Drone patrol

Radio frequency cyber technology can help combat the dangers posed by the growing number of rogue drones flying close to airports and, in some cases, breaching the perimeter fence, writes Jeffrey Starr, CMO of D-Fend Solutions.

Drone sightings and incidents around airports have increased significantly in recent years. Since the beginning of 2023 alone, there have been serious drone incidents at airports in Edinburgh, Madrid, Palm Beach, and famously, multiple incidents in Dublin.

At Edinburgh, flight departures were disrupted and delayed due to an unauthorised drone near the runway. A drone also caused delays at Madrid-Barajas Airport when it was spotted by an incoming flight from Paris.

In Palm Beach, a pilot reported a drone right off the side of an aircraft. Flights have also been suspended at least six times since January at Dublin Airport, causing the diversion of flights to other airports.

As drones proliferate, with increased popularity, greater ease of use, and cheaper prices, the likelihood of incidents near airports rises and the risk they pose to airports grows increasingly higher.

The implications and economic impact are enormous, as reflected in grounded flights, missed connections, angry passengers, and lost revenues.

Indeed, the after-effects of a drone incident can lead to serious consequences and substantial financial costs. Therefore, rogue drones operated by the criminal, careless or clueless create many challenging situations for airports.

Policymakers and regulators around the world have been taking steps to deliver strong messages that operating unauthorised drones near airports is illegal, and could lead to financial penalties, criminal charges, and even imprisonment.

The safety risk is significant. A *study* from the Canada National Research Council's Aerospace Research Center showed that common commercial drones with heavy payload capacity can cause serious damage to aircraft, including shattered windshields, penetration and inhalation hazards, lost optics and ultimately may require emergency landings after collision.

Even at slower speeds, such collisions were shown to be able to cause plastic damage and extensive deformation to the skin, as well as additional damage to the aircraft's internal honeycomb structure.

At higher speeds, collisions were shown as capable of causing severe deformation of slat curvature, damage to the leading edge, and even possible penetration of drone debris into the aircraft's fractured area.

The drone threat to aviation includes multiple types of dangers. The most obvious is a careless user risking a collision. A bad actor could want to make an attack. Espionage or surveillance for future incursions is also a risk.

In addition, there are lots of scenarios to consider beyond just everyday aviation. A VIP visit, for example, may pose additional factors requiring extraordinary preparations against a threatening drone.

The risks associated with a drone crashing into a plane, or being used for an attack, has caused many airports to start evaluating options for effective and specialised counter-drone technologies that are suitable for the unique and sensitive environments of an airport

Traditional countermeasures have issues at airports

Reaching desired levels of airspace safety in the context of increasing rogue drone activity has proven to be particularly challenging.

Many counter-drone technologies originated from the military realm. They have performed well in the environment for which they were originally designed. However, when they enter the sensitive airspace of a civilian airport, many glaring shortcomings become apparent.

For drone detection, radar has played a role for a long time, but in an airport environment radar may generate false positives from not always being able to clearly distinguish between a drone and other flying objects such as birds.

Optical systems require a clear line of sight, which can be difficult in urban environments or hilly terrain. Acoustic methods are challenged by noisy airport environments and increasingly quiet drones.

Radio frequency (RF) based methods such as directional finders may not be able to locate and track the drone to the highest degree of precision.

The challenges are even more steep when considering mitigation, especially when again looking at countermeasures that came from the military sector.

Jamming could be prohibitively problematic to a sensitive airport environment, given the possibility for disruption to communications and operations. It's also temporary by nature, and the rogue drone pilot could regain control when jamming ceases.

Any type of kinetic, that is physical mitigation method involving shooting some sort of projectile at the drone, carries with it the serious risk of collateral damage, either from the projectile itself or the downed drone and resulting debris.

The search for detection and mitigation countermeasures suitable for airports

It's become increasingly clear that sensitive airport environments would benefit most from a safe and innovative defense against rogue drones. Technology should also conform and evolve with current regulations and be future-ready as regulations rapidly evolve to confront the recognised threat.

An ideal solution could encompass both passive detection to raises the airport's situational awareness, with a migration path to eventually extend to also include full, seamless, and simple mitigation capabilities, as policies and regulations permit.

A new technology optimised for airports

A new generation counter-drone technology, RF cyber, is showing promising results for airports for both detection and mitigation. An RF cyber-detection solution facilitates agility, enabling airport security personnel to quickly adapt.

Unlike the legacy anti-drone technologies, cyber-detection detects and tracks both authorised drones and rogue drone threats, providing situational awareness along with a rich set of capabilities, including tracking drone location, home location, and drone operator location, accurately and in real-time.

Airport security staff can then choose how to utilise the information to contend with the risk and achieve optimal operational continuity.

When permitted by local regulations and policies, and performed by authorised security agency staff, RF-cyber takeover mitigation capabilities can be activated.

Detecting and, when permitted, mitigating the rogue drone threat quickly and efficiently can help maintain safe airport operations. Such a system could assert control over rogue drones and land them safely in a designated zone, as allowed by regulations and performed by the authorized personnel.

Airports could be empowered to detect threats without excessive burden on human resources, disrupting communications systems, or damaging existing infrastructure.

The system would understand the unique identifiers of each drone. Once a drone is classified as 'authorised', it would be labelled as such and be allowed to fly undisturbed in defined areas. The ability to distinguish between authorised and unauthorised drones would ensure continuity for drones performing essential functions at the airport.

The cyber counter-drone system must include stationary configurations specially designed for the unique requirements of airports, with enough long-range coverage for airport deployments to protect the airports' airspace.

The sensors must protect the approaching and take-off air corridors. The hardware should be designed to withstand any extreme environmental conditions of the airport's location.

Airport security, safety and continuity would be further facilitated by preventing the drone pilot from regaining control over the hostile or rogue drone, thereby smoothly mitigating the threat.

Airport authorities could receive preventative alerts while providing crucial data – such as drone take-off and pilot remote control locations, so authorities can deal with specific flights and dispatch appropriate personnel.

Airports rely on uninterrupted operations. A new generation of RF cyber detection and mitigation technology could help assure that airport operations continue to run as usual. Continuity prevails as flights, communications, security and everyday life in the protected airport area proceed smoothly. AW