingly clear that the People's Republic of China is using sUAS, both commercially purchased and purpose-built systems, to conduct close target reconnaissance in the United States. These incidents take place in very well-known training areas for the US Air Force and Navy — and together suggest that China is conducting an open campaign to collect and exploit US military technology.

Three incidents have been widely reported and underscore the scope of the problem. In 2019, Navy destroyers participating in an exercise near the California channel islands were shadowed by sUAS. The incident took place over two-nights and involved multiple AEGIS destroyers exercising near San Clemente island in US coastal waters just off California. The investigation reveals the challenges the United States has in both attributing drones to a state actor and having the means to investigate encounters after they take place. The sUAS in the 2019 incident also do not share much in common with commercial DJI-origin drones available on the market for purchase. The sUAS operated very closely to the ships, over successive nights, and were able to loiter for far longer than commercial batteries typically allow. The sUAS were also able to keep up with the ships and, despite the investigations, returned to shadow two different ships 10 days later. The reports suggest that these sUAS were flown by state actors, presumably on behalf of the

Phantom 3 4K drone in flight. (Suyash Dwivedi/Wikimedia)

Chinese government, and is suggestive of a broader trend: China is using sUAS to monitor American military exercises and, in certain cases, to test certain technology against US military platforms.[11]

An example of this type of activity over CONUS-based critical infrastructure can be seen in an incident that took place over 17 days along the east coast of the United States. The mix of UAS used during these incidents differed considerably from the events with the Navy in 2019. Langley Air Force Base was overflown by large UAS — estimated to be at least 20 feet long in certain cases — that had seemingly unfettered overflight access

to the US Air Force's Tactical Command. The events would start shortly after sunset and continue for hours until just before midnight. The sUAS would reportedly fly in formation, with larger faster drones overflying the base, only for smaller quadcopter-type sUAS to hover beneath them, presumably to collect intelligence. The incidents over Langley were part of a larger pattern of suspicious UAS activity. There were similar UAS overflights near Edwards Air Force Base in California, as well as over US nuclear test facilities in Nevada.[12]

While the scope of this project was initially limited to incidents in CONUS, two specific incidents that occurred at military bases abroad are worth mentioning. This is not only due to their similarities to CONUS-based incidents, but also because these incidents occurred at bases with significant US presence, and they are further indicators of intentional, foreign-led reconnaissance of US assets utilizing sUAS platforms.

At RAF Lakenheath and RAF Mildenhall in November 2024, two British air bases where the US Air Force has significant presence, similar UAS incursions occurred in November 2024. The incident raised concerns that Russia was using sUAS to threaten critical infrastructure, although that was never confirmed. The incursions took place over several days, but the open source details remain sparse. The incident reportedly included several different types of UAS and, according to The War Zone, may have prompted US Air Force F-15s to launch to investigate the incursion. The pattern is suggestive, given the similarity to the UAS

Researchers carrying an small unmanned aerial system, or sUAS, out to the launch area of the City Environment Range Testing for Autonomous Integrated Navigation Hampton, Virginia. (NASA)

incidents over Langley and in California.[13]

A similar incident occurred at Ramstein in Germany in December 2024. A number of sUAS were reported over both Ramstein Air Base and the German arms manufacturer Rheinmetall and chemical firm BASF,[14] a pattern reminiscent of UAS events in CONUS.

That same year, several more CONUS-based incidents occurred that continue to point toward a foreign-sponsored campaign. In an incident similar to the California channel islands events, a large "helicopter like UAS" was spotted near Virginia Beach and Naval Air Station Oceana. Small UAS were

Reported drone sightings in New Jersey, December 2024. (REUTERS)

also recorded over Randolph Air Base in December 2024, prompting speculation that the small craft were tasked with monitoring the military installation. Finally, at Vandenberg Air Force Base in California in December 2024, on the day of a planned launch of multiple National Reconnaissance Organization satellites, a Chinese national was arrested for flying a sUAS over the base. The goal, it appears, was to monitor the launch.

