D-FEND SOLUTIONS

Airport Counter-UAS:

Cyber Detection and Take-Over Mitigation as an Essential Enabler to Business Continuity

By **Philip Butterworth-Hayes**
Editor and Publisher of Unmanned Airspace
A White Paper from www.unmannedairspace.info

UNMANNED AIRSPACE

PHILIP BUTTERWORTH-HAYES

Philip Butterworth-Hayes is a consultant and writer specialising in air traffic management, aviation safety, military, and civil aviation issues. He was formerly Managing Editor of Jane's Transport Press and editor of Jane's Airport Review, Jane's World Airlines, Jane's Defence Industries and Jane's Aircraft Component Manufacturers. He has been the Director of Communications and Strategy at the Civil Air Navigation Services Organisation in Amsterdam and is currently the editor of Skyway, the official journal of EUROCONTROL, the European Organisation for the Safety of Air Navigation. He is the editorial director of PMI Media Limited, specialist contract publishers for the defence and aerospace industries, whose clients have included the European Defence Agency and Airbus Defence and Space. He is a regular contributor on ATM and aviation safety issues to global broadcast and print media, including the BBC, CNN, and the Wall Street Journal.

THE STATE OF THE DRONE THREAT AT AIRPORTS: HEIGHTENED AWARENESS

Many of the world's airports now have a relatively good awareness and understanding of the challenges involved in identifying and mitigating rogue drone incursions in and around airports, including both the airfield zone and its surroundings.

Airport operators are becoming acutely aware of not just the safety implications but also the costs to their business of drone security incidents. The 2018 drone disruption at London Gatwick airport disrupted about 1,000 flights, affecting more than 140,000 passengers. The economic loss of the 33-hour disruption have been estimated at approximately EUR55.8 million, primarily to airlines

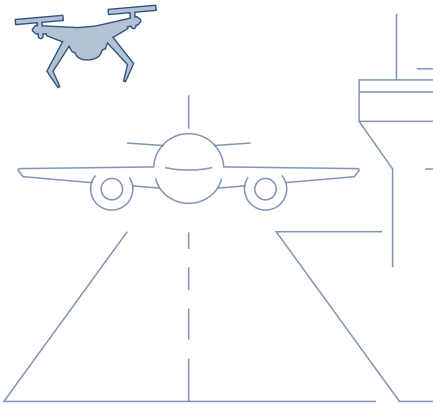
INCIDENTS PERSIST

Yet the number of airports whose business has been interrupted by rogue drones continues to rise; since the beginning of 2023, there have been serious drone incidents at airports in London, Edinburgh, Madrid, Pittsburgh, Palm Beach, and Dublin, among many others. And the number of incursions is growing. Towards the end of 2022 Norway's Oslo Gardermoen Airport was experiencing fifty drone alarms every month.

The drone threat is now more than just the sudden appearance of a consumer drone in or around the airport, piloted by an inept or malicious operator. As the use of drones increases, along with their range and capabilities, the threats are multiplying. From environmental protesters taking to the skies to disrupt airport operations with drones, to militant activists that have used armed drones to attack airports.

C-UAS IMPLEMENTATION IMPLICATIONS

So, implementing a network of effective Counter-Unmanned Aerial Systems (C-UASs), on a multi-agency basis, is now understood by the global airport community to be an essential capability, especially as airports start to integrate drone missions into their own operations – for navigational aid inspections, deliveries, perimeter security and aircraft maintenance.



This requires airport operations/ATC staff to understand the unique identifiers of each drone; once a drone is classified as 'authorised', it can be labelled as such and be allowed to fly undisturbed in defined areas. The ability to distinguish between authorised and unauthorised drones is vital to ensuring the safe and efficient management of drone operations at airports.

Associations such as ACI International have developed important guidance material on how airports can implement Drone Fly Zones:

> *The most common prevention measures in place are drone fly/no fly zones applicable to drone operations. These zones typically relate to drone operations below 120m (400ft) above ground level (AGL) and within 5 km of a protected aerodrome that potentially affect operations over the movement area, runway, or approach/departure path of that aerodrome. The Drone Fly Zone (DFZ) concept improves the information available to drone operators when planning to operate in areas where a specific clearance is required.*
> ACI

And there are new disruptive aviation actors about to enter the skies above airports whose growing activities will need to be further integrated within the airport eco-system. Air corridors in particular need special care and focus on monitoring and protection due to their vulnerabilities.

