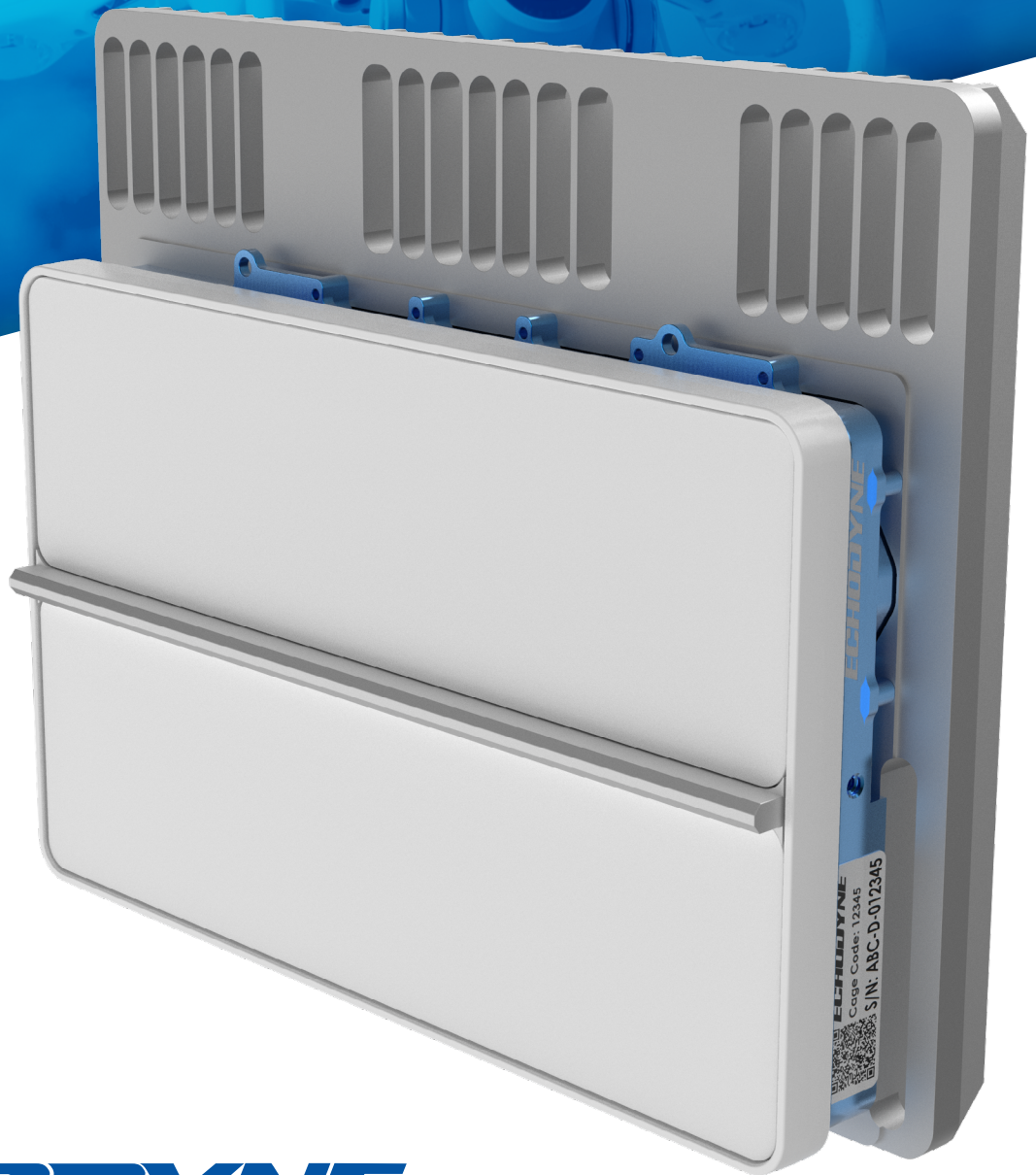


An Echodyne White Paper:

PROTECTING CRITICAL INFRASTRUCTURE FROM DRONES



ECHODYNE

Contents

- Introduction** 3
- Drones Threaten Critical Infrastructure** 4
 - A Vast Array of Critical Infrastructure Requires Protection 4
 - Many Avenues of Attack..... 5
 - Speed + Payload Make Drones Dangerous..... 7
 - The Kalashnikov Drone 9
 - Protecting Against Espionage 9
 - Summarizing the UAV Threat 9
 - Dynamic Threat Assessment..... 10
- The Need for 3D Situational Awareness of Critical Infrastructure Airspace**..... 11
- The Foundation of 3D Situational Awareness: High-Performance Radar**..... 11
 - Drones Require Precision Radar 11
 - Why ESA Radars on Fighter Jets are the (Very Expensive) Gold Standard..... 12
 - The Value of ESA Radar in UAV Detection 12
- High-Performance Ground & Airspace Surveillance** 13
 - More Precise Tracking 13
 - Active Interrogation of the Airspace..... 14
- Integrating with Other Detection Tools**..... 15
 - Electro-Optical and Infrared Cameras..... 15
 - Radio Frequency Detectors 17
 - Acoustic Sensors..... 18
 - Reaction Timeline & the Value of Multiple Sensors 18
- Interdiction Requires Detection and Tracking Competencies** 19
- About Echodyne** 20

Introduction

Modern security is justifiably focused on securing facilities and infrastructure from cyber intrusion. While stolen customer data can reduce brand and reputation value, the actual damage to business productivity or execution pales in comparison to hacked industrial controls or stolen product designs. The cyber threat is real.

