Barriers to the Implementation of Counter UAS Operations

By 34 North Drones LLC

It is generally agreed that counter drone operations are comprised of two phases. They are: 1. Detection, and; 2. Mitigation or neutralization. Technological and legal barriers exist for both as concerns private, commercial and governmental agencies. Statutory exemptions exist for select federal organizations. This article will primarily address non-military or domestic counter UAS (cUAS) operations.

Detection of Unmanned Aerial Vehicles

There are a number of methods that utilize technology in order to detect airborne small unmanned aircraft.

1. Radar
2. Electro-optical/Infrared visualization (EO/IR)
3. Radio frequency (RF) detection or sourcing
4. Acoustic or “listening” devices

Radar or radio detection and ranging utilizes radio transmissions and the return of deflected radio waves to detect the presence, range and speed of an object. Radar is considered a primary drone detection method. Specialized radar configurations are implemented for low altitude flying objects and in some cases the genesis of these systems are from military technology involving the detection of artillery, rockets and mortar fire.
These specialized radar systems are designed to track smaller objects and can offer a lower altitude azimuth profile with lower power transmission levels with some advanced systems being capable of full integration into longer range Air Traffic Control (ATC) radar systems. Because of the tuning of these specialized radars they may track larger aircraft at a distance as they appear to the system as being small objects.

Radar like all active detection radio frequency (RF) equipment requires unobstructed line of sight from the transmission source to the target and back to the source to be effective. Manned aircraft pilots will usually hear the transmission from ATC of “Radar contact lost.” when at very low altitudes or when flying below higher terrain which is between their aircraft and the radar source. These radar systems may have difficulty tracking hovering drones or drones that are tracking vertically. Radar provides 360 degree situational awareness and excellent early detection capabilities. Radar detects objects and not radio frequencies. Radio frequencies may or may not be emitted from a UAS as further discussed below.

Electro-optical and infrared (EO/IR) systems can be used as a stand alone system or as an integrated and validating component of a radar system to confirm that a target is not a “ghost”, artifact or bird. These systems are also valuable in providing visual separation of objects with a low radar signature from the background radar clutter of terrain which is behind and rises above the target. An available feature is that the optics can be made to “slew to cue” which causes the optics to automatically track the object identified by the radar system. The name EO/IR is descriptive as it is a dual optical system employing optical and thermal sensors designed for long range visual acquisitions day or night. This system configuration is common on military vehicles and platforms and can be easily identified on the nose of certain military helicopters.
These systems can be distracted on occasion in the event an object crosses the field of view of the optics. These systems are also capable of machine learning so as to identify the type of drone being visualized provided that the dimensions of the drone’s configuration has been added to the database within the software.

As with any optical or image capturing device quality is important and, in the case of drone detection, quality is critical. The FAA describes Pixels Per Foot (PPF) as a more predictable level of image quality. PPF is based on the area of coverage that the image captures, the distance from the camera, focal length and resolution of the camera.

Radio frequency (RF) detection systems detect frequency links being exchanged between the remote control device that commands the movement and features of the drone and the drone. The remote control link is also capable of receiving and displaying RF transmitted video and still imagery to a screen connected to the remote control device which is likewise detectable by RF systems. Depending on the software utilized these systems are able to determine the manufacturer of the targeted drone depending on the radio frequency data captured.

Much like radar systems these systems require unobstructed line of sight transmission reception for accuracy. Unlike radar systems these systems are susceptible to electromagnetic frequency disruption and environmental interference. Certain environments have a great number of potential sources of interference. Airports, busy marine terminals and metropolitan areas all have a very broad spectrum of radio frequencies being used.
There may be installations that emit byproduct interference such as high voltage power lines, generators, electrical motors and lighting fixtures or actual transmission fixtures or devices that emit interference such as transmission antennas, microwave towers, WiFi, cellular service and two way radio traffic. As any drone pilot will tell you, if there is significant interference in the area of operations that you are flying, your RF range to control the drone will be a fraction of the range the drone is capable of in normal conditions. The same holds true for RF detection systems.

A concern when performing GPS precision mapping is the issue of bouncing GPS signals off large objects. This is called multipathing and it causes inaccurate measurements or points. This phenomena also occurs with RF detection devices when the RF bounces off a building or large aircraft at an airport. An additional concern is the coverage area of RF devices as large areas require a number of sensors and in some instances multiple sensors confuse the location of the interloping drone.

