WHITE PAPER

Counter-Drone Technology for Airports

Points to Be Considered While Evaluating Various Solutions

Executive Summary

Current rise in the popularity of drones have caused a surge in aircraft-drone near-miss events and raised the risks of drone air traffic disruptions.

Commercial and consumer drones usually weigh less than 2 kg. While quadcopters are the most popular, other fixed-wing drones are available as well.

Drones have a battery life of around 30 min on a single charge. Notwithstanding any regulations, drones are capable of flying at heights of around 6000 m, with maximum possible range exceeding 8 km away from their controller. This is the same altitude level that passenger aircraft are at, while taking-off or landing at airports.

Recent studies have proved drone collisions to be more deadly than bird strikes of equivalent energy. An aircraft could suffer from structural damage from a drone collision, causing a crash.

Apart from unintentional collisions or disruptions caused by untrained drone operators, there is also the danger of purposeful collisions. Consumer drones can carry payloads of over 500g, with commercial drone capacity exceeding 6 kg. Terrorists may misuse this technology for delivering explosives and crashing planes via drones.

Several anti-drone technologies exist which can put an end to the menace. While monitoring is encouraged, drone neutralization methods are still not legally allowed in several countries. Typical monitoring tech equipment include RF Analyzers, Radar, Cameras and Acoustic Systems. They all come with their own pros & cons.

Typical countermeasure tech equipment includes Birds of Prey, HELs, Net Guns and Nets, HPM devices, GPS Spoofers, and RF Jammers. While none of them are permitted yet due to official regulations, Net Guns are highly suitable due to lower levels of collateral damage risks at airports.

EMPs, RF Jamming and GPS spoofing have higher collateral damage risks, but can yield successful results when used correctly.

What Is the Issue

with Using Drones Near Airports?

Usage of drones has become popular in recent years as they've become easier to obtain & fly, and are affordable. However, this comes with its own set of threats. Growth in current drone usage rates has caused a surge in aircraft-drone near-miss cases on a worldwide basis.

There are also growing concerns that drones could be used for nefarious purposes. This could include methods like flying them over airports or maneuvering them into flight paths of aircraft for causing a deadly collision.

Terrorists could also try to deliver & detonate explosives near an aircraft's wings via drones, which is a truly horrifying prospect.

What Kinds of

Drones Cause a Menace?

The drones that pose threats near airports are not military-grade drones. These are simple commercial or consumer drones, which mostly weigh below 2 kg. While quadcopters are the most common in this category, several other fixed-wing small aircraft are included as well.Various other names for such drones include SUAS and SUAV, commonly termed so, in defense circles.

DJI is a drone firm who supplies the world's most competitive drone models available in the market today. Their most sought-after drones and relevant specs have been included below:

	Spark	Mavic	Phantom	Inspire	Inspire Matrice 600
					
Dimensions	14x14x6cm	31x24x9cm	29x29x20cm	48x47x32cm	167x152x73cm
Weight	300g	700g	1.4kg	3.4kg	10kg
Max. Flight Time	16 mins	31 mins	30 mins	27 mins	18 mins
Max. Speed	50 km/h	72 km/h	72 km/h	94 km/h	65 km/h
Max. Altitude	4 km	6 km	6 km	4.5 km	4.5 km
Max. Transmission Distance	2 km	8 km	7 km	7 km	5 km
Max. Recommended Payload	N/A	N/A	N/A	810g	6kg
Autonomous Flight Capable?	YES	YES	YES	YES	YES

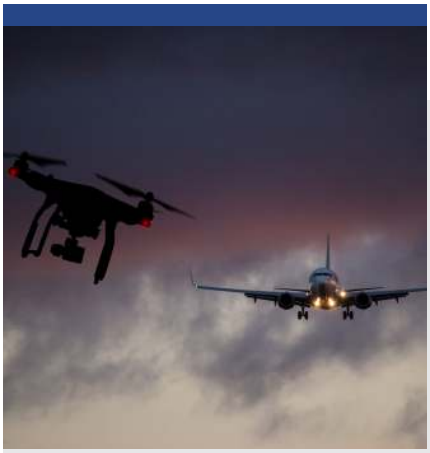
PERSISTENT AND INTENTIONAL AIRPORT DISRUPTION

Drone flight times happen to be quite limited, mostly between 15 – 30 minutes. However, batteries may be swapped out for newer ones in seconds, which means that flight times may be extended significantly with frequent, but short interruptions.