There is a concurrent security threat, though, that may actually be more pernicious. It transgresses even the most highly secured perimeters without alerting security operations. It lurks beyond sight or sound but can see and hear with great accuracy. It adapts easily to sensor, cyber, and payload needs. It is inexpensive to purchase in retail channels, can be self-built with minimal expertise and cheap parts, and requires little experience to operate.

This new threat is called the small unmanned aircraft system (sUAS), or sometimes an unmanned aerial vehicle (UAV), but most commonly called a drone. The current ground-only 2D security deployments now need airspace surveillance capabilities integrated with VMS-based security systems to create robust 3D situational awareness. Drones challenge every aspect of commercial and industrial facility security, with the risks most vividly illustrated by the critical infrastructure segment. The risk of cyber intrusion that cripples electricity services is very real and should command attention. The risk of careless or intentional drone flight that damages generation or distribution facilities is arguably just as real and should command equal attention.

This paper is intended for security professionals and provides context, data, and science for considering 3D security relative to risk factors. Indeed, this paper asserts that, among all airspace surveillance sensors, radar is essential for counter-drone capabilities in a 3D security world, especially for medium- and high-risk facilities and locations. However convenient this may seem coming from a manufacturer of an innovative 3D surveillance radar, this assertion is supported by every example of securing high-risk government and military perimeters with airspace surveillance requirements. Radar is essential.

We invite you to consider the science and data in this paper and welcome you to share your thoughts and experiences with us at echodyne.com/3Dradar.

Drones Threaten Critical Infrastructure

Critical infrastructure across the United States faces a growing threat from unmanned aerial vehicles (UAVs). The sophistication and carrying capacity of inexpensive UAVs continues to rise, while too much of our critical infrastructure remains unprotected from UAV use.

The massive vulnerability of our critical infrastructure is gaining attention:

- ▶ “In the United States, the authorities voice increasing concerns about possible Islamic State-inspired drone attacks against dams, nuclear power plants and other critical infrastructure.”
--Eric Schmitt, *The New York Times*
- ▶ FBI director Christopher Wray told a U.S. Senate panel the threat from drones “Is steadily escalating” and has “only increased in light of the publicity associated with the apparent attempted assassination of Venezuelan President Maduro using explosives-laden drones.”
--David Shepardson, *Reuters*
- ▶ Cybersecurity and Infrastructure Security Agency Assistant Director for Infrastructure Security Brian Harrell says of UAVs “This is not an emerging threat. This was emerging five years ago. This is here. It is now.”
--Bridget Johnson, *Homeland Security Today*

A Vast Array of Critical Infrastructure Requires Protection

The challenge of protecting critical infrastructure is placed in perspective when considering the complex systems we are dependent upon.

The U.S. Department of Homeland Security notes “There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”

DHS, in alphabetical order, lists the 16 areas of critical infrastructure as:

- ▶ Chemical Sector
- ▶ Commercial Facilities Sector
- ▶ Communications Sector



The world is filled with critical infrastructure that must be protected from UAV attacks.

- ▶ Critical Manufacturing Sector
- ▶ Dams Sector
- ▶ Defense Industrial Base Sector
- ▶ Emergency Services Sector
- ▶ Energy Sector
- ▶ Financial Services Sector
- ▶ Food and Agriculture Sector
- ▶ Government Facilities Sector
- ▶ Healthcare and Public Health Sector
- ▶ Information Technology Sector
- ▶ Nuclear Reactors, Materials, and Waste Sector
- ▶ Sector-Specific Agencies
- ▶ Transportation Systems Sector
- ▶ Water and Wastewater Systems Sector

Looking at just a few areas of the full critical infrastructure landscape underscores the vastness faced in protecting assets from attacks by UAVs. For example, there are an estimated:

- ▶ More than 8,600 power plants capable of generating at least 1 megawatt
- ▶ 98 nuclear reactors within 60 commercial nuclear power plants across 30 states
- ▶ More than 130 oil refineries spread across more than 30 states
- ▶ 2,400,000 miles of Energy pipelines
- ▶ More than 1,400 hydroelectric dams
- ▶ More than 80,000 unpowered dams
- ▶ More than 13,500 chemical manufacturing facilities
- ▶ Hundreds of transportation ports, with the largest 8 ports combining to handle more than 1 billion short tons of cargo per year
- ▶ More than 14,400 Water & Treatment plants
- ▶ More than 5,000 Airports with paved runways
- ▶ More than 400 Military bases within the continental US
- ▶ More than 1,800 Prisons

Many Avenues of Attack

Drones can be used to attack critical infrastructure in a number of ways, all of which challenge the prevailing security model of securing the ground plane. Drone threats include:

