GAO | Science, Technology Assessment, and Analytics

SCIENCE & TECH SPOTLIGHT:

COUNTER-DRONE TECHNOLOGIES

Accessible Version

MARCH 2022

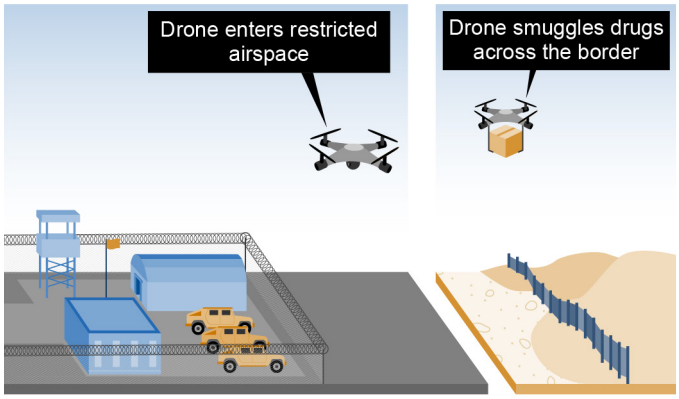
WHY THIS MATTERS

Uncrewed aircraft systems, or "drones," can pose safety and security risks to critical U.S. sites and may be used for smuggling or other criminal activity. With over 2 million drones projected in the U.S. by 2024, these risks are likely to grow. Detection and mitigation technologies could counter these risks, but may face challenges around effectiveness and unintended impacts.

/// THE TECHNOLOGY

What is it? Uncrewed aircraft systems (UAS), or "drones," have a variety of uses, such as photography, delivering packages, and monitoring crops. However, UAS can also pose significant safety and security risks if they enter airspace around critical U.S. sites without authorization or if used for illegal activities. To reduce these risks, counter-UAS technology can detect such unauthorized or unsafe UAS and, when needed, jam, capture, or disable them.

Several UAS incidents have been reported in the U.S. For example, in January 2019, Newark Liberty International Airport halted all landings and diverted planes for over an hour after a potential UAS sighting nearby. Furthermore, smugglers have used UAS to deliver illegal drugs into the country (see fig. 1).



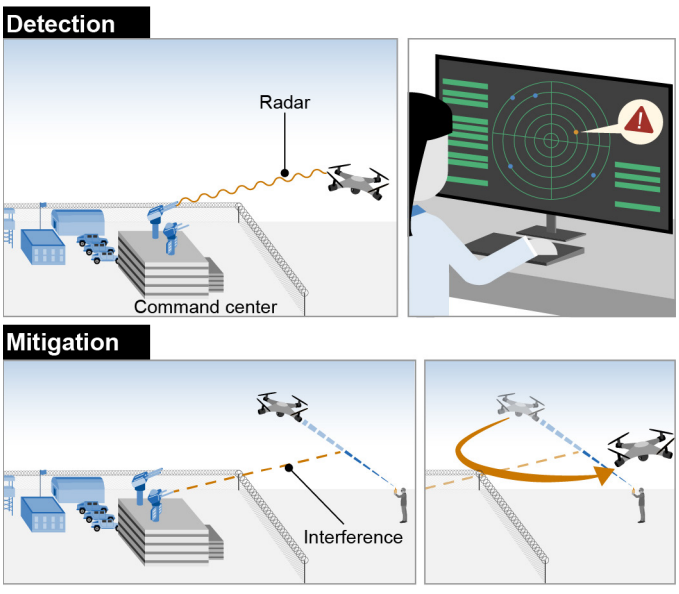
Source: GAO. | GAO-22-105705

Figure 1. Some of the risks posed by uncrewed aircraft systems.

Reported incidents like these may increase as the use of UAS increases. The Federal Aviation Administration (FAA) has forecast that by 2024, the commercial UAS fleet will reach around 828,000, and the recreational fleet will number around 1.48 million.

Domestically, counter-UAS activities may be restricted or prohibited by existing federal laws such as the Aircraft Sabotage Act or the Computer Fraud and Abuse Act. However, four federal agencies—the Departments of Defense, Energy, Justice, and Homeland Security—have been authorized to deploy counter-UAS technologies under certain circumstances, such as to protect sensitive government facilities, including domestic military bases and prisons, or to provide security during sports championships.

How does it work? Counter-UAS technologies generally fall into two categories: detection and mitigation. Detection technologies include infrared devices to track heat signatures, radio frequency systems to scan for control signals, and acoustic methods to recognize the unique sounds produced by UAS motors. According to a 2019 Bard College report, radio frequency and radar systems are the most common detection technologies (see fig. 2).



Source: GAO. | GAO-22-105705

Figure 2. In this example, a critical site detects an unauthorized UAS nearby. An interference signal jams the connection between the UAS and its operator to reroute the UAS away from the site.