The FAA by letter of July 19, 2018 describes a ten month study at four metropolitan airports with partners DHS, DoD, DOJ and others wherein the following determinations were made:

“The low technical readiness of the systems, combined with a multitude of other factors such as geography, interference… demonstrate this technology is not ready for use in domestic civilian airport environments… some of the FAA’s significant findings and recommendations include- Airport environments have numerous sources of potential interference- more than anticipated. High radio spectrum congestion in these environments made detection more difficult and, in some cases impossible… Certain aircraft [drones] operational states (e.g., hovering) and the degree of autonomy also limits detection… costs are prohibitive where higher levels of coverage are required…”

Copyright © 2019 34 North Drones LLC. All rights reserved.
“... An additional and critical component of this finding is that technology rapidly becomes obsolete upon installation as UAS technology is rapidly changing... Further the FAA does not endorse or advocate for the use of countermeasures in the airport environment given the likely impact on safety... successful mitigation is reliant on successful detection.”

Some questions presented by the FAA are: “Does the detection system depend on a library of known RF signatures? If yes, how often is the library updated? What is the process to update the library? Is there an ongoing cost for library updates?”

Most RF frequency detectors only detect common, known and legal frequencies utilized commercially by drone and RC hobbyist manufacturers. What is known is in the vast majority of incursions, off the shelf drones have been used thus facilitating detection as those frequencies are likely in a library of “known RF frequencies”. Presently, off the shelf hardware components and open source software are available for an individual to design and construct a small or heavy lift “homemade” drone. A sophisticated bad actor will utilize an unexpected (and likely illegal) radio frequency in which case there will be little to no chance of detection. There are perhaps hundreds if not thousands of radio frequencies that can be used to control a drone. Although the FAA is presently developing rules requiring drone manufacturers to implement Radio Frequency Identification (RFID) for drones, there will still be a vast number of previously manufactured drones without RFID and bad actors will not incorporate RFID into homemade drones.

If a drone is programmed to fly autonomously without control input from a remote controller there may be no frequencies for an RF detector to detect. It will simply fly to the GPS/GLONASS waypoint(s) as programmed.
The attempted jamming of the GPS/GLONASS signals will likely not be effective if the drone is equipped with an Inertial Navigation System (INS) that does not require or rely on GPS/GLONASS signals to navigate. INS systems which are sometimes referred to as IMUs use gyroscopes and accelerometers along with a computer to keep track of a vehicle’s orientation using a starting point, velocity and time. Small and light INS systems called Microelectricalmechanical systems (MEMs) are currently in use in drones, although they come at a high price tag. MEM’s typically use algorithms and GPS/GLONASS signals for drift correction. INS systems have been historically used on aircraft, ships, guided missiles and spacecraft.

RF detection systems may not be presently suitable in areas of high electromagnetic interference as suggested by the FAA. They are nonetheless a very effective and valuable tool in the vast majority of areas with reliable early detection capabilities. Due to their portability, affordability and rapid set up time they are the only option in a number scenarios.

Acoustic detection is another method of detection whereby listening devices detect a drone’s acoustic signature that has previously been loaded into a library or database. This system can serve as a validation tool. A basic acoustic system will not give an operator time, direction, speed or distance as the system provides an acoustic presence near a sensor. As with radar systems, no radio signals need be detected. Depending on a person or asset’s distance from the outer perimeter and numerosity of the acoustic sensors, ample warning can be given if the drone is in close enough proximity to be identified by the sensor. As the system is subject to picking up sound, the most effective areas of deployment are areas with little to no background noise. Wind, rain and other environmental sounds caused by these conditions could cause sonic interference.
Two important questions presented by the FAA are: “Does the system differentiate and track multiple simultaneous targets? If so, what is the upper limit on the number of targets it can track?” Depending on the technology deployed a number of systems can “track” multiple targets with a finite number. If there is a “swarm” of incoming drones, radar appears to be the most capable detection device.

Integration of different detection systems creates redundancy and validation combined into a single interface. The integration of systems can be performed by a single manufacturer or by the combination of systems designed and built by different manufacturers.

Mitigation or Neutralization of Drone Threats

Methods of mitigation or neutralization:

1. Electronic jamming or spoofing of a drone’s radio control frequencies or navigational GPS/GLONASS signals
2. Concealment, visual obstruction or distraction
3. Net systems (aerial and ground based)
4. Birds of prey
5. Ballistic or kinetic systems
6. Directed energy weapons (lasers and microwave)

After successful detection the measures that can be taken is dependent on what federal laws and local laws are applicable to the person or organization seeking to mitigate or neutralize the drone threat.

