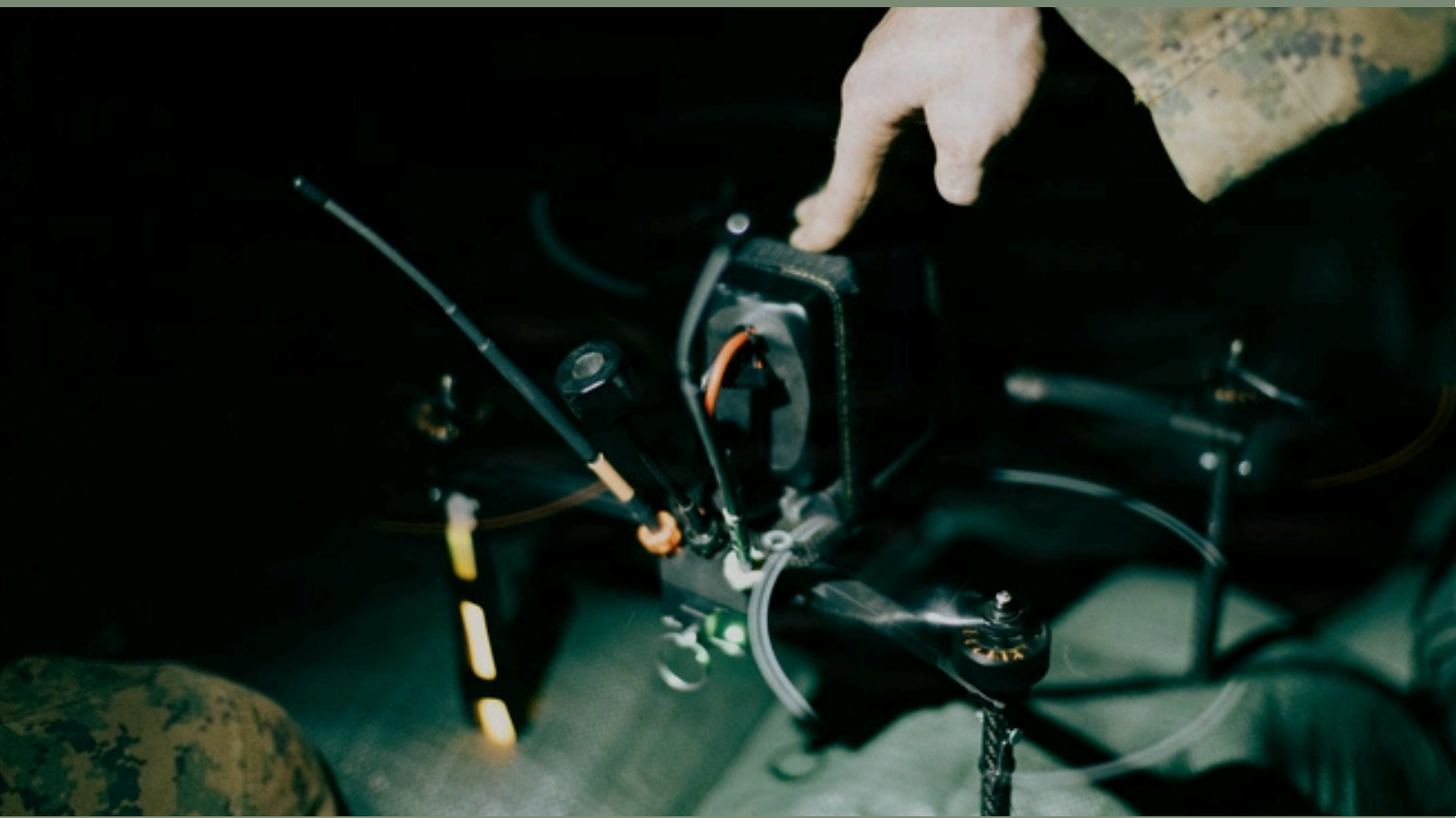
Cornell Brooks Public Policy

Tech Policy Institute

Defending America Against Drones

A Whole-of-Government Approach



Paul Lushenko & Joseph Amoroso

Defending America Against Drones;
A Whole-of-Government Approach

Paul Lushenko
Joseph Amoroso

On October 7, 2023, Hamas used drones to initiate its attack on Israel. On June 1, 2025, Ukraine conducted Operation Spider Web, using over 100 drones to strike Russian military bases and destroy one-third of the country's strategic bombers. Later in June, Israel conducted Operation Roaring Lion, using drones to destroy Iran's air defenses and enable jets to target Iranian missile production facilities.

