Brett Feddersen
Vice President for Strategy and Government Affairs
D-Fend Solutions AD, Inc.

BEFORE

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Transportation and Maritime Security

HEARING ENTITLED

Surveillance, Sabotage, and Strikes: Industry Perspectives on How Drone Warfare Abroad Is Transforming Threats at Home

ON

July 8, 2025
Washington, DC

INTRODUCTION

Chairmen Gimenez and Green, Ranking Members McIver and Thompson, and distinguished members of the Subcommittee, thank you for the opportunity to testify before you on matters critically important to the national security and public safety of our country and its citizens.

My name is Brett Feddersen, and I am the Vice President of Strategy and Government Affairs at D-Fend Solutions, the leading counter-drone manufacturer of radio frequency (RF)-cyber takeover solutions for the drone threat, both overseas and in the United States. I also serve as the Chair of the Security Industry Association's (SIA) Drone Security Subcommittee and have been working on the drone and counter-drone problem set since 2008, during my time in the military, as a federal civilian, and in the private sector. Today, I am honored to appear before the Subcommittee representing both D-Fend Solutions and the drone security industry.

Bottom line up front: Drone warfare abroad has evolved rapidly over the past decade, with state and non-state actors fielding drones for surveillance, sabotage, and strikes in theaters from Eastern Europe to the Middle East. Tactics refined in these conflict zones—persistent reconnaissance, weaponized loitering munitions, and saturation swarm attacks—are now manifesting as emerging threats to U.S. homeland and national security.

These threats are here to stay and mean that things like our critical infrastructure—such as power grids, water treatment plants, transportation networks, and communication systems—is increasingly vulnerable to threats from nefarious actors who can exploit drones' capabilities, including surveillance, sabotage, and payload delivery, to conduct physical attacks. Successful drone attacks on critical infrastructure can lead to power outages, transportation disruptions, communication failures, and substantial economic consequences. More concerning is the potential for the loss of human life, for example, a drone using aerosol dispersal or payload delivery over a mass gathering can cause mass panic, causing serious injury or even death to attendees. Confronting this reality requires a proactive and multi-layered homeland defense strategy that includes early detection, safe and effective mitigation technologies, and updated security protocols.

From local football games to open-air shopping centers, large gatherings of Americans are part of our everyday lives and remain incredibly vulnerable to drone-based threats. As the United States prepares to host high-profile, global sporting events like the 2026 FIFA World Cup and the 2028 Olympics, I am grateful that the Committee is closely overseeing the threat environment and preparations for these events and is willing to engage in difficult conversations surrounding our real vulnerability and capability gaps.

Today, I hope to help the Subcommittee better understand how overseas drone operations are transforming domestic risk vectors, the status of U.S. capabilities and legal frameworks, and offer targeted recommendations for Congress to bolster detection, interdiction, and resilience against drone-borne threats in the United States homeland.

MODERN DRONE WARFARE ABROAD AND AT HOME

Drones have transitioned from niche reconnaissance tools to central components of modern warfare. Their wide availability, small size, low cost, and modular payloads make them attractive for intelligence, surveillance, and reconnaissance missions, as well as the destruction of critical infrastructure and the effective delivery of ordnance.

Just weeks ago, the world witnessed a historic shift in small drone warfare. Ukraine's planning and execution of Operation Spider Web has rewritten the rulebook on drone threats: distance, cost, and autonomy no longer constrain adversary reach. Below are key counter-drone lessons drawn from Ukraine's Operation Spider Web—an audacious campaign in which Ukraine struck Russian airbases up to 5,000 km (3,106 miles) from the front using small, commercial AI-enabled drones. This is farther than driving from New York City to Los Angeles.

- *Rear Areas Are Not Safe*
  Ukraine proved that "strategic depth" offers no immunity: drones launched from deep inside friendly territory reached ostensibly secure Russian airfields, destroying billions of dollars' worth of aircraft. Defenders must extend coverage well beyond the frontlines to include logistics hubs, maintenance depots, and forward operating bases.[1]
- *Defense in Depth—Layer Every Segment*
  Traditional point-defense systems (e.g., local radar or a single interceptor battery) were overwhelmed. Operation Spider Web integrated covert logistics, telecom exploitation, and ground infiltration to bypass singular defenses, underscoring the need for a layered approach to counter-drone detection (RF, radar, EO/IR) and mitigation (RF cyber takeover, electronic warfare measures, and directed energy).[2]
- *Resilience to Jamming and GPS Denial*
  Spider Web's drones used dead-reckoning navigation and civilian cellular (SIM-card) links rather than GPS, making them resilient to traditional GNSS jamming. Given this, counter-drone systems should include extensive RF spectrum monitoring, non-GPS-dependent geofencing, and safe mitigation techniques that can detect, take control of, or disrupt alternate control channels

