THE WASHINGTON INSTITUTE for Near East Policy

PolicyWatch 3045

Counter-Drone Capabilities in the Middle East and Beyond: A Primer

Arthur Holland Michel

December 3, 2018

Despite growing interest and investment, countering unmanned aircraft remains a significant challenge given the nature of the threat, the rapid evolution of drone technology, and the dynamic nature of modern warfare.

This PolicyWatch is adapted from the author’s February 2018 monograph “Counter-Drone Systems.” The full report can be accessed here.

Drones are operated by numerous state and nonstate actors in the Middle East. Small commercially available drones, in particular, have been used extensively and to profound effect in the ongoing conflicts in Syria, Iraq, Gaza, and Yemen. Given the rapidly expanding use of small drones in conflicts around the globe, especially among nonstate groups and criminal organizations, counter-drone or counter-unmanned aerial system (C-UAS) technology—devices used to detect and/or intercept such aircraft—has received considerable attention of late, and is now adopted widely. Yet this emerging field still faces a number of critical issues.

While large unmanned aircraft can generally be countered using traditional antiaircraft technologies, the challenges in countering small drones are manifold. They can be difficult to spot with the naked eye from even short distances and are generally undetectable with air defense radars that were originally designed with large, fast aircraft in mind. Even when certain traditional antiaircraft systems are effective against small drones, their high cost—compared to the very low cost of the intruding unmanned aircraft—makes them an unsustainable solution. For instance, a single Patriot missile costs as much as $1 million while a small commercial drone as little as $500.

Over 200 C-UAS products are available on the market today and, according to an analysis by Center for the Study of the Drone co-director Dan Gettinger, counter-drone technology acquisition and development is the fastest-growing drone-related spending category in the most recent U.S. Defense Department budget. On the battlefield, C-UAS technologies are most commonly used for base and vessel protection, and there is growing interest in portable and mobile systems that could be used to protect ground units and convoys. Current civilian uses include airspace protection at airports, security for large public events, VIP protection, and counter-smuggling at prisons, as well as, increasingly, sensitive facility defense, port and maritime security, and personal security.

CAPABILITIES AND CHALLENGES OF C-UAS

Counter-drone technologies currently in use and development employ an impressive variety of detection and interception techniques. For instance, detection and tracking elements may rely on radar, radio frequency (RF) monitoring, electro-optical (EO) cameras, infrared (IR) sensors, acoustic sensors that recognize the distinct sound emitted by common drones, or, quite often, a combination thereof. Similarly, methods of interdiction include radio-link jamming, GPS jamming, spoofing (a technique for taking control of a drone by hijacking its communications link), lasers, electromagnetic pulses, nets or other entanglement systems, kinetic projectiles, and, again, a combination of methods. These systems may be ground-based, portable/hand-held, or, in some cases, mounted on drones that attack the intruding vehicle in the fashion of a World War I dogfighting plane.

Despite these many capabilities, C-UAS technology is still by no means an entirely equal match for the threat of small unmanned aircraft. Moving forward, the field must yet overcome a host of significant challenges.

Detection effectiveness. No single existing C-UAS detection technique is capable of detecting and tracking all types of drones under all conditions. EO systems can only operate during the daytime. Both EO and IR systems, as well as certain RF systems, must have a direct line of sight to the target, meaning that if an intruding drone passes behind a building, the countermeasure may no longer be able to detect and track it. Radars designed to detect objects with the small, low, and slow profile of the average consumer drone may not be able to distinguish between a drone and, say, a bird. Acoustic sensors will only recognize sounds that match the engine noises emitted by known drone models. They might, therefore, be deaf to new or uncommon drones that are not included in the system’s internal library, or that have been modified. Meanwhile, RF systems may likewise detect only those aircraft operating within known drone frequency bands. Given the rapid growth of the commercial drone industry, these library-based systems require regular updating to account for new models that enter the market.

False returns. C-UAS detection systems must generate low levels of false negatives and false positives. This means that they must be sensitive enough to detect all drones operating within the area of operation, but not so sensitive to create an overwhelming number of false positives by characterizing every bird, plane, and cloud as a security threat. Given the wide variety of drones in use and the limitations of detection systems listed above, achieving this balance is very difficult.

Distinguishing legitimate drone use. In future operating environments, C-UAS systems may need to differentiate between friendly and adversarial drones. This will be the case in both peacetime and wartime environments: say, a sporting event where the airspace may be crowded with aerial cinematography drones that are not a security risk, or a battlefield where C-UAS users must avoid shooting down friendly drones that are also operating in the area. At present, no commercially available counter-drone systems have proven capable of automatically differentiating between peaceful and malicious drones.