Our research revealed more incidents, either directly linked to a state actor or that we coded as "unknown" given the paucity of information in open sources. However, in the incidents that we coded as unknown, there is ample circumstantial evidence to suggest a foreign actor may have been involved. For example, there was an incident near Hill Air Force Base where UAS were reported by locals in December 2024, but which did not prompt any closure to the base.[15] In Dayton that same month, at Wright-Patterson Air Base, a number of sUAS, reportedly differing in size, forced base officials to close the airspace for about four hours.[16] The spike in reports came in December, when the UAS issue in New Jersey and New York prompted national concern about a foreign actor operating small drones in US airspace.

In each of these incidents, response options from the US military were limited by murky legalities, and unclear authorities. The US military does not have explicit authorization to shoot down sUAS when a commander deems it necessary, outside of a clear self-defense scenario. The use of non-kinetic means of deterrence requires deconfliction with the FAA and to ensure that any action does not interfere with commercial aviation. The Langley Air Force Base incident is a good example of the challenges that arise when attempting to counter sUAS over American soil. According to the Wall Street Journal, various non-kinetic means were considered to disable the drones, including jamming and directed energy weapons. All were ruled out. In the case of the jamming discussion, the concern was that such an effort would disable 911 services and local wifi. In the case of directed energy, "such a weapon carried too high a risk for commercial aircraft." The military, it appears, also had issues with tracking the slow-flying drones, presumably because assumptions about the speed and size of intruding aircraft dictated the type of detection equipment installed on the base.[17]

Findings

The majority of UAS incidents captured in our database are dangerous for commercial aviation, but largely innocuous in intent. The operator is almost certain to be an enthusiast or avid hobbyist, keen to take overhead images of commercial aviation operations. The risk is a catastrophic accident, similar in scope to the recent collision of a UH-60 Black Hawk and a passenger plane on final approach.[18] While a sUAS is obviously smaller than the Black Hawk helicopter, the risk is that a quadcopter-type drone would be ingested by an engine, leading to a catastrophic accident. The other pool of incidents are far more likely, specifically that a drone sighting near or over an airport halts air traffic and delays inbound and outbound flights.

The more ominous finding is that there is an undeniable foreign-sponsored led campaign to use a variety of different UAS to monitor US military exercises throughout the country. The incidents range from the simple, a foreign-born operator flying a DJI-type sUAS near or around US military facilities, to far more sophisticated sets of aircraft are also being used. This was certainly the case in southern California with the Navy and along the East Coast over both Naval and Air Force facilities. According to one of the authors' interviews with US Air Force personnel, these more sophisticated UAS were omni-present for a period of time during all types of exercises.[19] This private revelation is certainly reflected in the public data, but not all events are captured.

The frequency of these encounters is suggestive of a two-pronged strategy.

The first is that a state sponsor can easily "hide in the noise" of the frequent sUAS encounters near dual-use airports, which often host both national guard and civilian aircraft. This may explain why there was a spike in incidents in December 2024, which coincided with the broader public panic over sUAS sightings in New Jersey. The majority of those sightings were hysteria-driven false reports, but buried within the data is a similar spike in reports of sUAS incidents near US military infrastructure. This could simply be a false correlation, or reporters are simply paying more attention to incidents that now happen routinely. In any case, the spike in events underscores the severity of the problem. A "hide in the noise" approach is a classic strategy and one which we believe is worthy of further study.

The second, and more straightforward prong, is that a foreign actor is violating military airspace simply because they can, and to continue to test the response mechanisms of the United States to such incursions. There have, as of now, been few consequences for these actions. The lack of consequences stem, largely, from a confusing set of regulatory agencies, serious restrictions on enforcement of no-fly areas, and the need to empower government entities to address this growing issue.