If persistent and intentional airport disruption is the goal, that is achievable by using multiple drones or having an ample supply of batteries nearby.

AIRCRAFT MAY ENCOUNTER DRONES DURING LANDING OR TAKE-OFF

Most drones stay near the ground, with most countries mandating a maximum altitude, mostly at 120 m. However, drones are able to fly at altitudes of over 6 km in a few cases. While it is not a threat to an aircraft at a cruising altitude, it poses a significant threat during landing and take-off times.



DRONE OPERATORS NEED NOT BE CLOSE TO THE AIRPORT FOR OPERATING IT

While most regulations mandate that drones should never stray away from the operator's Line-of-Sight (LoS), typically set at 500 m, drones are capable of functioning smoothly even at distances of over 7-8 km away from their operators, which makes apprehending them a much harder task.

CONSEQUENCES OF A PASSENGER AIRCRAFT – DRONE COLLISION

As can be seen based on the table given above, consumer drones typically measure 30 cm across & weigh below 2 kg in most cases. Professional drones measure between 50 – 1500 cm and weigh between 3 – 10 kg. Batteries are responsible for most of this weight.

A research study from DRI discovered that when DJI Phantom Drones (which weigh 1.4 kg and measure 30 cm across) were fired at speeds of 383 km per hour at a GA aircraft's wings, the drone caused a

hole in the aircraft wing's leading edge and went deep, deforming its entire structure. This lab test simulated real-life conditions of an aircraft-drone collision during a landing procedure.

DRI's Impact Physics Group Leader Kevin Poorman stated that almost all the aircraft's weight happens to be suspended on its spars. If it gets damaged beyond a point, the aircraft will crash, without a doubt,

While this test was made on GA structures, the UK CAA downplayed these damage risks, stating that passenger aircraft were built to a much higher quality. However, they did caution that drone-aircraft collisions caused greater damage compared to equivalent impact caused by bird strikes.

WHAT'S THIS DRONE CARRYING?

As seen above, a few drones have been developed for carrying heavy payloads. DJI Inspire models can carry over 1 kg, with the DJI Matrice 600 model capable of carrying over 6 kg. DJI Phantom models have been used by ISIS terrorists for deploying and carrying 40 mm grenades, which can each weigh over 400 g. Several hundreds of such attacks have taken place in Syria and Iraq.

2 DJI Matrice 600 drones were used during the 2018 assassination attempt made on Venezuelan President Maduro. Although unsuccessful, the drones detonated powerful explosives near the President.

While no Drone-Borne IEDs (DBIEDs) have popped up so far near airports, it is ridiculously easy to implement such a strategy compared to smuggling explosives aboard a place via traditional methods.

Additional

Drone-Related Challenges

Many drone models happen to be controlled via radio or Wi-Fi capabilities. The most frequently used Wi-Fi spectrum frequencies happen to be the 5.725 GHz – 5.825 GHz or 2.400 GHz – 2.483 GHz ranges. Data is transmitted in both directions between the drone and its controller, as both have radio receivers and transmitters.

Drone data often includes its position, video feed, altitude, heading, and speed. This information is streamed to the operator, who can use this data for maneuvering their drones with a high degree of precision that is extremely useful.

AUTONOMOUS FLIGHT

While most drones are flown on a real-time basis, controlled by an operator, it's also feasible to set up pre-determined checkpoints for them to reach autonomously.

Drones employ a safety function, where any emergency event can force the drone to fly back to a home location, that's already been preset.They can be modified to prevent them from transmitting data, which is extremely helpful in avoiding radio detection devices.

SWARMS

Drone swarms happen to be a real possibility. For example, Intel has showcased drone swarms where over 1000 drones were synchronized, pre-programmed & controlled from one, single source. An airbase run by Russia in Syria had been attacked by thirteen pre-programmed military drones, carrying explosives. This swarm had been launched from a location over 50 km away from the base.

FOE OR FRIEND

As drones become increasingly used by emergency services and commercial businesses, it may become difficult to distinguish between legitimate and non-legitimate drones. For instance, the Gatwick disruption in Dec 2018 was thought to have been caused by legitimate police drone sightings which were mistaken by the authorities for rogue drones, who then enforced an unnecessary airport shutdown.

