AMERICAN FOREIGN POLICY COUNCIL

DEFENSE TECHNOLOGY PROGRAM BRIEF

We've Lost Control of Our Air Space

By: Chloe E. Smith and Peter Garretson

BRIEFING HIGHLIGHTS

- **Drones as Strategic Threats**: Unmanned Aerial Systems (UAS) have transformed modern warfare, giving adversaries a low-cost, high-impact tool to threaten critical infrastructure, disable military operations, and exploit U.S. vulnerabilities.
- **Rising Adversarial Activity**: Drone incursions by adversaries have targeted U.S. bases and infrastructure domestically and abroad, probing defense readiness while evading attribution.
- **Lessons from Ukraine**: Ukraine's battlefield innovation—fiber-optic comms, swarm tactics, and improvised countermeasures—shows how agile, necessity-driven responses can overcome superior firepower.
- **Fragmented Jurisdiction**: Disjointed authorities between DoD, DHS, FAA, and local law enforcement have created serious gaps in airspace defense, delayed responses, and weakened national security.
- **Legal and Operational Constraints**: Current laws restrict the military and law enforcement from using effective counter-drone technologies, complicating engagement with drones even when threats are evident.
- **U.S. Innovation Deficit**: Despite its resources, the U.S. has lagged in practical counter-UAS innovation due to bureaucratic red tape, leaving it ill-prepared for rapidly evolving drone threats.
- **Policy Roadmap**: Treat drone incursions as air sovereignty violations under NORTHCOM/NORAD; deploy pursuit drones via Guard units; launch a DARPA counter-UAS innovation challenge; adopt proportional deterrence; and streamline tech procurement for frontline units.

The proliferation of unmanned aerial systems (UAS), or drones, represents a critical threat to U.S. national security. From their potential to attack critical infrastructure to their capacity to disrupt civilian and military operations, drones have reshaped the battlefield and eroded the notion of secure airspace. This paper argues that **without immediate legal and technological reforms, the U.S. will remain vulnerable to adversarial drone incursions** that exploit current jurisdictional and strategic gaps in our existing system.

WHY DRONES ARE A UNIQUE THREAT

Drones have fundamentally altered the nature of conflict, possessing several characteristics that make them particularly dangerous. State and non-state actors now have an asymmetric advantage against conventional military forces. **Rapid and coordinated swarms have the ability to overwhelm defenses, targeting critical infrastructure such as power grids, airports, and**

Chloe E. Smith *is a Fellow in National Security Affairs at the American Foreign Policy Council and editor of the Resource Security Watch e-bulletin. She holds a B.A. in Political Science from Bucknell University and is currently pursuing an M.A. in Global Security Studies at USC.*

Peter Garretson *is a senior fellow in defense studies at the council and also serves as co-director of the AFPC Space Policy Initiative. He is co-author of* The Next Space Race: A Blueprint for American Primacy and Scramble for the Skies: The Great Power Competition to Control the Resources of Outer Space. *His forthcoming co-authored book,* Space Shock: 18 Threats That Will Define Space Power, *will be published in October 2025.*

communications systems. They are also easily concealed, deployed, and can be operated by small remote teams. Low-cost drones can also disable expensive military assets (including major investments such as bombers, fighters, or surface combatants) or infrastructure (such as fuel depots), making for exceptionally cost-effective destructive capabilities. The precision these advanced systems possess also heightens their psychological and strategic impact as they can recognize and eliminate specific targets. **The consequences for our defense systems as they now stand are clear: our air force is paralyzed if it cannot launch, our naval power is useless if vessels cannot deploy, and our army units will be ineffective if they are stranded without communication**.

Countering unmanned aerial systems (UAS) poses significant challenges due to both technological and jurisdictional limitations. Technologically, the use of kinetic countermeasures, including lasers, high-powered microwaves, and jammers, is also highly restricted due to legal restraints and the risk of potentially harming satellites, civilian infrastructure, or military systems.[1] The difficulty of distinguishing hostile drones from legitimate civilian or commercial ones complicates effective targeting, with the cost disparity between low-cost drones and expensive interceptors further straining resources.

A NEW ERA OF WARFARE

Over the past few decades, the growing sophistication of drone technology has been highlighted by key international incidents showcasing its expanding capabilities. From the early use of drones by terrorist organizations in Iraq to Ukrainian battlefields[2] and attacks on Saudi oil facilities,[3] these events underscore the strategic use of drones in modern conflicts. China's demonstrations of drone swarms underscore the alarming advancements in UAS capabilities. **While the U.S. has thus far avoided catastrophic domestic drone attacks, it is only a matter of time before adversaries exploit gaps in our readiness** and challenge the security of U.S. airspace.

