A Quick Guide on Mobile Drone Detection

Things to Consider When Evaluating Technologies

BY
Linda Ziemba, Founder, CEO, AeroDefense

THE DRONE—A DOUBLE-EDGED SWORD. THE EERIE THING ABOUT THAT PHRASE IN THIS CONTEXT IS THE CENTRAL INTELLIGENCE AGENCY HAS ACTUALLY CREATED AND USED A MISSILE WITH SWORD-LIKE BLADES FOR HIGHLY ACCURATE DRONE STRIKES.

While these missiles are military grade and quite a bit larger than hobby drones, there have been several examples in recent history of weapons being attached to hobby drones. In September 2019, for instance, a Pennsylvania man dropped explosive devices onto his ex-girlfriend's property using a drone. There are even flamethrower drone attachments for sale on the Internet today.

More constructively, law enforcement uses drones for good intents, such as to search for missing persons, deliver vital health supplies, drop life jackets and water to stranded boaters, and process crime scenes, among other things. According to the Center for The Study of The Drone at Bard College, in March 2020, 1,103 law enforcement agencies were using drones in some capacity. This is 70 percent of the total use by law enforcement, fire and rescue, and emergency management combined.

Drones have practical uses within many industries, not just law enforcement. Most notably, drones are used for videography, real estate, infrastructure inspections, and crop and field management. It is important to differentiate between beneficial, clueless or careless, and criminal drone use.

It's no secret that any commercial drone pilot in the United States is required to follow federal and state regulations, and law enforcement agencies must stay abreast of any changes in drone laws or regulations. The hobbyist pilots who are still clueless or careless are the ones to worry about. Just to name a few of many examples, hobbyists have unintentionally disrupted first responder

operations, delayed flights, and crashed into buildings. To add another threat layer, bad actors who don't care about the laws at all have found many ways to exploit drone technology, and their plots seem to become more sophisticated as the technology progresses.

Fixed drone detection systems have been around for a while and help mitigate the threats careless hobbyists and bad actors pose. When a law enforcement agency chooses a system that is right for its environment and legal tolerance, a drone detection system can provide actionable intelligence for response teams and the chance to stop attacks before they happen.

MOBILE DRONE DETECTION ARRIVES ON THE SCENE

Mobile drone detection systems are relatively new to the market. The concept is simple—situational awareness of the airspace around a location wherever it's needed. But mobile systems are not just drone detection systems that are installed temporarily at a location and then moved to another. Drone incidents could happen where not expected, so users may need to detect drones from a vehicle or marine vessel in motion or expand the range of a fixed deployment.

One thing is clear: mobile drone detection is incredibly useful for law enforcement agencies as locations of their operations are fluid. What's not so clear is what the best mobile drone detection system looks like. Large defense companies have created versions for military use, but law enforcement agencies don't have the same budget or mitigation options.

DETECTION SYSTEM CONSIDERATIONS

There are a few key factors to consider when procuring a mobile drone detection system that is best suited to an agency's needs.

LEGALITY

With any type of drone detection system, whether fixed or mobile, it's important for a public safety or private entity to fully understand the legalities of the technology they are seeking to use. There are several federal agencies that forbid certain drone mitigation activities.

The Department of Defense, Department of Energy, Department of Homeland Security, and Department of Justice are the only entities allowed to affect the flight of a drone according to the Federal Aviation Administration (FAA), Department of Transportation (DOT), and Federal Communications Commission (FCC). This includes signal jamming—the FCC prohibits jamming signals unless it is conducted under a strict set of legal parameters.

Many people outside of these government agencies think physical mitigation is the best defense against drones. However, even it were legal to affect drone flights, consider the following. How would one be alerted to a drone or pilot's presence? What happens to the shot that misses? What if the pilot sets the return-to-home coordinates to be a malicious target if the signal is jammed? Taking a drone down can create a more dangerous situation than the drone itself, and the person or agency who takes it down may be responsible for the damages caused by the crash.

As far as privacy is concerned, the FCC and DOJ have specific regulations that make it illegal for drone detection systems to extract *any* information from the drone communication channel. The National Telecommunications and Information Administration treats drones like flying computers and prohibits hacking and "spoofing." However, many drone detection systems on the market today blatantly go against these laws or try to quietly tiptoe around them. Potential users should be concerned about what other information the system is collecting if it is in fact demodulating or decoding electronic communications signals in any way.