- ▶ **Surveillance.** The most basic risk is the potential for one or more UAVs to loiter outside a critical perimeter in an ISR role, capturing sensitive information, which could range from raw materials delivery, to shift changes, parking lot counts, security patrol schedules, or other activities. This information gathering poses a fundamental security risk but may also be a precursor to further escalations and attacks once targets are identified and security capabilities mapped out. Sensors and systems that can easily identify persistent hovering drones over a large secure perimeter are a key piece of the air security puzzle.
- ▶ **Perimeter Intrusion.** Crossing a fence line or secure perimeter to enter a facility's airspace is an escalation that needs to be carefully monitored and potentially mitigated subject to prevailing legal authorization. While an accidental or clueless overflight may happen on occasion, this could represent a criminal act that needs a fully documented evidence trail. The [2018 Greenpeace stunt](#) in which a Superman-shaped drone was crashed into a French nuclear plant to demonstrate its vulnerability to outside attacks is an example of such an intrusion. Sensor solutions such as radar that provide precise time-stamped geo-location provide critical evidence for prosecution.
- ▶ **Extended Cyber Attack Surface.** Landing unobserved in remote locations to probe wireless networks for weaknesses is real. Industrial facilities in remote locations with a robust 2D security perimeter may have less security for network and systems access – after all, the threat of an inexpensive drone with cyber capabilities was science fiction just a few years ago. It's very real today. Extending the cyber perimeter requires sensor capabilities similar to surveillance needs.
- ▶ **Infrastructure Damage.** Beyond simple trespass, flying a UAV over traditional perimeters, such as a fence, and kinetically impacting critical infrastructure is a low effort approach that garners headlines. One might assume the small mass and velocity of a UAV may not by itself pose a significant threat to a hardened facility. In 2017, a Silicon Valley man [triggered a power outage](#) impacting 1,600 people when he crashed his drone into a Mountain View high-voltage wire and caused tens of thousands of dollars' worth of damage. The ability to configure these precision UAV platforms to deliver payloads to an exact location is a huge risk to power plants, substations and datacenters where outages can cost millions of dollars per hour. Sensors that can track and highlight air targets flying towards these particularly vulnerable areas offer critical situational awareness and time to react.
- ▶ **Explosive Delivery.** Finally, the potential for explosive payloads to be carried by these drone platforms and precisely delivered to weak points is an inevitable risk that needs to be discussed in the context of critical infrastructure. While even the popular Phantom4 UAV can be [modified](#) to carry a couple grenades as demonstrated by ISIS in the Middle East, the greater threat are the larger payload platforms that can deliver 5 kgs of improvised munitions into a chemical plant, refinery or similar target where they're most vulnerable. High risk locations must have sensors that can detect, track, and identify objects of interest in the airspace with sufficient advanced warning time to trigger precision interdiction.

Attacking critical infrastructure creates costs far beyond the actual physical damage to facilities. Losing key elements of the electrical distribution system could leave cities without power. Attacking a chemical plant could send poisonous clouds across population centers. Potential scenarios are frightful. All of this means that there is a vast and growing—and largely unmet—need for protecting critical infrastructure from UAV attacks.

Speed + Payload Make Drones Dangerous

In infrastructure security, the most pressing and asymmetric airborne threat is the proliferation of consumer drones that can be easily tasked toward a variety of threat scenarios. For a representative sample of the current UAV capabilities, one need look no further than DJI, a Shenzhen-based firm that dominates the consumer and professional drone industry with a 74% estimated global market share per Skylogic Research's 2018 report, as shown in Table 1.

DJI Model	Control Link (Ghz)	Max Speed [mph]	Payload	Flight Time [min]	Control Range/FCC	Cost
Spark	2.4/5.8	31	-	16	2km/1.2mi	\$399
Mavic 2 Pro	2.4/5.8	45	-	31	8km/5mi	\$1,500
Phantom 4	2.4/5.8	36	-	30	7km/4.3mi	\$1,500
M200	2.4/5.8	51	2.3 kg	24	7km/4.3mi	\$5,000
M600	2.4/5.8	40	6.0 kg	18	5km/3.1mi	\$4,999

Table 1. Examples of commercial UAV capabilities.

All other competitors, while still offering impressively capable UAV platforms, have market shares in the single digits. Worth highlighting in the same report as an area of concern is the 'Custom/DIY' drone market, ranked as third largest source of drones and includes aircraft from the vibrant FPV racing drone to hobbyists experimenting with combinations of control systems, motors, radio links, and accessory payloads.

Driving DJI's market dominance is a family of multicopters with industry leading flight times, remote control ranges, video stabilization and collision avoidance sensors. These highly integrated platforms extend the basic concept of a 'flight stabilization platform for video capture' to truly autonomous aerial vehicles with intelligent software offering programmable waypoint flight paths, automated take-off & landing routines and remote video streaming from miles away.

A commercially available DJI model M200 is capable of delivering a 2.3 kg (5 pound) load at a speed of 51 miles per hour, and across a distance of more than 4 miles. The M600 model can carry 6 kg (13.2 pounds) at a speed of 40 miles per hour across a distance of three miles.

Table 1 also shows the low cost of these commercial drones—just \$5,000 for the most powerful shown, with smaller versions available for a few hundred dollars.