The operational capabilities of UAS in military affairs have been recognized for years. Since the Air Force released its Unmanned Aircraft Systems Roadmap 2005-2030,[4] outlining plans to integrate UAS into military operations, the tactical advantages of small and medium UAS have been evident.

These systems provide flexible tactical superiority that traditional boots on the ground could not match. However, despite their clear advantages, **efforts to address the threat have lagged behind the pace of technological advancement**. Early attempts to counter this emerging challenge include the Defense Intelligence Agency's (DIA) Defense Warning Office-led Black Dart exercises[5] in the early 2000s, which were among the first to focus on testing and developing counter-UAS strategies.

It was not until 2019, following a significant incident involving drones at Offutt Air Force Base,[6] that the then DoD (now the Department of War, DoW) began to emphasize the need for proactive countermeasures in the face of risks posed by UAS to critical military installations and operations. Failure to respond quickly to evolving drone capacities and proliferation will only risk the U.S. falling behind in addressing one of the most significant threats in modern warfare.

NECESSITY DRIVES INNOVATION IN UKRAINE

Russia's invasion of Ukraine has also dramatically reshaped the nature of the modern battlefield, illustrating how necessity drives rapid innovation and adaptation. Ukraine's battlefield is an active testing ground for cutting-edge technologies, where advanced UAS systems—once controlled only by the most technologically sophisticated militaries—are now accessible due to both external support and domestic innovation. In a war where deterrence has already failed, innovation is a form of survival. Ukrainian forces—uninterested in limitations—have forged ahead with technological innovations that have redefined the battlefield, shifting a war that Putin seemed positioned to win.

One of the most striking developments has been the application of fiber optic cables, immune to electromagnetic interference, which provide communication channels that are nearly impossible to jam.[7] This marks a fundamental shift in how information flows in combat environments, enabling much faster and more efficient situational awareness that has allowed Ukraine to outmaneuver a technically superior adversary both offensively and defensively. On the defensive, Ukrainian forces have resorted to using fishnets to catch Russian drones when conventional defenses fail.[8] This is a clear example of how Ukrainian innovation is transforming

both the tactics and tools that have long defined the landscape of modern warfare.

On the battlefield, drones are proving to be decisive tools, as demonstrated by Ukraine's successful defenses against Russian attacks. **Operation Spiderweb exemplifies this transformation**.[9] Over the course of 18 months, Ukrainian forces smuggled short-range drones and explosives into Russia. Once positioned near key airbases, the drone strike penetrated deep into Russian territory, marking Ukraine's longest-range attack of the conflict. The attack hit four Russian airbases across three time zones, including locations as distant as Siberia, such as Belaya in Irkutsk, Olenya in Murmansk, Dyagilevo in Ryazan, and Ivanovo Severny. According to Ukrainian officials, **the operation damaged or destroyed 41 military aircraft, including strategic bombers like the Tu-95 and Tu-160, with total losses estimated at $7 billion**.[10] The operation involved 117 drones, highlighting Ukraine's growing capacity to expose deep strategic vulnerabilities inside Russia despite being outgunned.

In addition to the stunning success of Operation Spiderweb, an engagement in January 2025 near the Kursk region, Ukraine's 47th Mechanized Brigade "Magura," in coordination with SOU affiliates, effectively neutralized a large-scale Russian assault involving nearly 50 armored vehicles.[12] However, the damage extends both ways. Over the course of the conflict, **Russia has launched massive drone assault operations on Ukraine's critical infrastructure, sending over 14,700 one-way attack drones since 2022**.[13] These attacks are part of a strategic effort to recover from its military setbacks by **crippling energy grids, communications, and other vital infrastructure** to compensate for battlefield losses.

FIGURE 1: HEAD OF THE SECURITY SERVICE OF UKRAINE (SBU)[11]