Anti-Drone Solutions

Available for Airports

At the moment, airports are heavily reliant on alerts from the public, pilots, and ground staff. Although it's free, it can be disadvantageous, like the Gatwick Airport shutdown, where millions of pounds were lost as a result of the shutdown. Not maintaining a reliable drone surveillance system means lack of access to proper information. Even the data that you do obtain will be erratic, unreliable and unpredictable.

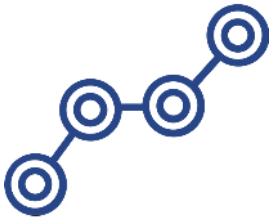
Uncertainty and safety aren't a good mix in airport environments. It could result in longer airport shutdowns, costing money and reputation.

Anti-drone technologies can be classified into two: Countermeasures; and Monitoring Equipment.

Drone Monitoring Equipment

These instruments can be active (sending signals out & analyzing the results) or passive (simply listening or looking) and can be used to perform several different functions like:

ALERTING



TRACKING AND LOCATING

IDENTIFICATION OR CLASSIFICATION

DETECTION

However, please be aware not every equipment performs the functionalities mentioned above, simultaneously.

There are 4 primary kinds of effective drone monitoring devices:

RADAR

OPTICAL SENSORS

ACOUSTIC SENSORS

RF ANALYZERS

RADIO FREQUENCY (RF) ANALYZERS

RF Analyzer consists of 1 or several antennas that receive specific radio waves & a processor that analyzes the radio frequency spectrum. They are used for detecting radio comms signals between controllers and their drones.

A few systems might even be capable of identifying common drone models and makes, with some capable of identifying the controller and the drone's MAC addresses as well (if that particular drone utilizes Wi-Fi comms networks). These are helpful for aiding prosecution arguments since it can prove that a certain controller and drone were active at a particular time.

Some advanced systems are also capable of triangulating a controller and his drone by utilizing several detection units that have been spread wide apart.

Pros: Can be cost-effective, can detect or even identify multiple controllers and drones, passive, therefore no licenses are required, some are capable of triangulating controller and drone position.

Cons: Does not always track and locate drones, cannot detect any autonomous drones, not very effective in areas with high RF levels, limited range abilities.

SOURCE: DGS

URBAN DYNAMITE RF-Based Drone Detection System, which utilizes the latest battlefield proven RF Spectrum Monitoring and Analyzing Technology, overcomes the above-mentioned technical disadvantages found in many other RF-based drone detection devices on the market, and provides following state-of-the-art features

- Real-Time ALL frequency spectrum monitoring
- Real-Time DF frequency monitoring and directions at the same time
- 3G, 4G and 5G drone detection capability
- Long Detection Range (up to 50 km)
- No-Gap Full Dome Coverage: 360° azimuth and 90° elevation with high tracking accuracy
- Tracks and Locates the drone operator(s)
- Identifies the drone model and make

ACOUSTIC SENSORS (MICROPHONES)

These are typically a microphone/a microphone array (consisting of many microphones) that can detect sounds made by drones and calculate direction. Adding more microphone array sets can enable rough triangulation capabilities.

Pros: Provides drone direction although it doesn't usually locate, medium prices.

Cons: Short ranges capped at a maximum of 300 to 500 meters, doesn't work well in a noisy environment.

OPTICAL SENSORS (CAMERAS)

Basically, it's an advanced video camera. Apart from imaging in standard daylight conditions, optical sensors may also have thermal or infrared imaging capabilities.

Pros: Can record pictures and collect forensic evidence for usage in prosecution arguments, can provide drone images along with its payload details.

Cons: Poor performance rates in fog, dark conditions, high false-trigger rates, is not an effective detection tool on its own.

RADAR

SOURCE: DGS

This device uses radio energy for detecting objects. The radar emits signals out and analyzes its reflection, measuring distance (position) and direction. Most radars emit radio signals in burst form and proceed to listen for its 'echo'. Almost every kind of radar is designed to pick out only large targets. They're designed for tracking large objects, such as a passenger aircraft.

Pros: Can track drones irrespective of any autonomous flight abilities, isn't dependent on visual conditions (fog, night, day, etc.), can track hundreds of objects/targets simultaneously, highly accurate location tracking abilities, constant tracking, long range.

Cons: Requires frequency check and transmission license for preventing interference, most of them cannot distinguish between drones and birds, detection ranges are dependent on the drone's size.

Drone Countermeasure Equipment

These can be classified as either:

- Taking full control of the enemy drone; or
- Neutralizing the enemy drone; or
- Physical destruction of the drones.