Michael Poznansky and Erik Sand argue that these were "spectacular" attacks akin to covert operations. They were deliberate, well resourced, and aimed at high payoffs, such as demonstrating resolve. Security conditions in the U.S. are different, Poznansky and Sand contend, such that fears of similar attacks in the homeland are "overstated."

Yet these operations are inconsistent with emerging trends in drone warfare. First, drone warfare is now enabled by dual-use technologies—those that perform military and commercial functions. Houthi rebels in Yemen have developed fiberglass shells of Iran's Shahed 136 drone, allowing them to withstand disruptions in Iran's drone trade. Second, though some experts conflate drone warfare with a platform, the use of drones to attack targets reflects a global contagion effect. The Islamic State's drone campaign against coalition forces in 2017 caused analysts to warn that drones were "the next improvised explosive device." Finally, drone proliferation crosses state and non-state boundaries. For instance, the Islamic State evolved into a proto-state with a bureaucratic drone program.

Together, these trends also suggest that the U.S. military must now defend against drones, everywhere and all the time. The proliferation of drones represents not merely an academic consideration of adaptation to modern warfare, but a threat to national security. In December 2023, dozens of drones disrupted operations at Joint Base Langley-Eustis in Virginia, forcing the relocation of F-22 Raptor jets responsible for defending the homeland. This and similar incidents contribute to the recent National Defense Strategy's prioritization of homeland defense.

While the U.S. military recognizes the challenge of defending against drones, analysts criticize its approach. Most focus on laborious acquisition processes that have undermined the Department of Defense's ability to outpace the threat. While hardware is necessary to defend the homeland against drones, it is insufficient. In their recent book on drones, *Drones—What Everyone Needs to Know*, Sarah Kreps and James Patton Rogers explain that countering drones "is a cat-and-mouse game, one that will not be won by a single 'panacea' counter-technology." Rather, what is needed is broader synchronization of the Department of Defense with federal agencies and departments that contribute to homeland defense against drones. This partnership will allow the Department of Defense to help update counter-drone policies and authorities, facilitate information sharing to enhance situational awareness of the threat, align funding for capability development, and shape joint training.

Drones make the homeland vulnerable

The terrorist attacks of 9/11 ushered in an era of remote warfare characterized by the use of large, armed, and networked drones to enhance force protection while removing combatants and reducing collateral damage. Since then, countries have increasingly miniaturized drones. This has led to the emergence of smaller, commercially-available, and easily weaponized drones, such as the Chinese DJI.

Militaries, paramilitary forces, and terrorists across the globe have adopted small drones. These capabilities weigh under 1,300 pounds, fly below 18,000 feet, and generally move slower than 250 miles-per-hour. They afford adversaries a low-cost way to disrupt U.S. military operations. More problematically, they have arrived at America's shores. They literally "fly below the radar" of countermeasures and most of the U.S. military's existing capabilities are mismatched to real-world challenges. Radars are tuned and arrayed to observe high-end drones, like the U.S. MQ-9 Reaper, which are larger and fly higher and faster than small drones. They also rely on exquisite jamming techniques that, while effective, can threaten civilian transportation in the homeland.

In 2023, for instance, American imports of small drones totaled nearly $700 million. One report finds that 85% of these drones are manufactured in China. According to Air Force General Gregory Guillot, Commander of U.S. Northern Command, a staggering rise of drone use represents "a safety and security risk to military and other critical infrastructure." Following the incident at Joint Base Langley-Eustis, New Jersey experienced "mysterious" drone sightings in late 2024. These sightings were characteristic of the several hundred detections in 2024 at over 100 military bases.

Mexican drug cartels are also weaponizing small drones in ways that reflect best practices from Ukraine, thus threatening soldiers and law enforcement deployed at the U.S. southern border. In October 2025, three drones attacked a prosecutor's office in Tijuana, a major crossing point between Mexico and the United States as well as a thoroughfare for drug-smuggling. These incidents raise concerns that the Department of Defense cannot defend U.S. military bases and critical infrastructure from drones, much less support the protection of mass gatherings of Americans. From 2021 to 2024, for example, drone incursions at NFL football stadiums nearly doubled from 1,300 to 2,300.

Focus on hardware

To contend with this challenge, defense analysts emphasize the need for new acquisition processes that will allow the Department of Defense to rapidly scale counter-drone capabilities. The Department of Defense should procure counter-drone solutions in months, not years, and at far lower cost. This would bend the cost-exchange ratio; the U.S. military spends millions of dollars to intercept drones that cost a fraction of the price. In the Red Sea, U.S. warships use multimillion dollar missiles to engage Houthi drones that cost a few thousand dollars to make.