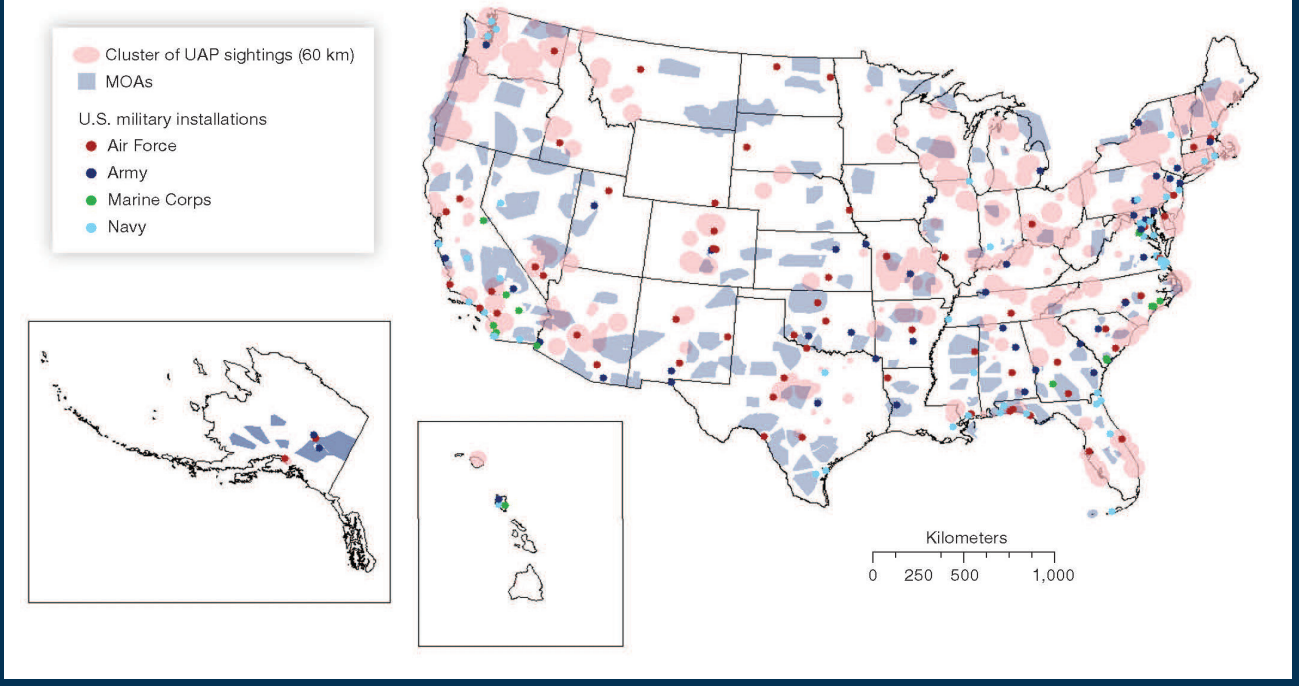
Today, the **United States remains vulnerable to a surprise drone attack**. The United States has largely lagged behind in research and development for drone technologies.[14] The pace of **meaningful innovation within the U.S. military has been hindered by bureaucratic intertia.** In contrast to Ukraine, which is directly involved in a hot war with Russia and has been driven to create practical solutions, the U.S. defense base seems to be caught in a protracted cycle of unmotivated technological development. **This gap risks leaving the U.S. unprepared for future conflicts where adversaries may leverage** the rapid innovation cycles that active warfare demands, as demonstrated by technological advances emerging from the Ukraine conflict.

DRONES ON AMERICAN SOIL

Drone operations frequently function in the "grey zone" of warfare, leveraging deniability to achieve strategic goals without triggering direct military confrontation. Adversaries have used drones as a litmus test to gauge the strength of U.S. defense systems, as demonstrated by recent balloon flyovers and drone incursions. By exploiting public interest in unidentified anamolous phenomena (UAPs), they can obscure their activities and erode confidence in national security systems. These actions align with asymmetric warfare doctrine aimed at undermining U.S. defense readiness through persistent, low-level threats without provoking direct confrontation.

Adversarial drone incidents are already degrading U.S. military operations. Incidents involving UAPs have led to temporary shutdowns of U.S. military bases, highlighting security vulnerabilities. In December 2024, the Wright-Patterson Air Force Base[15] in Ohio closed its airspace due to "heavy drone activity," and security forces were mobilized to address the situation. Similarly, the U.S. Air Force bases in the United Kingdom, including RAF Lakenheath, RAF Mildenhall, and RAF Feltwell, reported sightings of drones.[16] These incidents triggered investigations by U.K. and U.S. au-

FIGURE 2: LOCATIONS OF UAP SIGHTING CLUSTERS, MILITARY INSTALLATIONS, AND MOAS, 1998-2022[22]



thorities into possible Russian involvement, as these critical military bases house cutting-edge aircraft and defense technology.[17] These activities are part of broader concerns about Russia's influence operations that may have been testing the readiness of U.S. forces without directly engaging in military confrontation.[18] The DoW has acknowledged a concentration of UAP reports near U.S. military assets and sensors, and continues to monitor activity with various agencies to develop appropriate responses to these emerging threats.[19]

Gen. Gregory Guillot testified before the Senate Armed Services Committee, reporting that **350 drone incursions were detected last year across 100 U.S. military installations**.[20] He emphasized the need for expanded authorities under Section 130i of Title 10 U.S. Code to allow all base commanders to counter these threats, rather than just those at "covered installations."[21]

Recognizing these limitations, Sen. Tom Cotton and Sen. Kirsten Gillibrand are advocating for legislation to grant commanders the necessary authority and capability to protect their bases from drone surveillance and other potential threats. Meanwhile, the War Department has taken steps to bolster counter-drone measures, including creating a dedicated operations branch and hosting counter-drone technology demonstrations. NORAD and NORTHCOM are coordinating efforts to integrate new detection and mitigation technologies. **However, the current legal framework is hindering the military's ability to effectively engage with hostile or suspicious drones that enter U.S. airspace**.