In conflicts outside the U.S., inexpensive, commercially available, and do-it-yourself (DIY) drones have become the weapon of choice. Alarmingly, these same drones are flown across the U.S. every day. There are over one million drones registered with the FAA in the United States—a number that is predicted to grow to 2.7 million by 2027.[3]

The weaponization of private drones in the United States is a significant and growing concern. While drones have beneficial applications in public safety and various industries, their potential for misuse, especially when armed, poses challenges for law enforcement and national security. Battlefield tactics, techniques, and procedures for drones have proliferated through the internet, and the same drones used in combat overseas are available and in use here in the U.S.

During my time at the Federal Aviation Administration (FAA), we received several videos and briefings showcasing drones outfitted with chainsaws, flamethrowers, firearms, and makeshift chemical dispersal systems. We have witnessed rocket-propelled grenades (RPG) warheads and grenades being dropped from simple commercial and do-it-yourself (DIY) drones. Additionally, we have seen drones equipped with modified shotguns used to shoot down other drones.

[1] American University, "Ukraine's Operation Spider Web Upended Traditional Rules of War," June 5, 2025. Benjamin Jensen; chathamhouse.orgamerican.edu
[2] Counter-UAS Hub, "Putting Operation Spider's Web in Context," June 20, 2025, Ben Connable; cuashub.comirregularwarfare.org
[3] FAA, "Drones by the Numbers," updated April 1, 2025, https://www.faa.gov/node/54496; "Drone Operations," Government Accountability Office, https://www.gao.gov/drone-operations.

Key Concerns and Examples of Weaponization:

- *Potential for Malicious Use:* Drones can be easily outfitted with various weapons, including firearms, explosives, incendiary devices, or even chemical or biological agents, posing a risk to individuals, critical infrastructure, and government facilities.
    - *Terrorism:* terrorist organizations can adapt and exploit drone technology to target public spaces and infrastructure, potentially magnifying casualties and damage. Cartels operating in Mexico along the U.S. southern border are already using weaponized drones to drop munition payloads.
    - *Drone swarms:* Coordinated attacks utilizing drone swarms can overwhelm traditional defenses and enhance the effectiveness of sabotage operations.
- *Drone Incursions and Modern Espionage:* There have been numerous drone incursions over sensitive sites, including military bases and critical infrastructure, raising concerns about potential threats. Drones can be used for corporate and foreign espionage, including surveillance of facilities, intimidation through observation, and even cyberattacks by leveraging proximity to networks.
- *Smuggling and Criminal Activity:* Drones are used by criminals for illegal drug shipments, delivery of contraband into prisons, and counter-surveillance of law enforcement.
- *Privacy Concerns:* Drones equipped with cameras and other sensors can be used for unauthorized surveillance and invasion of privacy.
- *Interference with Public Events and Aircraft:* Unauthorized drone flights can disrupt public events and pose a risk to aviation safety, including the potential for collisions with manned aircraft.

Common commercial drones have already been used in attempts to destroy or damage critical infrastructure, and we continue to see variations of weaponized drones attempting to attack the public in the heartland and law enforcement in cities and on the border.

- *2020 Pennsylvania Power Substation Incident:* A modified drone was discovered outside an electrical substation in Pennsylvania. It was equipped with a copper wire, likely intended to create a short circuit and disrupt power. The drone crashed before reaching its target, but it highlights the potential threat.
- *Attempted Attack in Nashville (2024):* A man was arrested in November for planning to use a weapon of mass destruction to attack an energy facility in Nashville. Court documents indicated he planned to use a drone to deliver an explosive.
- *Suspicious Drone Activity near Energy Sites (2024):* In December, multiple energy sites requested temporary flight restrictions due to unusual drone activity in New Jersey, New York, and Maryland. Although the operators weren't identified, this incident reflects the ongoing concern about drone threats.

What is Our Current Airspace Protection Posture?