Table 2 shows the destructive force of even a 5-pound payload:










Threat	Threat Description	Explosive Capacity	Building Evacuation Distance	Outdoor Evacuation Distance
	Small Package/letter	1 lb	40 ft	900 ft
	Pipe Bomb	5 lb	70 ft	1,200 ft
	FedEx Package	10 lb	90 ft	1,080 ft
	Vest/Container Bombs	20 lb	110 ft	1,700 ft
	Parcel Package	50 lb	150 ft	1,850 ft
	Compact Car	500 lb	320 ft	1,900 ft
	Full Size Car/Minivan	1,000 lb	400 ft	2,400 ft
	Van/SUV/Pickup Truck	4,000 lb	640 ft	3,800 ft
	Delivery Truck	10,000 lb	860 ft	5,100 ft

Table 2. Explosive munitions ranges.

DJI’s market dominance has led to it becoming a leader in government and policy conversations around embedded restrictions, such as updatable geofencing, monitoring capabilities in their Aeroscope solution, announcement of their [AirSense](#) technology, and a recent [10-point plan](#) to address the growing concern of drone misuse. Not terribly complex modifications can mitigate these restrictions and monitoring capabilities, and of course they only work for DJI drones.

The same technology that enables the layperson to become an aerial cinematographer and has given birth to an entire industry of amateur pilots, through enabling great quality video capture (stabilized station-keeping via GPS in wind, precision flying with little training, long endurance, remote viewing of HD video) also provides an excellent platform for covert surveillance or the precision delivery of dangerous payloads from great distances.

The Kalashnikov Drone

To this point we've looked at the ways in which commercial general-purpose drones can be weaponized. The challenge becomes greater with the introduction of drones specifically built to be weapons. An example of this is the recently introduced Kalashnikov KUB-UAV — which is purported to be simple to operate, effective and cheap. The KUB is four feet wide, can fly for 30 minutes at a speed of 80 mph and carries six pounds of explosives. That makes it roughly the size of a coffee table that can be guided to explode on a target 40 miles away — the equivalent of a “small, slow and presumably inexpensive cruise missile,” according to a report by the National Interest website. The proliferation of these low cost, long range flying wings brings another level of concern to an already outmatched security industry.

Putting the threat of the Kalashnikov into chilling perspective, the *Washington Post* quotes Nicholas Grossman, a professor of international relations at the University of Illinois and author of the book *Drones and Terrorism*, as saying, “Whoever buys one will have the ability to steer a bomb with a high degree of accuracy unparalleled except by some of the U.S. military’s smartest bombs.”

Protecting Against Espionage

Drone-based espionage is also a concern. Every building that houses computer systems, whether a small business, a regional bank, or the server farms that host internet and cloud-based resources is potentially vulnerable to a small UAV landing on the roof, tapping into the local Wi-Fi, breaching security systems, and unleashing software to subvert systems to steal intellectual property, gain trade secrets, or to directly attack and damage the operational resources.

The potential threats from drones sound like something from science fiction, but unfortunately, many of the stories are already coming true—from the attempted assassination of President Maduro of Venezuela to terrorists arming drones as distressingly effective explosives-delivery devices.

This is why the world so greatly needs the technology that can provide the most precise airspace situational awareness possible.

Summarizing the UAV Threat

What this all means for airspace security is the current state of the art in UAV technology is a threat profile that encompasses:

- ▶ A reasonable low cost, precision platform that is easily obtainable in the range of \$500-\$5,000 without a required license or training;
- ▶ Flight speeds in the 30-50 mph range for commercial multicopters;
- ▶ Flight durations up to 30 minutes including perfectly stationary hovering for multicopters;

- ▶ Remote controllable from many miles distance via radio link or potentially autonomous flying via GPS waypoints or vision systems requiring no RF link;
- ▶ Stabilized HD imagery;
- ▶ The potential delivery of payloads (explosive, chemical or other) in the 5-pound range with pin-point accuracy.

Dynamic Threat Assessment

One of the aspects of UAV intrusion into protected airspace is how it challenges existing threat assessment paradigms. In 2D security, critical infrastructure erects multiple layers of physical defense and traps – fences, barriers, gated entry, guard patrols, and cameras everywhere. Any person or vehicle advancing on the facility that has neither been deterred by barriers nor cleared by guards is considered a threat, triggering response protocols.

In 3D security, this is no longer true. There are no physical impediments or checks upon advancing aircraft, so the unchanged response protocol will scramble for every drone overflight. The challenge is that, unlike 2D security, the advancing drone is likely controlled by someone without the proper training or the good sense to know where they are flying.

Figure 1 represents the bell curve of UAV operators. The 3D security challenge is discerning the intention of the advancing UAV. Critical infrastructure located near population centers, parks, or quiet outdoor spaces may appear to be the perfect place for drone use. The casual flyer is likely unaware of the security perimeter location or how their flying is perceived by sensors or security personnel. Unfortunately, there are no simple answers, no indications of the threat from any one UAV to another. Vigilance against airspace intrusions will need to fight against the complacency of one benign overflight after another.