Drone espionage has impacted America's most classified military projects. Recent United States Air Force (USAF) reports suggest that seven drone incursions over Plant 42 and Palmdale Regional Airport have also raised significant concerns of espionage.[23] The drones displayed advanced capabilities far beyond that of typical hobbyist drones and moved in coordinated flight patterns. Despite security patrols and assistance from the Federal Aviation Administration (FAA) and local law enforcement, the drones could not be identified.

Earlier this year, numerous reports of drones operating over the New York and New Jersey areas,[24] particularly near military installations, as well as civilian infrastructure, triggered investigations by federal and state authorities, including DHS and the FBI. **These incidents showcased a deficit in America's ability to respond effectively**.[25] In response, the FAA imposed temporary flight restrictions in certain areas, and state officials called

Fragmented jurisdiction and technological limitations have created a catastrophic gap in U.S. readiness to counter drone threats.

for advanced radar systems capable of detecting drones to assist ongoing investigations.[26] The failure of local NJ law enforcement advanced industrial drones failed to intercept the unidentified aircraft, which demonstrated superior maneuverability and speed capabilities. The situation highlights the challenges authorities face in regulating drone usage and ensuring public safety from UAS and UAP threats under the current regulatory system.

NEW JERSEY'S WAKE-UP CALL

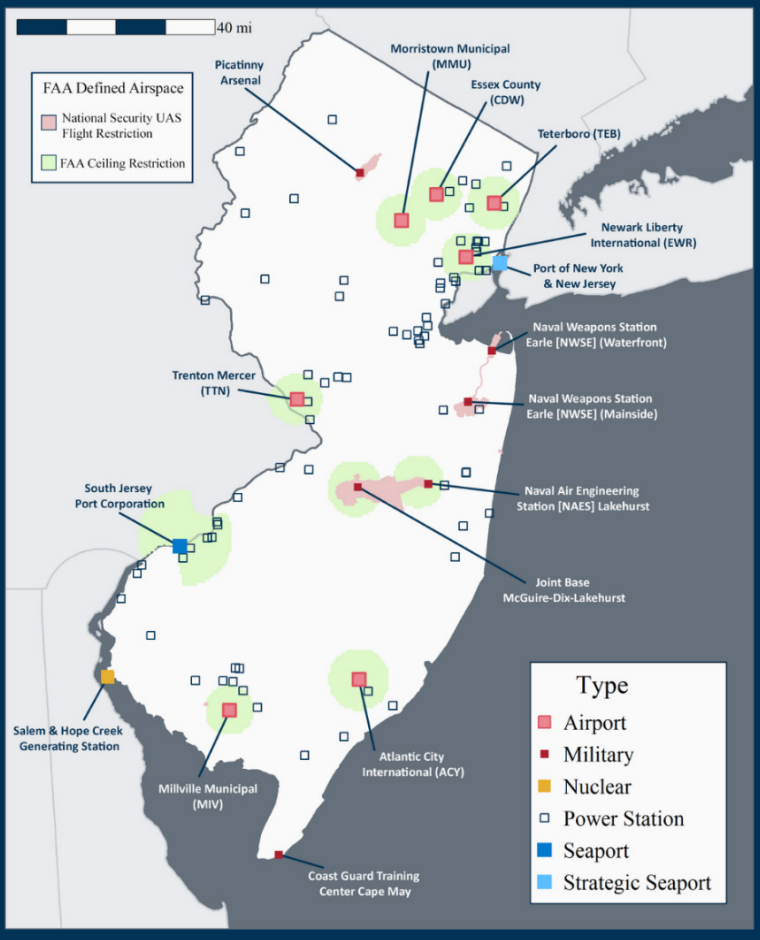
The series of unidentified drone sightings over New Jersey sparked alarm among the public and triggered a multi-agency investigation, revealing significant challenges in America's ability to counter aerial threats. Reports indicated that drones were operating near critical infrastructure. Despite deploying advanced detection systems and high-speed pursuit drones, authorities could not intercept or identify the origin of the drones. **The drones demonstrated unexpected agility, outmaneuvering law enforcement equipment**.

State leadership, the FAA, DHS, and other domestic agencies offered no clear reassurances about whether a threat existed. **The case exposed the troubling reality that fragmented jurisdiction and technological limitations have created a major gap in U.S. readiness to counter drone threats**. The inability to track or verify the drones' origins underscores the urgent need for better interagency coordination to block UAS capabilities.