Interdiction hazards. Drones intercepted by physical means—for example, by a laser or projectile—can fall to the ground at speed. Even certain net-based systems that use parachutes to bring down ensnared drones in a controlled manner could pose a hazard to those on the ground if the parachute fails or if the drone carries an explosive payload. For this reason, kinetic C-UAS techniques may not be viable for use in crowded areas, such as sporting events or urban environments. Jamming systems, while not a physical hazard, can nevertheless interfere with legitimate communications in the vicinity of C-UAS operations (this is why signal jammers are illegal in the United States and many other countries).

Counter-countermeasures. Non-kinetic means may also be problematic for different reasons. RF jamming systems disrupt the drone's communications with the operator, but many drones can be programmed to operate without an RF link. A variety of both military and commercial groups are developing drones that can operate in GPS-denied environments, and such systems would be resilient to GPS jamming. Spoofing, meanwhile, may be ineffective against drones with hardened communications, as well as those with communications protocols that the spoofing software has not been designed to address.

General effectiveness. As is often the case with emerging complex technologies, many C-UAS systems are not as effective as advertised. For example, at a five-day counter-drone exercise organized by the Pentagon in 2017, a variety of established defense firms and startups tested their C-UAS products on drones operating at a distance of roughly 200 meters. Afterward, the event organizers reported that the drones were, in general, "very resilient against damage" and concluded that most of the counter-drone systems needed further development. In real operations, too, C-UAS products have failed to perform; for example, a number of drones appear to have bypassed the eight counter-drone systems deployed at the 2016 Rio Olympics, including during the opening ceremony. The continuous evolution of commercially available drones also poses a challenge, since drones will increasingly take new forms and employ new communications, navigation, and power systems that might be impervious to existing detection or interdiction techniques.

Lack of standards. No international standards exist for the design and use of C-UAS technology. This means there may be significant variance between the performance, reliability, and safety of systems that might appear similar on paper. At best, a malfunctioning or ineffective system is simply a waste of resources. At worst, and particularly in civilian environments, such a counter-drone system might present a public safety threat (e.g., a directed jamming system that interferes with emergency radio communications, or a kinetic system that misses its intended target).

Legal issues. In the United States and some other countries, countermeasures against drones—such as spoofing, interdiction by jamming, and detecting/tracking by downloading information about the aircraft's location and telemetry—may be restricted or prohibited by law. Kinetic and nonkinetic systems may also violate the U.S. Aircraft Sabotage Act, which imposes heavy fines and even prison sentences for anybody who willfully "sets fire to, damages, destroys, disables, or wrecks any aircraft" in U.S. airspace.

"OLD FASHIONED" C-UAS TECHNIQUES

In recent years, various weapons technologies that were not originally designed for C-UAS can and have been used against small unmanned aircraft. On several occasions in the past decade, Israel has used missiles launched from helicopter gunships and fighter aircraft, as well as U.S.-made Patriot surface-to-air missiles (which are designed to shoot down aircraft and missiles), to interdict Hezbollah, Syrian, and Iranian drones flying over its airspace, albeit with mixed success (and, as stated above, with a high cost). Russian forces, meanwhile, have used the Pantsir air defense system and electronic jammers to down or disable drones engaged in attacks on its military installations in Syria. Moreover, twice in 2017, U.S. F-15 fighters shot down Iranian-made Shahed 129 drones operating near coalition forces in Syria.

Given that certain traditional antiaircraft systems can, in some cases, achieve a measure of effectiveness against commercial drones, a number of firms are marketing such products for counter-drone use. For example, Raytheon claims that its C-RAM air defense system, traditionally used to defend against mortars and rockets, is equally effective against slow-moving unmanned aircraft. In 2016, the U.S. Army awarded Lockheed Martin $27.8 million to tweak its existing AN/TPQ-53 radar to detect drones. And at a 2017 demonstration in the Persian Gulf, the U.S. Navy Laser Weapon System, which was designed to defend ships against a range of threats, shot down a target drone; it is now generally seen as a potentially viable option for protecting against small unmanned aircraft.

As commercial unmanned aircraft continue to proliferate, the demand for C-UAS systems will only grow in the coming years, and continued investment in the field will seek to address many of the limitations listed above. However, by the same token, coming advances in communications, precision guidance systems, automation, and sensor capability will make the unmanned threat more formidable, enabling even small nonstate groups to potentially carry out sophisticated reconnaissance, surveillance, and strike operations, in addition to swarming tactics to overwhelm enemy defenses. It remains to be seen, then, whether C-UAS capabilities will keep up with this evolving threat.

Arthur Holland Michel is codirector of the Center for the Study of the Drone at Bard College, an inquiry-driven education and research institute founded in 2012.