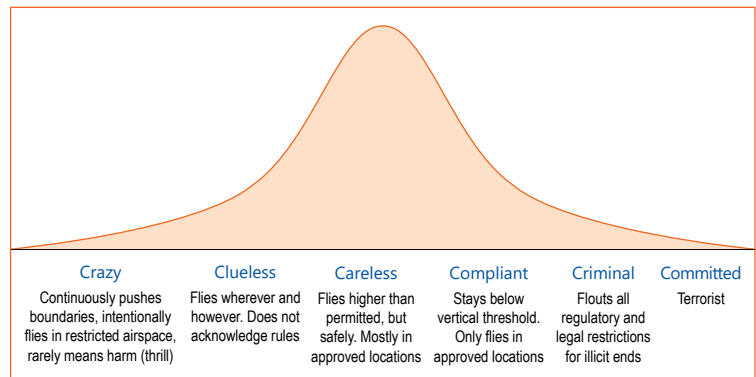


Figure 1. Drone operator types.

The Need for 3D Situational Awareness of Critical Infrastructure Airspace

Protecting critical infrastructure requires high-performance radar and other sensing devices that can work together to provide real-time situational awareness to help protect the airspace. While major airports have long had radar, a new type of high-performance radar, along with other sensors, needs to be deployed specifically for UAV detection to protect critical infrastructure.

The potential for attack isn't just theoretical. In May of 2019 Forbes, and other media, reported that two pump stations on Saudi Arabia's key East-West pipeline were attacked by armed drones, causing a fire and minor damage.

Closer to home, Rezwan Ferdaus was sentenced to 17 years in prison after the FBI uncovered a plot that Reuters reports involved a plan to use "remote-controlled model aircraft capable of flying 100 miles per hour and planned to fill the aircraft with explosives and crash them into the Pentagon and the Capitol using a GPS system in each aircraft."

The Foundation of 3D Situational Awareness: High-Performance Radar

While later in this paper we will look at the important role that other sensing and detection modalities, such as high-definition and infrared cameras, RF detection, and acoustic sensors, can play in creating effective multi-sensor solutions tailored to risk assessments, we assert that high-performance radar is the foundation upon which any effective 3D situational awareness solution should be built.

With radar playing such a foundational role in creating situational awareness solutions, it's good to take a closer look at radar, especially at how new radar designs can provide the superior performance required to detect, track, and classify UAVs entering a controlled airspace.

Drones Require Precision Radar

Historically, radar systems for aerial surveillance have either been relatively crude and ineffective or military grade and ultra-expensive. To provide wide area 3D surveillance, the radar system must be able to search a large volume of airspace, which can be accomplished via mechanical rotation or through flat panel radar with electronic beam steering techniques.

The classic marine or ground security radar with a rotating antenna and low/no elevation field of view is targeted for surveilling relatively flat terrain and water, while tracking slow moving objects such as boats and pedestrians with update rates of 1 Hz or less and subject to related mechanical part wear.

With multiple small airborne UAV targets the size of a bird, able to move at 50+ mph with great agility in three dimensions, the radar technology necessary to maintain unambiguous tracks is an electronically scanned array (or ESA) with agile beam steering. With true beam pointing control, ESA radars balance between a broad background grid search while simultaneously directing high-update tracking beams at targets of interest.

Why ESA Radars on Fighter Jets are the (Very Expensive) Gold Standard

When it comes to high-performance radar, the ESA units found in fighter jets around the world are the gold standard for radar performance. A form of phased array antenna, an ESA is computer controlled so its beam of radio waves can be electronically moved to focus on targets, without moving the antenna, while continuously scanning the entire field of view for new targets.

ESA eliminates the rotational latency inherent to mechanical radar. Its ability to instantaneously direct tracking resources on objects of interest at rates approaching 10hz provides ultimate precision for detecting and tracking objects of interest.

The speed and precision of ESA makes it ideal for airspace situational awareness. Unfortunately, the size, weight, power requirements, and direct and maintenance costs of ESA technology has proven prohibitive for all but the most critical national security needs. Echodyne's breakthrough technology packages the same ESA capabilities into a compact, solid-state, low cost, high-performance format for government and industry security needs.

The Value of ESA Radar in UAV Detection

ESA radar should serve as the foundation of an airspace situational awareness deployment because it can provide super-fast all-weather performance:

- ▶ Direct (not triangulated) measurement of drone position and velocity
- ▶ Long range detection and tracking of multiple simultaneous targets
- ▶ Continuous Search while Track (SWT)
- ▶ Wide field of view with high update rates
- ▶ Insensitive to weather or lighting variability
- ▶ Target size proportional to radar return levels
- ▶ Additional characteristics that can be used in target classification and prioritization.

With radar providing early detection, additional elements, such as cameras for device identification, or RF detection for determining origin of control, can be incorporated into hybrid solutions. But for detection and tracking, radar provides the foundation.

High-Performance Ground & Airspace Surveillance

Echodyne's patented Metamaterial Electronically Scanning Array (MESA™) radar provides a true ESA radar at a small fraction of the cost. MESA, which powers our EchoGuard 3D surveillance radar, operates just like a high-end phased array radar, instantly steering a high-resolution beam around a 3D field of view, providing real beam scanning in both azimuth and elevation.