Over the years, drones have evolved from simple weekend toys to sophisticated tools used for smuggling, corporate espionage, and terrorist surveillance. Unfortunately, federal policies have struggled to keep up with these emerging threats, leaving state, local, tribal, and territorial (SLTT) law enforcement agencies in a challenging position and their constituents unprotected. These agencies and trained security professionals are on the frontlines protecting critical locations—such as stadiums, power plants, and city skylines—but they face legal restrictions that prevent them from effectively addressing drones that pose a danger to these sites and the American public.

As you know, only a few federal law enforcement components in the Department of Homeland Security (DHS), Justice (DOJ), and Defense (DoD)—have explicit legal authority under 6 U.S.C. § 124(n) and 10 U.S.C. § 130(i) to detect and mitigate (or stop) illicit drone activities. Other entities, including state and local police departments and trained security professionals, must rely on federal support or remain powerless, while unidentified drones fly dangerously over parades, concerts, major sporting events, and critical infrastructure. By their own admission, the DOJ and DHS can only respond to less than one percent of the thousands of counter-drone operational requests they receive each year.

According to FAA data and previous DoD testimony, drone incursions have steadily increased since the establishment of federal counter-drone authorities in 2018. First responders report that drones are tailing SWAT teams, dropping contraband into prisons, spying on neighbors, and hovering over chemical plants. While the threat is local, the legal tools remain predominantly federal in nature.

In 2014, while serving as the National Security Council Director for Aviation Security at the White House, we encountered drone incursions on the White House and Capitol campuses. Subsequently, the interagency met to develop a response plan for these "non-traditional aviation threats." As a result of these efforts, the FAA received Congressional direction to begin testing counter-drone technology systems in 2016. In 2017, the Department of Defense was granted additional authorities. In 2018, Congress authorized a five-year pilot program for federal law enforcement as part of the FAA Reauthorization process to provide counter-drone authorities to the Department of Homeland Security (DHS) and the Department of Justice (DOJ). Seven years later, these authorities remain unchanged.

DHS, DOJ, the security industry, and state, local, tribal, and territorial (SLTT) law enforcement agencies and trained security professionals have repeatedly urged Congress to expand authorities to enable air domain awareness and drone protection in American communities and over our critical infrastructure. Unfortunately, those requests have not resulted in any expanded or new authorities, and the limited authorities from 2018 have been periodically renewed only for short periods of time, creating uncertainty for law enforcement and the industry.

LEGISLATIVE RECOMMENDATIONS AND NEXT STEPS

The President's recent executive orders are a good start to address our legislative and regulatory inaction. However, executive action alone is not a permanent shield—it can be revoked by future administrations or challenged in court. Congress must move now to codify SLTT counter-UAS authorities with the same privacy safeguards and oversight as outlined in President Trump's executive orders.

I strongly urge the Subcommittee and full Committee to take bipartisan legislative action now. The industry, public safety professionals, and the American public are calling for three simple actions that can be taken immediately to make Americans and our skies safer.

1. Expand the current 6 U.S.C. §124(n) detection and mitigation authorities to all SLTT-LE and trained security professionals, safeguarding our critical infrastructure, and amend 49 U.S.C. § 14501 to include an explicit "Counter-UAS Exception," authorizing approved non-federal entities to employ safe and effective, non-kinetic mitigation under DHS oversight.
2. Develop, implement, and oversee a counter-drone operator training regime, using a federally accredited curriculum required for all counter-drone operators using approved mitigation

technology; and

3. Provide dedicated funding programs that enable critical infrastructure operators to procure, train, deploy, and operate counter-drone systems deemed safe and effective by the federal government.

CONCLUSION

The tactics developed in overseas drone conflicts—such as persistent surveillance, sabotage using payload delivery, loitering munitions, and swarm saturation strikes—are now poised to harm us at home. The increasing number of drone incursions into sensitive airspace we've seen in recent years should serve as a loud and distinct alarm bell, warning us of the immediate necessity for deploying safe and effective counter-drone technology to enable rapid response capabilities. While the industry has developed effective detection, identification, and mitigation solutions, challenges such as legal uncertainties, regulatory delays, and funding shortages are hindering nationwide implementation. To address these issues, Congress should clarify its legal authorities, streamline the approval process, and establish dedicated funding. This will enable U.S. stakeholders to effectively deter and counter drone-related threats before they reach our shores. Now is the time to strengthen our defenses in the skies before tomorrow's headlines report the first successful drone strike on U.S. soil.

Thank you for your leadership and the opportunity to appear before you today. I look forward to answering any questions you may have.

Figure 1
Drone Threat Progression Abroad and in the Homeland