Jacquelyn Schneider and Julia Macdonald argue that the U.S. military risks losing the drone war because it prioritizes expensive and exquisite systems over cheaper and adaptable ones, which have been used

effectively by Azerbaijan, Israel, Russia, and Ukraine, among other countries. Stacie Pettyjohn and Molly Campbell discuss the same claim. So do Thomas Bunzel and Tom Donilon, who most recently emphasized that the United States "needs to double down on counterdrone measures."

Consistent with these arguments, Secretary of Defense Pete Hegseth directed the Department of Defense to accelerate counter-drone solutions. This initiative builds on President Donald Trump's intent to unleash "American drone dominance." At the same time, homeland defense against drones is a wicked collective action problem requiring greater unity of effort across federal agencies and departments, as well as local law enforcement. What is needed, *Bloomberg's* editorial board argues, is broader synchronization across these organizations.

Unity of effort is key to defend the homeland against drones

The drone threat spans military, homeland defense, and law enforcement domains. As such, the U.S. military's contribution to homeland defense against drones depends on effective cooperation and coordination with federal agencies and departments, as well as with law enforcement. Such a "whole-of-government" approach should focus on several efforts to maintain America's airspace sovereignty.

First, policymakers and defense officials should update the policies and authorities that enable counter-drone operations in the homeland, ensuring more timely responses to incursions. This includes streamlining interdiction efforts by local and state authorities. Although these authorities respond to public sightings of drones, they are guided by what Kreps and Rogers call "a tapestry of heterogeneous policies that reflect state-level views about the appropriate use of drones." Fortunately, Congress has recently passed legislation that enhances the ability of local and state authorities, pending certification from the Department of Justice, to interdict drones at public gatherings, such as sporting events. The National Guard, represented in every state and territory, offers another potential solution to help protect the homeland from drones. If appropriately aligned, resourced, and trained, the National Guard could coordinate with law enforcement to interdict drone incursions before triggering a response from federal authorities, namely U.S. Northern Command.

Second, a whole-of-government approach should be based on broader information sharing across federal agencies and departments for the evolving threat of drones in the homeland. Echoing a finding from the 9/11 Commission Report, information sharing is crucial to build situational awareness and enable complementary responses against drones, especially with local and state authorities. The key is to incentivize information sharing, which is often conditioned by a "need to know" that weighs the risk of inadvertent disclosure above the outcome of shared understanding. Outfitted with appropriate credentials and accesses, liaison officers can serve as a bridging mechanism across federal agencies and departments, helping to flag intelligence that informs understanding of key trends for the adversarial use of drones in the homeland.

Third, funding should also be aligned across the U.S. government for capability development to minimize redundancy and wasteful spending. This includes Replicator

2, which is the Department of Defense's primary way to fund counter-drone capability development and procurement. On their own, capabilities are not a silver-bullet against drones. Rather, the intent should be to offer a range of capabilities that, when enabled by the right data, software, training, authorities, and sustainment, and uniquely configured within different operating environments, provide a layered defense against drones. This approach integrates both nonlethal and lethal capabilities against drones. In the homeland, layered defense is conditioned by "low collateral defeat" capabilities such as high-powered microwaves. These reduce risks to civilians and their property, and research shows these considerations are important to Americans.

Finally, the U.S. military should closely train with federal agencies and departments, as well as law enforcement. This would baseline understanding of the threat of drones in the homeland and shape interoperability for counter-drone operations, which will help protect Americans at events such as the World Cup. This will unfold across the U.S. from June to July 2026. Training opportunities exist at the Joint Counter-Small Unmanned Aircraft Systems University in Oklahoma, which is designed to enhance miliary readiness to confront drones. Similarly, the Federal Bureau of Investigation recently opened a National Counter-Unmanned Training Center in Alabama that also enables joint training.

Untying the Gordan knot of countering drones in the homeland

In August 2025, the Department of Defense established the Joint Interagency Task Force 401 to address the threat of drones. It offers a way to shape a whole-of-government approach to defend the homeland against drones. The task force's mission is to synchronize the Department of Defense's counter-drone efforts to rapidly deliver joint capabilities at scale to protect U.S. and allied forces and assist federal agencies and departments in defending critical infrastructure and the homeland.

Specifically, the task force synchronizes the Department of Defense's counter-drone research, development, test, and evaluation efforts. It authorizes adoption of new counter-drone capabilities across the military services and can approve up to $50 million for development of novel counter-drone solutions. Many of these will have implications for federal agencies and departments, as well as local law enforcement. The task force also has a special hiring authorization to rapidly onboard experts and liaisons from across the joint force and U.S. government. These enhanced authorities enable the task force, which reports to the Deputy Secretary of Defense, Stephen Feinberg, to work with the National Security Council to help update counter-drone policies and authorities. This includes feedback to legislative proposals that expand the defense of U.S military bases against drones as well as empower local law enforcement to interdict drones.