Additional precision is provided by MESA integration with Echodyne's Acuity, an intelligent radar control software suite that enables maximum user configurability. Acuity unlocks the power of MESA technology through deep customization, intelligent radar resource allocation, and data processing algorithms. This unique blend of agile hardware and intelligent software provides unprecedented precision for establishing 3D security perimeters through early detection of UAVs.

The affordable price point combined with a size and form factor that makes for easy deployment means airports and other facilities can deploy multiple units to provide coverage that might otherwise be blocked by buildings or other obstructions.

With the tower-mounted configuration, as shown in Figure 2, the MESA radars provide simultaneous overlapping coverage to support 360° azimuth by 80° elevation airspace surveillance without the inherent track update delay or mechanical unreliability of rotational radar systems.



Figure 2. Echodyne Tower Kit with 360 surveillance.

More Precise Tracking

The system's <10 msec time per unique beam direction with nearly instant pointing update rate allows in excess of 100 unique look directions per second which are scheduled on a real-time basis, interrogating up to 20 airborne targets at rates as high as 10Hz while still searching the full FOV for new contacts.

While the system's 2° Az x 6° El beam is well matched to highly zoomed camera systems, the ability to bracket a tracked target with a cluster of sequential beams allows interpolation techniques that yield high angular track (~1°) resolution for extremely precise camera pointing allowing maximum range identification and enhancing EM jammer or other countermeasure performance.

Active Interrogation of the Airspace

Echodyne's MESA technology, coupled with its Acuity software, gives the radar the ability to track and interrogate multiple simultaneous objects within the airspace, focusing attention on signatures that could be associated with threats.

Beyond precise target 3D position and velocity tracking, radar provides a rich dataset of information not available in other sensing modalities. Incoming target velocities can be used to prioritize threat levels. Target altitude can be used to discriminate from ground clutter, and target properties such as radar cross section indicate the size of the object and potential payload danger. Close following drones can be distinguished as separate threats and hovering drones can be detected via their propeller motion at ranges beyond the typical security perimeter.

EchoGuard Tracking Ranges

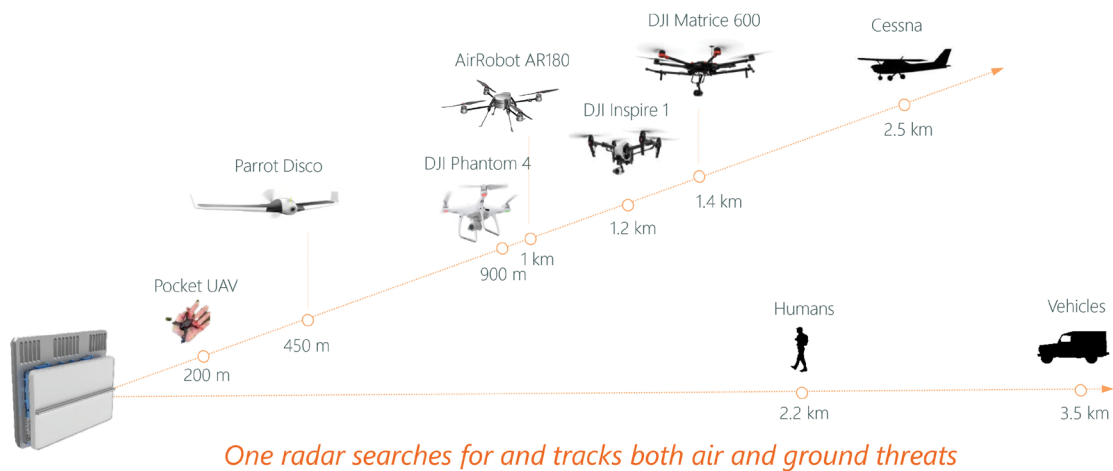


Figure 3. Echodyne radar tracking ranges.

Integrating with Other Detection Tools

For the foreseeable future, high-performance radar—such as Echodyne’s MESA-powered EchoGuard—will provide the foundation of the best deployments to protect airspace through situational awareness.

However, this radar foundation can be made even more efficient through hybrid, best-of-breed solutions in which additional layers of sensors are integrated with the radar. Echodyne is designed to easily interoperate with other sensor systems.

Common building blocks for radar integration include:

- ▶ Electro-Optical and Infrared Cameras
- ▶ Radio Frequency Detectors
- ▶ Acoustic Sensors

Electro-Optical and Infrared Cameras

As [vision-centric](#) creatures with 30% of the cortex dedicated to sight, the natural inclination for detecting perimeter intrusions is a camera-based system comprising an excellent sensor (visible and/or thermal), high quality zoom optics and a ruggedized pan/tilt pedestal for surveilling the surrounding air space. Real-time video of a drone flying over critical infrastructure is clear evidence to enable appropriate mitigation techniques. Quality security camera partners such as FLIR and Bosch provide a large portfolio of choices at varying performance levels and price points.