Recommendations

1. Establish a Joint Interagency Task Force (JIATF)

Amidst ongoing cuts in both personnel and budgets at numerous federal agencies, interagency coordination efforts for counter-sUAS activities can be expected to get worse, not better. The "whole of government" approach to problems only works if there is a forcing function established that places all relevant agencies in the same room, with clearly defined roles and responsibilities. Currently, that forcing function seems to be missing from the counter-sUAS mission that so many different government agencies are trying to execute.

In order to synchronize efforts across the whole of government, we recommend establishing a Joint Interagency Task Force (JIATF) tasked with not only recording sUAS incidents around critical infrastructure, but also developing a strategy for coordinated response between various government entities. This JIATF should consist of elements from the Departments of Defense, Justice, Energy, Homeland Security, and Transportation. All of these elements have vested interest in establishing controls around the use of sUAS to not only prevent malign actors from exploiting vulnerabilities, but also to ensure the US government has the tools to respond effectively.

2. Maintain a single, consolidated reporting database for any sUAs activity over critical infrastructure

The JIATF should establish a single, consolidated reporting database for any sUAS activity over critical infrastructure. This database should be maintained on an unclassified network in order to maximize the opportunity for local, state, and federal entities to utilize the data. The FAA's database on drone activity around airports is an excellent starting point but should be expanded to include other critical infrastructure vital to homeland defense. This includes all military installations, in addition to seaports and railheads. Specific tactics, techniques, and procedures for countering sUAS activity will inevitably require a higher classification level. The JIATF must ensure that this information remains accessible for all stakeholders and does not become "stove-piped" on networks not accessible to all.

3. NORTHCOM should lead DoD efforts within this new JIATF

NORTHCOM should lead DoD efforts within this new JIATF. As Guillot testified to the Senate Armed Services Committee in February 2025, NORTHCOM was tasked by the Secretary of Defense in late 2024 to "serve as the synchronizer, coordinator, and/or coordinator of domestic counter-small UAS (C-sUAS) within the continental United States

and Alaska for DoD and, when requested and approved, for the interagency." As part of this tasking, Guillot testified that NORTHCOM had established a C-sUAS branch within the headquarters. The JIATF simply builds on this existing task for NORTHCOM and provides an environment that facilitates coordination with interagency partners, and NORTHCOM already has a dedicated team that it can contribute to the JIATF.

In addition to day-to-day operations within the JIATF, the NORTHCOM C-sUAS team should also utilize data gathered by the JIATF in order to begin integrating more complex sUAS scenarios in any homeland defense training or exercises. By including these scenarios in annual exercises, NORTHCOM will create a forcing function for its staff to stay current on sUAS incidents and trends around critical infrastructure. This will also allow for further innovation in countering sUAS activity around critical infrastructure and, more specifically, denying sUAS access to DoD bases and facilities. DoD members of the JIATF should play a central role in exercise planning, ensuring any scenarios are consistent with current trends being monitored and countered by the JIATF.

4. NORTHCOM should also leverage DoD congressional liaisons in order to codify DoD's role in countering sUAS activity

NORTHCOM should also leverage DoD congressional liaisons in order to codify DoD's role in countering sUAS activity in CONUS and vastly expand its authority in countering sUAS activity. This role needs to be properly defined in context of what DoD is responsible for around non-DoD facilities and infrastructure, as well as clearly defining DoD's authorities to counter sUAS activity near or over its own facilities and infrastructure. These authorities must be easily understood so that commanders have the freedom to defend critical infrastructure without concerns over interpreting their authorities correctly. There are numerous UAS-related bills that have emerged from bipartisan elements in both the House of Representatives and the Senate, some of which do not include DoD in the text of the bill.[20] NORTHCOM, along with stakeholders from the new JIATF, should coordinate closely with members of Congress in order to properly deconflict C-sUAS authorities and activities, while providing a clear roadmap for all stakeholders so that they understand their roles and responsibilities, along with limitations. DoD has an important role to play in countering sUAS activity over critical infrastructure in the United States, and should not be left out of any C-sUAS legislation emerging from Congress.