On November 13, 2025, the Secretary of the Army and Joint Interagency Task Force 401 hosted a meeting at the White House with senior officials across the U.S. government. The discussion emphasized the need for stronger cooperation across the Department of Defense and federal agencies and departments for homeland defense against drones. As the task force's leadership explained, "the drone threat is evolving faster than any other, and no single agency can solve it alone."

Paul Lushenko is a Non-Resident Senior Fellow at the Tech Policy Institute.

Joseph Amoroso is a Council on Foreign Relations Term Member.

The views expressed are those of the authors and do not reflect the official position of the U.S. government, Department of Defense, or Department of the Army.

The appearance of U.S. Department of Defense (DoW) visual information does not imply or constitute DoW endorsement.

Sources

New Tech, Old Tactic: Does Hamas Have a Real Strategy?

Ukraine's Operation Spider's Web Shows Future of Drone Warfare

Israel Strikes Iran, With Steven Cook

Spectacular Drone Strikes and the Future Sanctuary of the U.S. Homeland

Inside the Situation Room

Resolve in International Politics

The Legitimacy of Drone Warfare: Evaluating Public Perceptions

The Third Drone Age: Visions Out to 2040

Drone Warfare in Waziristan and the New Military Humanism

How the Army Out-Innovated the Islamic State's Drones

ISIS Is Not a Terrorist Group: Why Counterterrorism Won't Stop the Latest Jihadist Threat

The Islamic State and Drones: Supply, Scale, and Future Threats

Mars Adapting: Military Change During War

Pentagon confirms 'incursions' of unauthorized drones over Air Force base
Statement on the Development of the 2025 National Defense Strategy

Joint Chiefs Chairman Caine has an 'algorithm' for US 'winning'

How to Lose the Drone War: American Military Doctrine Is Stifling Innovation

Drones: What Everyone Needs to Know

The role of culture in military innovation studies: Lessons learned from the US Air Force's adoption of the Predator Drone, 1993-1997

The Empirical Determinants of Violent Nonstate Actor Drone Adoption

Drone Games, Terror Drone Diffusion, and Near-Term Threats

Whose "drone revolution"? Expert-media gaps in perceptions of drone warfare

Flying under the radar: A study of public attitudes towards unmanned aerial vehicles

Closing the Counter-Drone Capability Gap

Unmanned Aircraft Systems (UAS)

Most Drones in Controlled Airspace Lack FAA Approval and a Third Fly Too High, Researchers Report

Statement of General Gregory M. Guillot, United States Air Force Commander United States Northern Command and North American Aerospace Defense Command Before the Senate Armed Services Committee Delivery Date 14 March 2024

Crude drone attack hits Mexican govt office in Tijuana, no deaths or injuries

Pentagon warns it's not prepared for homeland drone attack

Unauthorized drone flights pose rising threat to U.S. bases, border, civilian events, senator warns

Army Sec. Dan Driscoll on partnering with the private sector and the surge in defense tech startups

Countering the Swarm: Protecting the Joint Force in the Drone Age

A $2M missile vs. a $2,000 drone: Pentagon worried over cost of Houthi attacks

How to Secure the Sky: America Needs a Defense Against Drones

Unleashing American Drone Dominance

The US Needs Better Ways to Defend Against Drones

S.2296 - National Defense Authorization Act for Fiscal Year 2026

Defending U.S. Military Bases Against Drones? A Recent Tabletop Exercise Explores How

United States Northern Command Assigned as DOD's Lead Synchronizer for Counter Small Unmanned Aircraft Systems Operations in the Continental United States and Alaska

The 9/11 Commission Report

Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands Defense Agency and DoD Field Activity Directors, Subject: Replicator 2 Direction And Execution

Countering Small Drones: Office Works Toward Joint Solutions to Growing Threat

Defending America's Skies: Public Support for Homeland Counter-Drone Operations

Fort Sill's Joint C-sUAS University: Spearheading the charge against drone threats

First-of-its-kind FBI facility opens in Alabama

Memorandum For Senior Pentagon Leadership Commanders of the Combat Ant Commands Defense Agency and Dod Field Activity Directors, Subject: Establishment of Joint Interagency Task Force 401

Hon. Steve Feinberg, Deputy Secretary of War

Cotton, Gillibrand Introduce Bipartisan Bill to Protect Military Installations from Unauthorized Drones

Pentagon leaders host interagency meeting to strengthen US counter-drone cooperation