Initial reports of drone activity in New Jersey surfaced on November 19, 2024, when local law enforcement in Morris County observed drones in the area.[27] On November 22, the FAA issued temporary flight restrictions (TFRs) over critical infrastructure in New Jersey, followed by another TFR over the Picatinny Arsenal only days later, a premier research and development center for the U.S. Army that focuses on the innovation and production of advanced weaponry, ammunition, and military technology.[28] Finally, on December 12, the FBI, DHS, FAA, and DoW issued a joint statement that there was no evidence of a threat.[29] Frustration from the response to the drone sightings along the East Coast was **plagued by fragmented interagency communication and a slow escalation of security measures, resulting in mounting public frustration** that ultimately led to dangerous actions by civilians.

The potential ramifications of these incidents were significant. **The failure to respond effectively to these drone sightings exposed serious vulnerabilities**. If the drones spotted over New Jersey airspace were adversarial, they could have conducted surveillance on sensitive military installations or carried out unprecedented attacks on critical infrastructure. **Key targets such as military bases, dams, airports, nuclear power plants, power transformers, and bridges were**

FIGURE 3: CRITICAL INFRASTRUCTURE IN NEW JERSEY



Source: American Foreign Policy Council

all within range of the sightings. New Jersey is home to several critical military and defense installations, including Joint Base McGuire-Dix-Lakehurst, which serves as a hub for the U.S. Air Force, Army, and Navy, supporting air mobility, training, and logistical operations. Additionally, Naval Weapons Station Earle is a key facility for the U.S. Navy responsible for storing and supplying munitions to naval vessels. **This case study serves as a stark reminder that the U.S. must urgently enhance its capabilities to prevent future security breaches**.

FIGURE 4: ESSENTIAL CRITICAL INFRASTRUCTURE[32]

INTERAGENCY COOPERATION AND RESPONSIBILITIES

The division of jurisdiction over U.S. airspace is fragmented, with various entities operating under their own limited authority and resources. **The DoW does not have the authority to defend critical infrastructure such as nuclear power plants, power transformers, bridges, and dams**. This confines military action to within their own perimeters, leaving domestic threats to be handled by DHS.[30] The DoW depends on a vast network of critical infrastructure that is vulnerable to adversarial attacks, and while it has been developing protective policies, including the Defense Critical Infrastructure Program (DCIP), there are still challenges to effectively identifying and coordinating the safeguarding of critical assets.[31]

Local law enforcement lacks the expertise and legal authority to address threats effectively, and the FAA's role is confined to regulating civilian airspace without sufficient capacity to deal with security issues. **Federal laws further restrict the use of counter-drone technologies, such as jammers and kinetic defense**, with specific exceptions only from federal agencies. The military's inability to intervene domestically without extensive coordination delays responses and allows for gaps in areas where countermeasures are ineffective. **A unified approach is critical to protect U.S. airspace from emerging threats** and project confidence in U.S. aerial defense systems.

These legal and jurisdictional barriers are hindering our readiness to respond to threats in U.S. airspace. **Adversaries can exploit delayed response times by operating in areas where ambiguous jurisdictional ambiguity limits effective countermeasures**. Addressing these challenges requires a more unified approach to securing our airspace. This includes enhancing interagency coordination and ensuring that the U.S. is investing in technology that strengthens our counter-UAS capabilities. **Without decisive action, these inefficiencies will continue to create exploitable vulnerabilities that undermine U.S. national security infrastructure**.

Fragmented jurisdiction over U.S. airspace poses significant challenges to coordinating responses to aerial security threats. Military bases have authority only within their perimeters, local law enforcement often lacks the necessary expertise and resources, and the FAA has limited capacity to address security threats in civilian airspace. **This fragmented system creates vulnerabilities and makes effective countermeasures easier for adversaries to exploit**.

Determining who has the authority to neutralize a drone involves complex legal and jurisdictional considerations. The use of kinetic counter-drone technology is heavily restricted under U.S. federal law. According to the U.S. Department of Justice, the **Aircraft Sabotage Act, 18 U.S.C. § 32(a)**[33] criminalizes certain destructive actions with respect to "aircraft," including damaging,

destroying, or disabling those aircraft. Similarly, the **Aircraft Piracy Act, 49 U.S.C. § 46502**[34] criminalizes the act of seizing or exercising control of an "aircraft" with "wrongful intent."

Federal agencies such as the DoW and Department of Homeland Security (DHS) have limited exemptions under certain circumstances, particularly in protecting critical infrastructure or military facilities. When questioned about the DHS' inaction against illegal drones, Mayorkas explained that DHS's authority is limited, highlighting the roles of the Coast Guard, Secret Service, and Customs and Border Protection.[35] Local law enforcement, however, typically lacks the authority to respond, primarily relying on federal support.