> *Many airports are looking to seize opportunities to incorporate drones, electric Vertical Take Off and Landing (eVTOL) aircraft, and other vehicles into their operations. However, this integration will come with its own set of challenges. This rapidly expanding segment of air transport activities has resulted in airport operators' awareness and consideration of the potential impacts these operations will have on their airport in the future.*
> ACI

THE STATE OF C-UAS TECHNOLOGY FOR AIRPORTS

The ability to detect, identify and track rogue drones while making room for friendly new entrants has improved considerably over the last few years. The ideal airport airspace management system with an integrated C-UAS capability is a "layered" one, which means employing several sensors – radar, RF detection, acoustic, optical – integrating information from these sensors into a command-and-control system which gives the operator an early opportunity to differentiate between friend and foe with no false alarms. And, if foe, detailed data to provide clues about the intention of the operator.

C-UAS CONSIDERATIONS

"The installation of counter-UAS systems in airports needs careful consideration."

In order to protect people, aircraft, and infrastructure, and ensure the efficient operation of the airport, there are a number of technologies providing C-UAS solutions. Those solutions are varying in technical design, services, and capabilities based on the needs of the airport. The implementation and use of technologies must be proportionate to the level of threat defined. As every airport has unique needs (geography, environment, economics, and threats) all counter-UAS solutions will differ from one another. A complete C-UAS system solution could take into consideration the following elements to prevent the disruption of airport operations and/or would assist the restoration of normal operations:

- Detection.
- Tracking.
- Identification, Threat Assessment and Classification.
- Neutralization or interceptions.
- Command and control.
- Operational instructions.
- Integration into normal operation (ATM, local authorities...).
- Training of operators.
- Accurate reporting

For an airport, the objectives of these solutions are to:

- Protect people and infrastructure.
- Prevent accidents.
- Ensure efficient operation.
- Integrate into the normal operation the airport systems and operations

The C-UAS detection systems can be in turn based on different technologies. Many combine a set of these different technologies in order to provide a more robust detection, tracking, and identification capability. Identification technologies are comparable to detection systems. All solutions have potential limitations and possible impacts that need to be explored for the specific environment and understood before deployment. All solutions have a limited detection performance which depends on varied factors according to the type of sensor, configuration, etc. Consequently, the installation of counter-UAS systems in airports needs careful consideration as every technological solution such as neutralization technologies cannot be a "stand-alone" option for decision-makers as it presents both advantages and disadvantages.

INTERPOL Drone Countermeasure Exercise Report, page 21

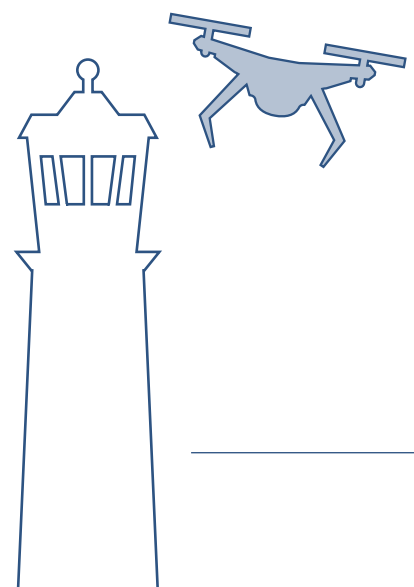
But no detection system will ever be perfect. As drones proliferate and their operators gain new insights into ways of avoiding detection there will need to be a continual review of C-UAS capabilities to ensure they stay ahead of the threat. For example, new threats emerge in the form of modified or adapted drones that may not comply with identification systems such as Remote ID. C-UAS systems should be able to detect and provide early warning for even such modified drones.

Airports have a key role to play in gathering as much granular data as possible in logging incidents so persistent offenders can be identified and the information can be passed to the police or other investigating authorities. For any airport, it is important that the data they capture is in a standardised format which can be used for forensic analysis and acceptable as evidence in legal proceedings. Data analysis tools should enable not only the logging of data but also the ability to investigate cases around drones tagged as suspicious and provide early warning if they reappear.

But sometimes logging and investigating incidents is not enough.