It's vital to understand that while this technology is already available, prevailing regulations in several countries explicitly forbid the usage of the below-mentioned tech equipment for enemy drone neutralization purposes.

Exceptions may be made for law enforcement or military agencies at times.

LOCATING & PHYSICALLY APRHENDING DRONE OPERATORS

Law enforcement or security agencies are still allowed to apprehend drone operators. However, you'll need to discover their location first.

COUNTER DRONE RF JAMMERS

RF Jammers are handheld, mobile, or static devices that transmit large amounts of RF waves towards enemy drones, masking controller signals. This may lead to any 1 of these 4 scenarios, based on the make and model of the drone.

- The drone flies away in an uncontrolled, random direction.
- The drone falls to the Earth in an uncontrolled fashion.
- The drone returns back to a home location set by the user (which may also be a target location instead of its launch location)
- The drone attempts a landing without changing its position.

Pros: Non-kinetic neutralization, medium price.

Cons: Can jam or affect other radio comms, short range.

The **Urban Dynamite Anti-Drone Jammer** transmits multi-bands RF and GNSS (Europe's Galileo, USA's NAVSTAR GPS, Russia's GLONASS, and China's BeiDou Navigation Satellite System) jamming signals to disrupt commercial drones' control functions and causes no damage to drone hardware or surrounding environment. The intruding target drone will be forced to

1. Enter vertical safe-landing mode
2. Return to the starting point or the drone operator which allows the drone operator to be tracked down

GPS SPOOFERS

These devices emit new signals targeted at the enemy drone, which replace its GPS satellite communications, used by it for navigation purposes. This way, drones can be 'spoofed' into incorrectly thinking that they are somewhere else. A drone's position may be controlled by trained spoofers by altering GPS coordinates dynamically on a real-time basis.

Pros: Non-kinetic neutralization, medium price.

Cons: May unintentionally lead the enemy drone to a target location, may cause unpredictability in drone behavior, can jam or affect other radio comms, short range.

HIGH POWER MICROWAVE (HPM) DEVICES

An HPM or High Power Microwave device generates an EMP (Electromagnetic Pulse) that is able to disrupt electronic devices. This EMP causes interference with the drone's radio links, which may result in disruption or even destruction of electronic circuitry systems in drones (along with other electronic devices in the range as well) due to damaging current and voltage levels created by it. An antenna may be included in HPM devices as well, for focusing this EMP blast in a particular direction that reduces chances of collateral damage.

Pros: Non-kinetic, drones can be neutralized effectively within range.

Cons: Drones may effectively switch off, which results in them falling down in an uncontrollable fashion immediately, risk of unintentional disruption of comms networks or destruction of electronic devices located in the vicinity, high cost.

NETS & NET GUNS

Firing nets at drones or enveloping drones with a net can stop drones by blocking off their rotor blades, crippling motion abilities. There are 3 main kinds:

Hanging nets that are deployed from 'net drones': Drones are captured by maneuvering friendly drones (carrying nets) towards rogue drones. 'Net drones' are normally capable of carrying rogue drones into safe zones, or in case the drone happens to be too heavy, they can release captured drones without or with parachutes for enabling controlled descent.

Net cannons fired from other drones: This overcomes the net cannon's limited range abilities. It can be tough to capture a moving drone. It is typically used with parachutes for ensuring that the captured drones undergo a controlled descent.

Net Cannons fired from ground level: Can be turret-mounted, hand-held, or shoulder-launched. Range effectiveness can be anywhere between 20m – 300m. May be used without or with parachutes for ensuring that the captured drones undergo a controlled descent.

Pros: Can physically capture drones – good for prosecution and forensics, low collateral damage risks, long range abilities of nets deployed by drones, net cannons that are launched from the ground tend to have semi-automatic abilities along with a high accuracy level.

Cons: Nets launched from the ground have shorter ranges, nets deployed via drones have long reload times and are often imprecise, kinetic solutions may result in drone destruction, based on whether a parachute was used or not.

HIGH-ENERGY LASERS

High-powered, advanced optical devices that produce extremely focused beams of light, also known as laser beams. Lasers defeat drones by destroying inner electronics or/and drone structure.

Pros: Can physically stop the drone.

Cons: Experimental technology, large system, high collateral damage risks, high cost.