The U.S. military has sophisticated counter-UAS technologies, including directed energy weapons, signal jamming systems, and advanced radar. However, the **Posse Comitatus Act** largely restricts the use of military personnel for domestic law enforcement purposes. These limitations directly undermine successful counter-UAS operations and highlight the need for reform.

Military intervention is typically limited to defending military installations and responding to national security threats, requiring coordination with federal civilian agencies. When operating domestically, military actions must align with legal frameworks such as the **National Defense Authorization Act (NDAA)**,[36] which grants specific counter-UAS authorization to the DoW under specific conditions. **This creates a scenario where the military may detect a threat outside of its jurisdiction but cannot respond without proper authorization**.

POLICY RECOMMENDATIONS

Drone warfare represents a paradigm shift in what may constitute the most dangerous asymmetric national security threat. **The U.S. must act decisively to reclaim control of its airspace and prepare for a new era of warfare**. By rethinking jurisdictional responsibilities, enhancing counter-UAS capabilities, and fostering innovation, the United States can secure its skies and maintain its strategic advantage. Failure to act will leave the nation vulnerable to potential future aerial security threats.

To address the escalating threat posed by drone warfare and ensure effective defense of U.S. airspace, the following policy recommendations outline a strategic framework for tackling this complex challenge. These recommendations focus on two main areas: redefining the mission to treat drone incursions as air sovereignty threats and enhancing counter-UAS capabilities nationally. By fostering innovation, integrating public and private efforts, and adopting deterrence strategies, these measures aim to improve detection and response capabilities, strengthen resilience against drone threats, and ensure the United States maintains control of its airspace in the face of evolving technological and strategic challenges.

Drone warfare represents a paradigm shift in what may constitute the most dangerous asymmetric national security threat.

First, **we must treat drone incursions not as merely law enforcement issues, but as critical air sovereignty threats** under the jurisdiction of U.S. Northern Command (NORTHCOM) and North American Aerospace Defense Command (NORAD). This shift would enable a more coordinated and robust response to unauthorized drones. **Legislative measures should empower NORTHCOM to assume unidentified or unauthorized drones in restricted or sensitive airspace are potential threats and grant the authority to take action to neutralize them before they pose significant risks**.

Second, to strengthen the nation's defense, enhancing counter-UAS capabilities by **deploying "pursuit drones" and counter-UAS systems across Air National Guard, Civil Air Patrol, and Army National Guard units is essential**. Existing networks allow for broad geographical reach and readiness for accelerated deployment. Additionally, the deployment of advanced sensor suites should be prioritized to enhance the detection of drones, ensuring a comprehensive surveillance infrastructure.

Innovation on this front is also critical to staying ahead of the evolving threat environment. **A multi-year grand challenge hosted by DARPA should be launched to incentivize the development of advanced drone apprehension and destruction technologies**. By fostering competition and innovation, this initiative can identify cutting-edge solutions to counter UAS threats. Furthermore, flexible acquisition models

should be employed to scale successful technologies for rapid procurement by authorized front-line units.

Third, to deter hostile activity, **the United States should adopt a Tit-for-Tat strategy (responding to aggression with proportional retaliation)**. When intelligence confirms adversarial use of drones against the U.S., appropriate countermeasures should be employed to neutralize the threat and demonstrate willingness to retaliate effectively. This approach would discourage further aggression and foster a policy of strategic deterrence.

Considering the growing sophistication and proliferation of drone technology, the United States must act decisively to address this critical threat to national security and regain control over our airspace. Implementing these measures will mitigate current vulnerabilities while ensuring the nation is prepared to counter emerging threats in the rapidly evolving landscape of drone warfare.

ENDNOTES

[1] Science & Tech Spotlight: Counter-Drone Technologies", Government Accountability Office, March 2022, https://www.gao.gov/assets/720/719512.pdf.

[2] "Ukraine strikes Russia with missiles and drones in one of largest air attacks", Reuters, January 15, 2025, https://www.reuters.com/world/europe/ukraine-strikes-russia-with-massive-drone-atacms-attack-russian-telegram-2025-01-14/?utm_source=chatgpt.com.

[3] Ben Hubbard, Palko Karasz, Stanley Reed, "Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran", *The New York Times*, September 15, 2019, https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html.

[4] "Unmanned Aircraft Systems Roadmap 2005-2030", *Department of Defense*, August 4, 2005, https://irp.fas.org/program/collect/uav_roadmap2005.pdf.

[5] Richard Whittle, "Military exercise Black Dart to tackle nightmare drone scenario", *New York Post*, July 25, 2015, https://nypost.com/2015/07/25/military-operation-black-dart-to-tackle-nightmare-drone-scenario/.