5. NORTHCOM should continue to push for border-specific C-sUAS authorities

Finally, NORTHCOM should continue to push for border-specific C-sUAS authorities.[21] Guillot recently testified to the House Armed Services Committee, noting that he had asked for a change in rules of engagement that would "allow us to shoot down or bring down drones that are surveilling over our deployed and mobile troops … not just that are in self-defense, but anything that's

surveilling and planning the next attack on us within five miles of the border." The southern border mission objectives are rapidly evolving, and NORTHCOM must be given the authorities to deal with the sUAS threat, as it deploys and maintains troops along the border. As Guillot pointed out in his testimony, current authorities are inadequate for force protection. If sUAS activity along the border continues to go unchallenged due to inadequate laws and authorities, it simply creates another exploitable situation for malign state and non-state actors to take advantage of.[22]

Conclusion

The proliferation of sUAS in the United States has created an environment that is easily exploitable by foreign adversaries. Our research has concluded that existing counter-sUAS authorities are not strong enough and are poorly defined. As a result, multiple agencies who share responsibility for homeland defense are unable to properly deconflict roles and responsibilities when it comes to monitoring and countering sUAS activity. By establishing a JIATF dedicated to the sUAS problem set, agencies can be brought together to share data, while producing new and innovative techniques for maintaining safe skies around airports, and also denying foreign adversaries the ability to utilize sUAS platforms for malign activities. With help from Congress in establishing clear authorities for all parties, a JIATF will drastically reduce interagency friction, while increasing their capability to secure and defend the homeland.

1 Statement of General Gregory M. Guillot, Commander, United States Northern Command, to the Senate Armed Services Committee, US Senate Armed Services Committee, February 13, 2025, https://www.armed-services.senate.gov/imo/media/doc/guillot_statement1.pdf.

2 Jack Watling and Nick Reynolds, "Tactical Developments During the Third Year of the Russo-Ukrainian War," Royal United Services Institute, February 14, 2025, https://www.rusi.org/explore-our-research/publications/special-resources/tactical-developments-during-third-year-russo-ukrainian-war,

3 FAA Drone Registry Tops One Million, Department of Transition, January 10, 2018, https://www.transportation.gov/briefing-room/faa-drone-registry-tops-one-million.

4 Drone Sightings Near Airports, Federal Aviation Administration, Last Updated in March 2025, https://www.faa.gov/uas/resources/public_records/uas_sightings_report.

5 Joint Publication 3-27, Homeland Defense, Department of Defense, April 10, 2018, https://irp.fas.org/doddir/dod/jp3_27.pdf.

6 Drone Sightings Near Airports, https://www.faa.gov/uas/resources/public_records/uas_sightings_report.

7 DJI-type drones broadly refer to small Chinese-manufactured sUAS that are available for purchase online in large numbers and which make up 90% of the commercial drone market.

8 Drone Sightings Near Airports, https://www.faa.gov/uas/resources/public_records/uas_sightings_report.

9 Small Unmanned Aircraft Systems, 14 CFR Part 107, Federal Aviation Administration, June 28, 2016, https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-107; "What to Know About Drones," Federal Aviation Administration, January 14, 2025, https://www.faa.gov/newsroom/what-know-about-drones.

10 Statement by Governor Kathy Hochul on Additional Drone Activity, State of New York, December 14, 2024, https://www.governor.ny.gov/news/statement-governor-kathy-hochul-additional-drone-activity.

11 Adam Kehoe and Marc Cecotti, "Multiple Destroyers Were Swarmed By Mysterious 'Drones' Off California Over Numerous Nights," *The War Zone*, May 23, 2021, https://www.twz.com/39913/multiple-destroyers-were-swarmed-by-mysterious-drones-off-california-over-numerous-nights; Adam Kehoe and Marc Cecotti, "Drone Swarms That Harassed Navy Ships Off California Demystified In New Documents," *The War Zone*, June 2022, https://www.twz.com/drone-swarms-that-harassed-navy-ships-demystified-in-new-documents.