Mitigation technologies can repel or intercept an unauthorized UAS. For example, interference signals can jam or break the communications connection between the UAS and its operator, which can trigger the UAS to land or return to its operator. According to the Bard College report, jamming is the most common mitigation technology. Other mitigation technologies can use a net or kinetic force (such as lasers or projectiles) to disable or destroy the UAS. However, kinetic methods can be problematic because a falling or exploding UAS may cause unintended damage.

How mature is it? Although the Department of Defense has used counter-UAS technology abroad since at least 2014, domestic use has been limited. Over the last 4 years, the authorized agencies have deployed some counter-UAS technologies domestically. However, some of

these technologies have limited ability to detect and track small UAS (less than 55 pounds). Furthermore, few can successfully jam or disable a UAS, and many of those that can are only effective at around 1,000 feet or less.

To counter UAS risks, the FAA (which has been authorized to conduct limited testing activities) and the authorized agencies are continuing to test, evaluate, and develop integrated counter-UAS platforms. These platforms' capabilities are designed to address specific risk environments. For example, a powerful long-range signal jammer may be effective at mitigating UAS in rural locations, like near some domestic military bases, but this same technology could also disrupt legitimate and vital communications if used in a city or near an airport.

UAS technology continues to advance and become more accessible to the public. For example, UAS have become smaller and more maneuverable, making detection and mitigation more challenging. To stay effective, counter-UAS technology will need to adapt to such changes.

/// OPPORTUNITIES

- **Enhanced security.** UAS have interfered with military and commercial aircraft operations, entered airspace over large sporting events, illegally accessed wireless networks, and been sighted over sensitive national security facilities. Counter-UAS technologies could address such threats to critical sites and assets.
- **Better situational awareness.** Counter-UAS platforms could allow tracking of UAS activity near critical sites and allow data analysis over time or locations to better understand the threat.

/// CHALLENGES

- **Effectiveness.** Electromagnetic interference (e.g., power lines and LEDs) and small airborne objects (e.g., birds) can decrease detection capabilities or generate false detections. Mitigation systems may have a limited effective range or have difficulty against UAS that are quick or move in unpredictable patterns.
- **Unintended effects.** Counter-UAS platforms may pose safety hazards by interfering with nearby communications, such as devices that use navigation systems. For kinetic mitigation, errant projectiles or falling UAS could damage property or injure people on the ground.
- **Limited number of authorized agencies.** As of March 2022, only four federal agencies are authorized to conduct counter-UAS operations under certain circumstances, and no state or local agencies (or individuals) have such specific federal authorization. According to the Bard College report, local agencies generally rely on a small number of federal counter-UAS units to respond to and protect against UAS threats in their area.
- **Privacy concerns.** Counter-UAS detection methods could collect personally identifiable information, such as information about the operators or camera images of bystanders.

/// POLICY CONTEXT AND QUESTIONS

With increased use of UAS and, along with it, increased demand for counter-UAS technologies, key questions for policymakers include:

- What research and development might lead to innovative counter-UAS solutions that can more effectively address UAS safety and security risks while minimizing unintended effects on airspace or the public?
- What are the potential trade-offs if policymakers consider authorizing the use of counter-UAS by others, including state and local law enforcement agencies, and expanding the use of these technologies?
- If policymakers consider expanding authorization, what is the appropriate level of jurisdictional coordination and regulatory oversight for the use of these technologies among federal agencies and others?

/// SELECTED GAO WORK

- See GAO's "Uncrewed Aircraft Systems" issue area website for additional information and products, Washington, D.C., 2022.
- Unmanned Aircraft Systems: Current Jurisdictional, Property, and Privacy Legal Issues Regarding the Commercial and Recreational Use of Drones, B-330570, Washington, D.C., 2020.

/// SELECTED REFERENCES

Michel, Arthur H. *Counter-Drone Systems*, 2nd ed. Annandale-on-Hudson, N.Y.: The Center for the Study of the Drone at Bard College, December 2019.

Federal Aviation Administration, Department of Justice, Federal Communications Commission, and Department of Homeland Security. *Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems*, 9.95.300-UAS. Washington, D.C.: August 2020.

GAO SUPPORT:

GAO meets congressional information needs in several ways, including by providing oversight, insight, and foresight on science and technology issues. GAO staff are available to brief on completed bodies of work or specific reports and answer follow-up questions. GAO also provides targeted assistance on specific science and technology topics to support congressional oversight activities and provide advice on legislative proposals.

For more information, contact: Brian Bothwell at (202) 512-6888 or BothwellB@gao.gov.

Staff Acknowledgments: Katrina Pekar-Carpenter (Assistant Director), Rah Cantatore (Analyst-in-Charge), Anna Beischer, Maggie Bryson, Richard Hung, Anika McMillon, and Ben Shouse.