[6] "Air Force Rolling Out Drone Defenses", *AVweb*, April 12, 2019, https://www.avweb.com/recent-updates/business-military/air-force-rolling-out-drone-defenses/.

[7] Howard Altman, "Inside Ukraine's Fiber-Optic Drone War", *The War Zone*, May 28, 2025, https://www.twz.com/news-features/inside-ukraines-fiber-optic-drone-war.

[8] Constant Méheut, "Ukraine Turns to Fishing Nets to Catch Russian Drones" *The New York Times*, July 8, 2025, https://www.nytimes.com/2025/07/07/world/europe/ukraine-russia-drones-nets.html.

[9] "Operation Spiderweb: a visual guide to Ukraine's destruction of Russian aircraft", *The Guardian*, June 2, 2025, https://www.theguardian.com/world/2025/jun/02/operation-spiderweb-visual-guide-ukraine-drone-attack-russian-aircraft.

[10] Ben Wolfgang, "'Russian Pearl Harbor': Moscow stunned after Ukrainian drones hit 5 bases, destroy 40 aircraft", *The Washington Times*, June 2, 2025, https://www.washingtontimes.com/news/2025/jun/2/russian-pearl-harbor-moscow-stunned-ukrainian-drones-hit-5-bases/.

[11] Laura Gozzi, "How Ukraine carried out daring 'Spider Web' attack on Russian bombers", *BBC News*, June 2, 2025, https://www.bbc.com/news/articles/cq69qnvj6nlo.

[12] "Two Waves of Equipment And Infantry: 47th Separate Mechanized Brigade 'Magura' Repels Russian Assault in Kursk Region", *Militarnyi*, March 3, 2025, https://mil.in.ua/en/news/two-waves-of-equipment-and-infantry-47th-separate-mechanized-brigade-magura-repels-russian-assault-in-kursk-region/.

[13] Neil Hollenbeck, Muhammed Hamza Altaf, Faith Avila, Javier Ramirez, Anurag Sharma, and Benjamin Jensen, "Calculating the Cost-Effectiveness of Russia's Drone Strikes", *CSIS*, February 19, 2025, https://www.csis.org/analysis/calculating-cost-effectiveness-russias-drone-strikes.

[14] Farah Stockman, "Drones Are Key to Winning Wars Now. The U.S. Makes Hardly Any." *The New York Times*, July 13, 2025, https://www.nytimes.com/2025/07/13/business/drones-us-military-manufacturing-lags.html.

[15] Brad Lendon and Hanna Park, "Key US Air Force base closes airspace amid drone sightings", *CNN*, December 16, 2024, https://www.cnn.com/2024/12/16/us/us-air-force-base-closes-airspace-drone-sightings-hnk/index.html.

[16] Kai Greet, "Additional U.S. Bases in the UK Now Protected by Restricted Airspace as Counter-Drone Operation Continues", *The Aviationist*, November 30, 2024, https://theaviationist.com/2024/11/30/us-bases-uk-drone-incursions-update/.