While these cameras are an integral part of any system, traditional security deployments are limited by the legacy of a 2D threat, as cameras typically are mounted high on buildings or poles, generally in fixed locations, looking down at entrances, parking lots and fence lines for bipedal intrusions. To detect high-flying drones, the problem space becomes 3D where one needs to monitor an extremely large region, essentially an entire hemisphere of airspace. Camera solutions include upward looking gigapixel camera arrays (prohibitively expensive) or the more traditional PTZ (pan/tilt/zoom) camera solution, constantly patrolling a search grid with the associated slew rate limitations, accelerated mechanical wear and inability to track distributed air targets.

To get a better feel for the limitations, consider a typical commercially available [1/2.8" 2MP HD CMOS Sony sensor](#) (1920 x 1080 pixels) matched with a 4.3-125mm focal length zoom lens, yielding at max zoom (125 mm focal length for max detection range) an image field of view (FOV) of just [2.4°V x 4.3°H](#). For a single camera to survey the surrounding horizontal 360° perimeter, assuming an average 1 second



Figure 4. Cameras are integral to situational awareness.

dwelling per look direction with fast focusing and analytics, would require over 80 seconds, ignoring image stabilization issues at such high magnification. Extend this patrol in the vertical direction (with $\sim 2.4^\circ$ steps) and you have a single optical scan over the FOV on the order of an hour. Quite clearly, the camera needs to be directed or 'cued' where to look in the sky to find the target—which is precisely what Echodyne's high-performance radar can do.

Why is high optical magnification necessary for a counter-UAV mission? In the video security industry, [DORI](#) (Detect, Observe, Recognize, Identify) is a standard (EN-IEC 62676-4) for defining the ability of a camera to distinguish persons or objects within the FOV. Each level increases the amount of image detail that can be extracted for decision making. At the lowest level, the defined 'Detection' threshold requires at least 25 pixels/meter of object for an operator to reliably and easily determine whether or not any target (e.g. person or vehicle) is present. For the miniscule DJI Phantom 4 drone (0.3m W x 0.2m T), this corresponds to roughly a detection range of 1 km at maximum focal length and reduced range at lower zoom levels.

Criteria	Threshold	4.3 mm (1x)	43mm (10x)	125mm (~30x)	Detail Level
Detect	25 px/m	62 m	94 m	1030 m	Is target present or not?
Observe	63 px/m	24 m	37 m	409 m	Characteristic details of target, e.g. quadcopter?
Recognize	125 px/m	12 m	19 m	206 m	Determine with high degree of certainty target type
Identify	250 px/m	6 m	9.4 m	103 m	Identify target beyond reasonable doubt, Phantom 4

Table 3. Example DORI thresholds for a Phantom 4 UAV at various focal lengths for representative 1/2.8" sensor.

Finally, any visible optical detection technique will be degraded by environmental factors such as sun glare and shadows, day/night cycles and the variabilities of weather such as fog, rain, and dust. Thermal sensors can reduce sensitivity to sunlight and dust, but at much greater cost and are subject to export regulations for the higher resolution displays necessary in long range UAV identification.

In Summary: Camera systems excel for confirmation and identification of the drone threat, but they're poor at aerial threat detection and multiple target tracking.

Radio Frequency Detectors

To date, nearly all commercial UAVs are advanced forms of the classic remote control (R/C) plane, utilizing a continuous radio command and control (C2) link for flight as well as video transmission.

As part of a situational awareness solution, to augment camera sensing, RF detectors can be used to locate RF transmissions from both the flying drone and its ground control station. This allows for both tracking the airborne threat as well as dispatching law enforcement toward the location of the pilot.

RF detection and direction finding is a technology that traces its history to the signals intelligence efforts of World War 1, with a century worth of improvements in signal processing, sensitivity and antenna design. Even so, monitoring the entire, modern-day radio spectrum in real-time is a challenge while looking for particular R/C communication packets. Fortunately, nearly all commercial drone C2 and video link bands are constrained to the unlicensed ISM (Industrial, Scientific & Medical) spectrum, predominantly the familiar Wi-Fi (2.4 and 5 GHz) as well as the less popular, but longer propagating 400 & 900 MHz bands. This allows for a more affordable detection systems targeted to monitoring likely ISM channels for particular control signals patterns.

RF detection companies such as [Dedrone](#) offer advanced systems that can detect radio-controlled drones the moment the system is turned on, providing an early warning that a launch is imminent; as well as issuing alerts during the duration of the flight that an active drone is in the area. Range performance can be quite good, 1-2 km depending upon background conditions, but high levels of Wi-Fi usage such as near a sports stadium on game day can degrade detection performance. This type of sensor provides an excellent warning capability and is a useful tool for security teams interested in ascertaining current threat levels and locations and activity statistics, often needed to justify further counter UAV expenditures.

With multiple radio receiver locations spread over a sufficient geographic baseline, RF systems can also determine a bearing to the threat and direct attention and potential countermeasures toward the region of concern. However, RF detectors lack the precise target range, velocity and critical elevation information for the target, which limits its use for cueing zoomed cameras at long ranges.

RF is currently the best choice for addressing compliant/careless/clueless drone operators such as the negligent hobbyist. However, determined bad actors can sidestep RF detection via various means. Radio-links can be reconfigured to non-standard frequency bands via mail-order modules without requiring expert knowledge. The radio link can even be abandoned altogether, with the system utilizing pre-programmed GPS waypoints to fly completely automated hostile missions into infrastructure.