Currently the DHS, DoD, DOJ, USCG and DOE are authorized under federal statute to use any means necessary to deter a drone on up to: “Reasonable force, if necessary, to disable, damage or destroy the unmanned aircraft system or unmanned aircraft.”
Except for the specifically named federal agencies, all others including private citizens, local and state public safety and non-enumerated federal agencies are restricted from using most active countermeasures.

The jamming, spoofing or interference with drone transmissions or GPS/GLONASS signals could violate several federal criminal law statutes and FCC regulations including the prohibitions against the use of unlicensed RF jammers, interference with: radio communications, the operations of aircraft, satellite communications and statutes regarding wiretapping and computer fraud. Civil liability may attach to an operator using active countermeasure causing an aircraft to descend to earth uncontrolled causing injury or damage to persons or property. These laws arise, in part, because of the proclivity of jamming equipment to cause unintentional Electromagnetic Interference (EMI) of radio communications, GPS signals, aircraft navigation signals, WiFi signals, cellular signals, infrastructure communication links and emergency communications. Most jamming devices developed for domestic use are directional and are of limited power output and range unlike military applications. Hand held targeting and range effectiveness is not optimal.

Some detection systems have active countermeasures available as an optional capability. As mentioned above, only certain agencies are legally authorized to use these countermeasures. The only “countermeasures” available to all others is more in the form of mitigation. A question presented by the FAA is: “Can the system detect and geolocate the UAS pilot-in-command (using RF)?” After the threat is identified, involved personnel could be directed to the perceived takeoff point to locate the drone operator. This countermeasure would be the optimal solution for local and state public safety in view of the legal restrictions currently in place. Private citizens and business interests could mitigate privacy issues and proprietary exposure by concealment, visual obstructions or distraction.
Netting systems much like the casting of a fisherman’s net have been developed to either ensnare the offending drone causing it to crash or to catch and retain the offending drone by ensnaring it with a net system tethered to a larger drone. Some ground based systems will use compressed air to cannon launch a net system to ensnare a drone. The problem with airborne net systems is the size and speed necessary of the interceptor drone in order to catch and then carry an offending drone. The pilot of any such interceptor drone must possess considerable skill to catch a maneuvering target drone. Ground based cannon launch systems may be limited by range and an arching trajectory.

Ballistic and kinetic systems may involve gunfire, shotguns or another aerial vehicle being set on a collision course against the offending drone. Firearms, long gun fire and kinetic countermeasures could violate criminal statutes prohibiting the destruction of aircraft or statutes prohibiting the discharge of weapons in certain geographic areas. Discharged rounds could return to earth causing injury or death to persons or damage to property. Successful kinetic measures and ballistic measures could also cause injury or damage to persons or property on the ground creating both criminal and civil liability.

Birds of Prey have been trained to capture small drones but the effectiveness of this method is questionable. Larger drones can cause serious propeller injury to humans and animals alike and are too large for a bird of prey to disturb or capture.

Directed energy weapons are for now within the realm of the military. Laser and microwave weapons must have significant power sources for effectiveness. Ultimately counter drone destructive technology appears to be in the form of highly accurate laser systems particularly when the targeted drone is not susceptible to RF disruption.
The laws restricting the utilization of promising active countermeasures were made at a time when the future proliferation of drones were unforeseen. State laws and ordinances across the country vary or conflict. A congressional solution would ensure all law enforcement agencies have the authority to utilize whatever measures or tools that are necessary to respond to real or perceived threats caused by offending drones while at the same time preserving the ability to utilize these measures or tools safely in the National Airspace System.

**Conclusion**

Effective counter UAS measures require planning, technical training and good decision making. The technology involving drones and drone countermeasures is rapidly evolving. The magnitude of the threat should determine the technological sophistication of the countermeasures deployed. State and federal ruling bodies have taken preliminary steps to address this evolving technology and the potential threats presented by unmanned aerial systems. State and local law enforcement agencies will likely have the authority and tools necessary to address errant and rogue drones in the not so distant future. This article is not meant to be legal advice and any counter UAS implementation should be reviewed by the person or organization’s legal counsel.

*Copyright © 2019 34 North Drones LLC. All rights reserved.*