[17] Richard Holmes, "Russian links to drone sightings over UK air bases probed", *The i Paper*, February 24, 2025, https://inews.co.uk/news/russian-links-drone-sightings-uk-air-base-3542584.
[18] "Annual Threat Assessment of The U.S. Intelligence Community," Office of the Director of National Intelligence, March 2025, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.
[19] Howard Altman, "FAA Insider Opens Up About Drone Incursions Over Military Bases", *TWZ*, August 15, 2025, https://www.twz.com/air/foreign-nexus-in-military-base-drone-incursions-detailed-by-government-insider.
[20] Chrissmith.house.gov, "NORTHCOM Commander confirms mysterious drones may have been operated with nefarious intentions", February 14, 2025, https://chrissmith.house.gov/news/documentsingle.aspx?DocumentID=413528&fbclid=IwZXh0bgNhZW0CMTEAAR2E8bCJEey9ripRMfMQBVmodX3fHRKTQEFCpqjfa2xlZbaPfD0McXsilXg_aem_9jk9oZ7GIrfDjVLifXe1Sg.
[21] Jon Harper, "NORAD commander says hundreds of drone incursions were detected at US military installations", *DefenseScoop*, February 13, 2025, https://defensescoop.com/2025/02/13/drone-incursions-us-military-bases-norad-northcom-counter-small-uas/.
[22] Marek N. Posard, Ashley Gromis, Mary Lee, "Not the X-Files", RAND Corporation, Jul 25, 2023, https://www.rand.org/pubs/research_reports/RRA2475-1.html.
[23] Kyle Warfel and Christopher Sharp, "Newly Obtained USAF Reports Expose Drone Breaches at Plant 42, Home to B-21 Raider and Other Top Secret Programs, Sparking Espionage Concerns", *Liberation Times*, February 12, 2025, https://www.liberationtimes.com/home/newly-obtained-usaf-reports-expose-drone-breaches-at-plant-42-home-to-b-21-raider-and-other-top-secret-programs-sparking-espionage-concerns.
[24] Alyce McFadden, "Unidentified Drones Light Up New Jersey's Skies, Baffling Residents", *The New York Times*, December 7, 2024, https://www.nytimes.com/2024/12/07/nyregion/new-jersey-drones.html.
[25] Joseph De Avila, "Mystery Drones Leave Local Officials Seeking Action, Answers From Feds", *The Wall Street Journal*, December 16, 2024, https://www.wsj.com/us-news/drone-sightings-east-coast-response-380c1b84?st=cn9MqJ&reflink=article_imessage_share.
[26] Alex Nitzberg, " Schumer requests 360-degree radar system for NY, NJ to detect drones", *Fox News*, December 16, 2024, https://www.foxnews.com/politics/schumer-requests-360-degree-radar-system-ny-nj-detect-drones.
[27] Calvin Milliner, "Mystery drones in New Jersey, New York: A timeline of what officials have said", *ABC News*, December 17, 2024, https://abcnews.go.com/US/mystery-drones-new-jersey-new-york-timeline-what-officials-said/story?id=116824178.
[28] Dave Collins, "Mystery drone sightings continue in New Jersey and across the US. Here's what we know", *AP News*, December 20, 2024, https://apnews.com/article/drones-new-jersey-what-to-know-e6f565f5d51d9d47ad140e7e7d131842.
[29] "Joint DHS/FBI Statement on Reports of Drones in New Jersey", U.S. Department of Homeland Security, December 12, 2024, https://www.dhs.gov/archive/news/2024/12/12/joint-dhsfbi-statement-reports-drones-new-jersey#:~:text=Today%2C%20the%20FBI%20and%20DHS,or%20have%20a%20foreign%20nexus.
[30] "The Physical Protection of Critical Infrastructures and Key Assets", https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.
[31] "Defense Critical Infrastructure", U.S. Government Accountability Office, July 17, 2009, https://www.gao.gov/products/gao-09-740r.
[32] "Cybersecurity and Critical Infrastructure", Department of Homeland Security, September 9, 2024, https://www.dhs.gov/archive/coronavirus/cybersecurity-and-critical-infrastructure.
[33] "1423. Destruction Of Aircraft -- 18 U.S.C. 32(a)", U.S. Department of Justice, August 1999, https://www.justice.gov/archives/jm/criminal-resource-manual-1423-destruction-aircraft-18-usc-32a#:~:text=1423.-,Destruction%20Of%20Aircraft%20%2D%2D%2018%20U.S.C.,is%20defined%20in%2049%20U.S.C.
[34] "1407. Aircraft Piracy Within Special Aircraft Jurisdiction—49 U.S.C. 46502(a)", U.S. Department of Justice, August 1999, https://www.justice.gov/archives/jm/criminal-resource-manual-1407-aircraft-piracy-within-special-aircraft-jurisdiction-49-usc#:~:text=1407.-,Aircraft%20Piracy%20Within%20Special%20Aircraft%20Jurisdiction%E2%80%9449%20

U.S.C.,jurisdiction%20of%20the%20United%20States.

[35] Ina Fried, Colin Demarest, "DHS secretary calls for more money to track drones", *Axios*, https://www.axios.com/2024/12/17/drones-mayorkas-homeland-security.

[36] Jon Harper, "NDAA directs Pentagon's UAP office to team with new counter-drone task force", *DefenseScoop*, December 10, 2024, https://defensescoop.com/2024/12/10/uap-aaro-2025-ndaa-counter-uas-task-force/.

AMERICAN FOREIGN POLICY COUNCIL

DEFENSE TECHNOLOGY PROGRAM BRIEF

September 2025 | No. 27

ABOUT THE DEFENSE TECHNOLOGY PROGRAM

A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's (AFPC) work in these areas is aimed at helping U.S. offcials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Vice President of Operations and Director of Defense Technology Programs at Harrison@afpc.org.

ABOUT AFPC

For more than four decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies.

AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC MISSION STATEMENT

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:
1. Providing primary source information, as well as policy options,
to persons and organizations who make or influence the national security and foreign policies of the United States;
2. Arranging meetings and facilitating dialogue between American
Statesmen and their counterparts
in other countries; and
3. Fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

AMERICAN FOREIGN POLICY COUNCIL
509 C Street NE, Washington, D.C. 20002 | Telephone: 202.543.1006 | Fax: 202.543.1007 | www.afpc.org