Figure 5. RF detectors enhance situational awareness.

Finally, [computer-vision based aerial navigation](#) leveraging high resolution satellite imagery and advanced computing enables a completely self-contained drone with no RF signature for detection or manipulation.

[More detail is available](#) in the radio control packets such as precise GPS position, heading and speed, but decoding, protocol inspection and manipulation is currently legal only at sites with special US Federal designation, such as the Department of Defense, Department of Justice, or Department of Homeland Security.

Acoustic Sensors

To remain airborne, nearly all UAVs require a method of propulsion that moves air and generates some level of noise. Sensing drones by the acoustic signature of their propeller blades is an approach that companies such as Squarehead Technologies' Discoverair and Dynetics SoundAware offer. These sensors have unique properties, in that they're passive (for covert sensing), largely immune to visibility impacts such as fog and dust, and don't require line-of-sight to the drone, as sound can echo in urban canyons.

These systems can detect bearings to multiple drones and, similar to RF direction finding, two or more acoustic sensors with sufficient baseline separation can provide a triangulated position of that drone, albeit with no elevation information—limiting the accurate cueing of a camera for identification. Acoustic systems remain operational when electronic countermeasures such as jamming are applied that can temporarily blind RF sensing equipment. Interestingly, acoustic detection of drones without the associated RF signature may be a potential indicator of a greater threat of the so-called 'dark drone'.

Acoustic systems claim effectiveness out to a maximum range of 500m in ideal conditions, but in denser urban environments with elevated noise floors (road noise, HVAC, etc.) this can be degraded. They form a good 2nd sensor for confirmation of targets and false alarm mitigation.

Reaction Timeline & the Value of Multiple Sensors

Given the summary specs above, one can calculate that an approaching commercial UAV on an incoming vector can cover a mile (1600m) in just 1-2 minutes which allows precious little time for detection, classification, threat assessment and potential mitigation. Sensors which can detect these platforms have a timeline of mere minutes to provide actionable intelligence the critical infrastructure operator.



Figure 6. SoundAware system.

Consequently, an array of sensors is available, each with unique strengths and potential weaknesses, that offers a layered approach to addressing this threat. High-performance radar, EO/IR cameras, acoustic sensors, RF detectors and other technologies will all be needed in the battle to protect airspace from unauthorized UAVs. And as shown in Table 4, radar plays a foundational role.

	Range	Angular Dir. Det.	Accuracy	Tracking	Classification	Hovering Drone	Autonomous (No-RF-Link)	Mitigation	Comments
Acoustics	Red	Yellow	Red	Yellow	Green	Green	Green	Red	Environmentally sensitive to other noise sources
RF Radio ID	Yellow	Red	Red	Red	Green	Green	Red	Red	Limited by range and RF library
RF Direction Finding	Yellow	Green	Yellow	Yellow	Red	Green	Red	Red	Sensitive to RF emitters and sensor base line
Ground Radar	Green	Green	Green	Green	Yellow	Yellow	Green	Red	Not passive, but insensitive to drone RF signature
EO/IR Camera	Yellow	Red	Yellow	Green	Green	Green	Green	Red	Needs to be cued by other sensors
RF Packet Sniff & Spoofing	Yellow	Yellow	Green	Green	Green	Green	Red	Yellow	Limited by range, RF library, GPS position TX
Multi-Sensor	Green	Green	Green	Green	Green	Green	Green	Yellow	

Table 4. Radar is the only sensor capable of providing RF-independent, accurate drone location and is complementary to most other sensor types.

Interdiction Requires Detection and Tracking Competencies

One of the most commonly asked questions—and this is a question that becomes more urgent with the passage of time—is: Once you lock on an unauthorized UAV, what can you do?

The answer for the U.S. military, under battlefield conditions, is simple: If it appears to be a hostile threat, shoot it down.

The answer is more complex—and unresolved—for the rest of us. And it is a question that will need to be resolved on the federal level, with the U.S. Congress and the FAA, as well as at the state and local level.

An array of interdiction methodologies have been suggested, ranging from jamming the RF frequency a drone might be using, to training birds of prey to attack and retrieve a drone, to deploying counter UAVs with nets to snare the intruding device so it can be captured, without falling from the sky and injuring those below. All of these are currently illegal under a variety of laws and regulations.

Whatever counter measures are developed—and approved for use by the federal government—the crucial first step will remain early detection and precision tracking, which all begins with high-performance radar.

About Echodyne

Echodyne introduces the world's first compact, software-defined, solid-state, true electronically scanned array (ESA) radar sensor. Ideally suited for machine perception in an autonomous age, Echodyne offers high-performance commercially-priced radars to governments, industries, and integrators engineering solutions for border security, critical infrastructure protection, first responders, unmanned aircraft systems, and autonomous vehicles. Privately held, the company is based in Kirkland, Washington, and is backed by Bill Gates, NEA, Madrona Venture Group, Vulcan Capital, and Lux Capital among others. For more information, please visit: Echodyne.com