BIRDS OF PREY

Eagles can be imparted training for capturing small drones. However, this is a very low-tech measure that requires considerable manpower resources for training (estimated at a year for one bird alone) and the maintenance of these birds of prey. Dutch law enforcement agencies, who had originally come up with this idea, disbanded this service as these birds weren't always responding to commands to capture drones. However, it doesn't mean this measure is completely ineffective though.

Pros: If these birds happen to be available near your location, the interception of drones can be accurate and quick with low collateral damage risks.

Cons: Intensive manpower resources needed for maintenance and training, birds do not always respond to capture commands, difficult to operationalize, birds can be hazards themselves in several environments.

Recommendation

AIRPORTS REQUIRE INTEGRATED SYSTEMS

No solutions given previously in this white paper are effective in stopping drone-related issues on their own. An effective system would include all these systems, which complement each other finely. And it's up to you, whether or not to combine countermeasures with monitoring solutions based on prevailing laws in your country.

BUT WHAT IS THE USE IN MONITORING WITHOUT BEING ABLE TO DEPLOY COUNTERMEASURES?

It's like a smoke alarm: While it doesn't put out any fires, not having any installed in your home would be a foolish move.For implementing an anti-drone solution, you need to understand this problem thoroughly, from all angles. You should devise a proper system that lets you defend against drone intrusions.If you are going to do this, you'll require a potent drone monitoring solution. For airport security, we suggest a powerful RF device, with cameras equipped into it, and a reliable drone radar. This solution will have an early warning, long range, highly accurate radar tracking, drone and controller identification along with camera abilities. While individual modules in such systems could raise false alarms, when they all work together, a significant improvement can be observed in accuracy rates.

YOU REQUIRE MICRO-DOPPLER RADARS IN YOUR INTEGRATED SECURITY SYSTEM

While radars' Pros and Cons were mentioned earlier, these are mostly applicable only for traditional radars, which aren't all that accurate. At DGS, we use micro-doppler radars, which are efficient at classifying, tracking, and detecting drones.

In case of drones, micro-doppler radars are capable of identifying propeller presence by detecting speed differences between the rotor blades.

This technique allows birds to be excluded from the scan, as they do not have propellers. This method works for fixed-wing aircraft and quadcopters as well.

Unlike traditional radars, our micro-doppler drone detection radar overcome some of the Cons mentioned earlier:

- Affordable alternative to conventional radar systems
- Can distinguish between birds and drones
- Have low power requirements, which make them safe and easy to operate & obtain transmission permits.
- Provide early warnings
- Track and detect autonomous drones unidentifiable by most RF solutions
- Provide a 360-degree radar coverage

Micro-Doppler Radar 'Urban Dynamite' 2018

Conclusion

Recent studies have proved drone collisions to be more deadly than bird strikes of equivalent energy. An aircraft could suffer from structural damage from a drone collision, causing a crash.

Apart from unintentional collisions or disruptions caused by untrained drone operators, there is also the danger of purposeful collisions. Consumer drones can carry payloads of over 500g, with commercial drone capacity exceeding 6 kg. Terrorists may misuse this technology for delivering explosives and crashing planes via drones.

Several anti-drone technologies exist which can put an end to the menace. While monitoring is encouraged, drone neutralization methods are still not legally allowed in several countries.

Typical monitoring tech equipment include RF Analyzers, Radar, Cameras and Acoustic Systems. They all come with their own pros & cons.

It is suggested that airport anti-drone monitoring systems have

- RF abilities for triangulation and identification of controllers and drones
- Cameras, for enabling visual identification
- Radar, for accurate tracking and localization and detection over long distances

When utilizing radar tech for detecting drones, regardless of whether it belongs to an integrated or a stand-alone solution, it has to be a micro-doppler radar, which are capable of differentiating between drones and birds. This prevents false drone alerts due to birds; which is a common disadvantage with radar.

Typical counter-drone technologies include Birds of Prey, HELs, Net Guns and Nets, HPM devices, GPS Spoofers, and RF Jammers. While none of them are permitted yet due to official regulations.

Net Guns are highly suitable due to lower collateral damage risks at airports. EMPs, RF Jamming and GPS spoofing have higher collateral damage risks, but can yield successful results when used correctly.

For discovering how the implementation of an advanced anti-drone solution could benefit your airport, contact our team, available at *info@usdgs.com* or visit us at *www.usdgs.com.*

Dynamite Global Strategies, Inc

7260 W. Azure Dr Ste 140-2518
Las Vegas, NV 89130, USA

https://usdgs.com

info@usdgs.com