The most effective C-UAS systems integrate detection, identification and tracking with mitigation measures. Security agencies tasked with the responsibility for dealing with an emerging airport drone threat are very limited in the mitigation measures they can employ in an airport environment, as the standard methods for dealing with rogue drones (net capture systems; jamming/spoofing; counter-drone drones; munitions and missiles; directed energy) cannot be employed in an airport.

Mitigators		
Technology type	Strengths	Weaknesses
Net capture systems	Reduces the risk of collateral damage.	Difficult to get into the correct position to deploy. Limited range. Normally a "one-shot" capability – if they miss, the drone escapes.
Jamming/spoofing	Relatively low cost, portable.	Difficult to get into the correct position to fire. Limited range. Will normally interfere with airport/ATC/airline communication/navigation systems, posing safety risk, and will prevent similar but friendly drones from operating. May be less effective against newer drones with counter-jamming AI.
Counter-drone drones	Very precise engagements	Expensive, rely on accurate targeting, normally only capable of engaging a single target. Collateral damage likely. Extremely unreliable vis-à-vis fast flying drones.
Munitions and missiles	Currently available systems can be adapted to C-UAS operations with training	Rely on accurate targeting, with heavy risk of collateral damage. Very few civil applications and certainly not at airports. Not always effective against small drones.
Directed energy	Very precise engagement	Still in its infancy. Expensive, requires high power, accurate long-range targeting and with some weather limits. Mainly a military solution.



Ideally, the same team who detects rogue drone activity should also be the team that undertakes to resolve the problem, though in most of the world this is not yet the case. In an operational environment speed is the key – and the priority is to detect the threat at the earliest possible opportunity, identify the drone type and operator, understand possible intent, and then seamlessly apply an appropriate resolution.

Depending on local regulations, authority for detection and mitigation may be distributed across multiple security agencies. C-UAS systems should be able to accommodate processes which align with the need for such cooperation.

EMERGENCE OF A NEW CATEGORY C-UAS – CYBER DETECTION AND TAKEDOWN MITIGATION

For airports in recent years cyber take-down has emerged as one of the most effective and precise methods of disabling rogue drones by taking over control and landing the drone in a safe area or returning it to its take-off position. It gives airport operators a new level of control over their airspace.

Cyber take-over systems passively detect RF transmissions, based on the protocol or frequency the drone is operating, identify the drone model serial number and the operator position via a function linked to a knowledgebase of known drone characteristics. Following detection of an authorized drone, mitigation can commence.

How an airport cyber take-over system works

D-Fend's EnforceAir seamlessly detects, and tracks authorized and rogue drone threats, providing a single holistic threat picture and situational awareness along with a varied set of capabilities, including tracking drone location, home location, and drone operator location, accurately and in real-time. Airport police and security staff can then choose how to utilize the information to contend with the risk and achieve optimal operational continuity. When permitted by regulations, EnforceAir's mitigation capabilities can be easily activated. EnforceAir empowers airports to detect threats without excessive burden on human resources, or disrupting communications systems, or damaging existing infrastructure. EnforceAir can read unique identifiers per drone. Once a drone is tagged as "authorized" and recorded on the authorized list, it can be visually monitored while it flies undisturbed in defined areas of the airport. EnforceAir's ability to distinguishing between authorized and unauthorized drones ensures continuity for drones performing essential functions at the airport.

Airport security, safety and continuity are further facilitated by EnforceAir's preventing the drone pilot from regaining control over the drone, thereby fully and smoothly eliminating the threat.

EnforceAir can also provide airport authorities with 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.

CYBER C-UAS - OPTIMAL FOR AIRPORTS

There are many clear benefits to such a technology: it is surgically precise without causing collateral damage; it allows for operational continuity as the incident is being managed (and for authorised drone operations); it provides a proportionality of response; it can be configured for both mobile and static applications; it gives the C-UAS operator considerable flexibility in defining the defensive envelope; it allows for a precise analysis of incidents, which can be used for forensic reporting; it can be constantly updated to take account of new threat types.

The technology is now available, as allowed by relevant national and local detection and mitigation regulations and authorities, so airports can move from reactive to proactive mode in managing drone operations in and around their facilities. Low level airspace of the future will be vastly different from that of today. As beyond visual line of sight (BVLOS) and autonomous drone operations multiply, the need for airports to manage their airspace in a more systematic way to ensure business continuity at all times is becoming a new imperative. Cyber takeover is a key enabler in this regard.

D-Fend assisted in the compilation of this white paper.