Ronald Leach, former unmanned aircraft systems program coordinator for the New Jersey State Police and current principal at Leach Strategic Partners and vice chairman of the Urban Low Altitude Transport Association, echoes the importance of these regulations:

> *There is no asking for forgiveness when a law is broken, no matter how well-intentioned the action taken. The exposure to violating Federal, State, or local laws may have the opposite effect on the outcome, not to mention the liability factor. Locating the UAS operator is currently the best way to reduce non-cooperative UAS incidents related to "Clueless," "Careless" and possibly "Criminal" operators.*

DRONE DETECTION SENSOR TYPE

There are four different sensor types: radio frequency (RF), radar, acoustic, and camera/infrared. Acoustic and camera/infrared systems need additional data from other sensor types in order to accurately detect drone threats with a low false alarm rate and shouldn't be used as standalone systems. Each sensor type has advantages and disadvantages, as detailed in Table 1.

SIZE, POWER, AND NETWORK REQUIREMENTS

Vendors have brought several different versions of mobile drone detection systems to the market. Many of them are cost prohibitive for law enforcement agencies, requiring a vehicle or some other large hardware purchase. Large hardware becomes an issue with temporary deployments in an urban environment where RF traffic is very high and surrounding buildings form urban canyons that create multipath issues. RF-based drone detection sensors should be placed above obstructions and away from heavy RF traffic if possible. This requires permission of building owners to place

TABLE 1: SENSOR TYPE PROS AND CONS

SENSOR TYPE	PROS	CONS
RADIO FREQUENCY (RF)	• Only solution that can detect both drone and controller • Does not require line of sight • Can detect a drone and controller as soon as they are turned on and connected	• Must be configured to filter out ambient RF signals • Varied location accuracy depending on the environment • Performance degradation in heavy RF environments
RADAR	• Very long range • Provides altitude	• Detects anything that moves, therefore, has a high false positive rate in a busy urban environment • Cannot detect until a drone is in flight • Cannot detect a controller • Actively transmits a signal, which could be inappropriate for some environments
ACOUSTIC	• Does not require line of sight	• Must be combined with another detection method • High false positive rate in busy urban environments • Very short range • Cannot detect a controller
CAMERA/INFRARED	• Easily captures visual evidence	• Requires line of sight • Must be combined with another detection method to guide camera angle

sensors on their rooftops. If the sensor equipment is bulky, building owners may be hesitant to bring unwanted attention to their building as a potential target. Additionally, large hardware can be difficult to move from location to location.

With large size usually comes large power consumption. Agencies need to keep in mind how the power requirements for the sensor will fit into their infrastructure. Will this system integrate into an existing response vehicle like a police cruiser or will it need to go into a command center–style vehicle? Will the power requirements of the system fit into that platform without additional power supply or generators?

Networking will be required for the system to function. Find out if the system will be available only within the platform where the system is installed or if it can be monitored remotely. If the system is functioning on an LTE network, consider the likely use cases and whether LTE coverage is always available. With a temporary deployment, operators may be able to use point-to-point or local network infrastructure instead of LTE. If the agency's command center vehicle already has its own network infrastructure, be sure the drone detection system can work within that network. Another question to ask is whether the system has networking redundancies or if it can function offline.

STOP THE ATTACK BEFORE IT HAPPENS

Nefarious actors will often test flight paths and security team response to drone incursions before the real attack. Law enforcement must protect outdoor events that draw large crowds where public safety is always a top priority. There may be an opportunity to stop an attack before it happens with a mobile drone detection system. The system can alert response teams to a drone being flown in the area. It's important to note that not all systems on the market are able to accurately locate both the drone and the controller (pilot), and very few can locate them simultaneously.

There is a lot to consider when evaluating any drone detection system, whether fixed or mobile, and no solution is a silver bullet. However, knowing the right questions to ask ensures the best result. Agencies considering these systems should seek vendors who are transparent and take the time to determine whether their solutions are a fit for the agency's uses.