12 Gordon Lubold, Lara Seligman, and Aruna Viswanatha, "Mystery Drones Swarmed a U.S. Military Base for 17 Days. The Pentagon Is Stumped," *The Wall Street Journal*, October 12, 2024, https://www.wsj.com/politics/national-security/drones-military-pentagon-defense-331871f4.

13 Tyler Rogoway and Howard Altman, "Mysterious Drones Have Descended Again On U.S. Air Bases In The United Kingdom (Updated)," *The War Zone*, November 25, 2024, https://www.twz.com/news-features/mysterious-drones-are-back-near-u-s-air-bases-in-the-united-kingdom.

14 Andreas Rinke and Rachel More, "U.S. military confirms drone sightings at air base in Germany," *Reuters*, December 13, 2024, https://www.reuters.com/world/europe/unidentified-drones-sighted-over-us-air-base-germany-spiegel-reports-2024-12-13/.

15 Brien McElhatten, "Documents describe drone sightings at Hill Air Force Base," *ABC4 Utah*, December 18, 2024, https://www.abc4.com/news/local-news/documents-describe-drone-sightings-at-hill-air-force-base/.

16 Howard Altman, "Drone Incursions Closed Wright-Patterson Air Force Base's Airspace Friday Night," *The War Zone*, December 15, 2024, https://www.twz.com/air/drone-incursions-closed-wright-patterson-air-force-bases-airspace-friday-night.

17 Mystery Drones Swarmed a U.S. Military Base for 17 Days," October 12, 2024, https://www.wsj.com/politics/national-security/drones-military-pentagon-defense-331871f4.

18 Elissa Salamy, "Black Hawk pilot failed to heed flight instructor before DCA plane crash: report," *Fox 5*, April 28, 2025, https://www.fox5dc.com/news/black-hawk-pilot-failed-heed-flight-instructor-before-dca-plane-crash.

19 Author Interview, US Air Force Official, April 2024.

20 For example, see: H.R.8610 - Counter-UAS Authority Security, Safety, and Reauthorization Act, US House of Representatives, https://www.congress.gov/bill/118th-congress/house-bill/8610/text.

21 Matthew Olay, "NORAD commander: Incursions by unmanned aircraft systems on southern border likely exceed 1,000 a month," DoD News, March 15, 2024, https://www.jbsa.mil/News/News/Article/3708006/norad-commander-incursions-by-unmanned-aircraft-systems-on-southern-border-like/.

22 Matthew Olay, "NORAD commander."

The Foreign Policy Research Institute (FPRI) is a nonpartisan Philadelphia-based think tank dedicated to strengthening US national security and improving American foreign policy.

Established in 1955 by the noted 20th century geopolitical strategist, Ambassador Robert Strausz-Hupé, FPRI was founded on the premise that an informed and educated citizenry is essential for the United States to understand complex international issues and formulate foreign policy. FPRI remains committed to this principle and strives to inform both policymakers and the general public through FPRI research and educational programs.

FPRI is a nonpartisan 501(c)(3) non-profit organization and takes no institutional positions on issues andt conducts no advocacy. The organization has four main research programs, covering US National Security, Eurasia, Asia, and Africa. Each program produces reports, articles, public events, and private briefings for policymakers, FPRI members, and the general public.

Join the Conversation

123 S Broad St, Suite 1920,
Philadelphia, PA 19109
215.732.3774 | fpri.org | @FPRI

FPRI Editorial Team

Authors
Aaron Stein
Tim Ball

Editing
Emma Salisbury

Layout and Design
Natalia Kopytnik


75 YEARS
FPRI
FOREIGN POLICY RESEARCH INSTITUTE