Preventing another Gatwick incident

Ben Marcus, Chairman, AirMap, explains the three steps needed if drones are not to continually disrupt airport operations.

From 19 December to 21 December 2018, 67 reports of drone sightings close to the runway of Gatwick Airport resulted in the cancellation of hundreds of flights and brought chaos for an estimated 140,000 passengers.

In the weeks since, it is estimated that the aviation industry has suffered a loss in revenue of between £50 million and £70 million.

Regular operations have since resumed at Gatwick, but reactions by the UK police, military and government officials exposed a lack of preparation in responding to unlawful drone incursions and have left the rest of the world questioning the ability of air navigation service providers, civil aviation authorities, governments and airports to manage such a crisis.

As of writing this article, the perpetrator(s) remains at large, and further suspected drone sightings also affected Heathrow Airport on 8 January 2019 and Newark Airport on 22 January 2019.

Many early reactions have called for counter-UAS technology as the most effective solution for prevention. Of course, there is a key role for counter-UAS (unmanned aircraft systems) in airport safety, but they are a last resort against criminals. Without the ability to remotely identify the good actors from the bad ones, these counter systems will be constrained as drone operations increase.

Thankfully, a lot can be done today to reduce the risks of drone incursions to a manageable level that only requires basic regulation and technology. Here are three concrete steps that airports and aviation authorities can take to keep airports safe from unwanted and/or criminal drone activity.

Step 1: Implement a registration mandate with reliable, easy-to-use technology.

Airspace authorities should establish clear regulations that require all drone operators to register themselves and their aircraft along with a simple, streamlined process for doing so.

Implementing a digital registration system is relatively easy – drone operators can enter name, contact, and aircraft details on an Internet-enabled device, which populates a secured registration

Credit: iStock.com/abadonian

Many airports, ANSPs, civil aviation authorities and governments around the world are not yet prepared to respond to drone incursions.

server, that also confirm identities and authenticate users. Access to registration data is managed by authorised personnel, with appropriate protections in place.

Mandatory registration can also require that a drone operator self-identifies to get authorised access to fly in controlled airspace near airports. Registered operators are responsible actors who have demonstrated intent to operate in compliance with regulations.

Step 2: Enforce civil aviation regulations with a UAS traffic management (UTM) system.

Popular drone manufacturers already implement geofencing options and firmware updates to meet national airspace regulations. In practice, geofencing prevents a drone from flying in restricted, controlled and other unsafe airspace, which helps ward against illegal drone operations by careless and clueless operators.

Geofencing can be unlocked for authorised drone operators, such as airport maintenance staff or law enforcement operators, by connecting to a UTM system with services and procedures designed to support safe, efficient and secure access to airspace for drones.

These services include registration, flight planning, geofencing, airspace authorisation, conformance monitoring, telemetry, deconfliction, and remote identification, among others.

The right UTM system analyses operator details, flight path information, real-time air traffic positions and more to enable airspace authorities to grant permission-based access to drone operators in controlled airspace, either manually or programmatically. The result is enablement of safe drone operations while controlling against non-compliant or illegal activity.

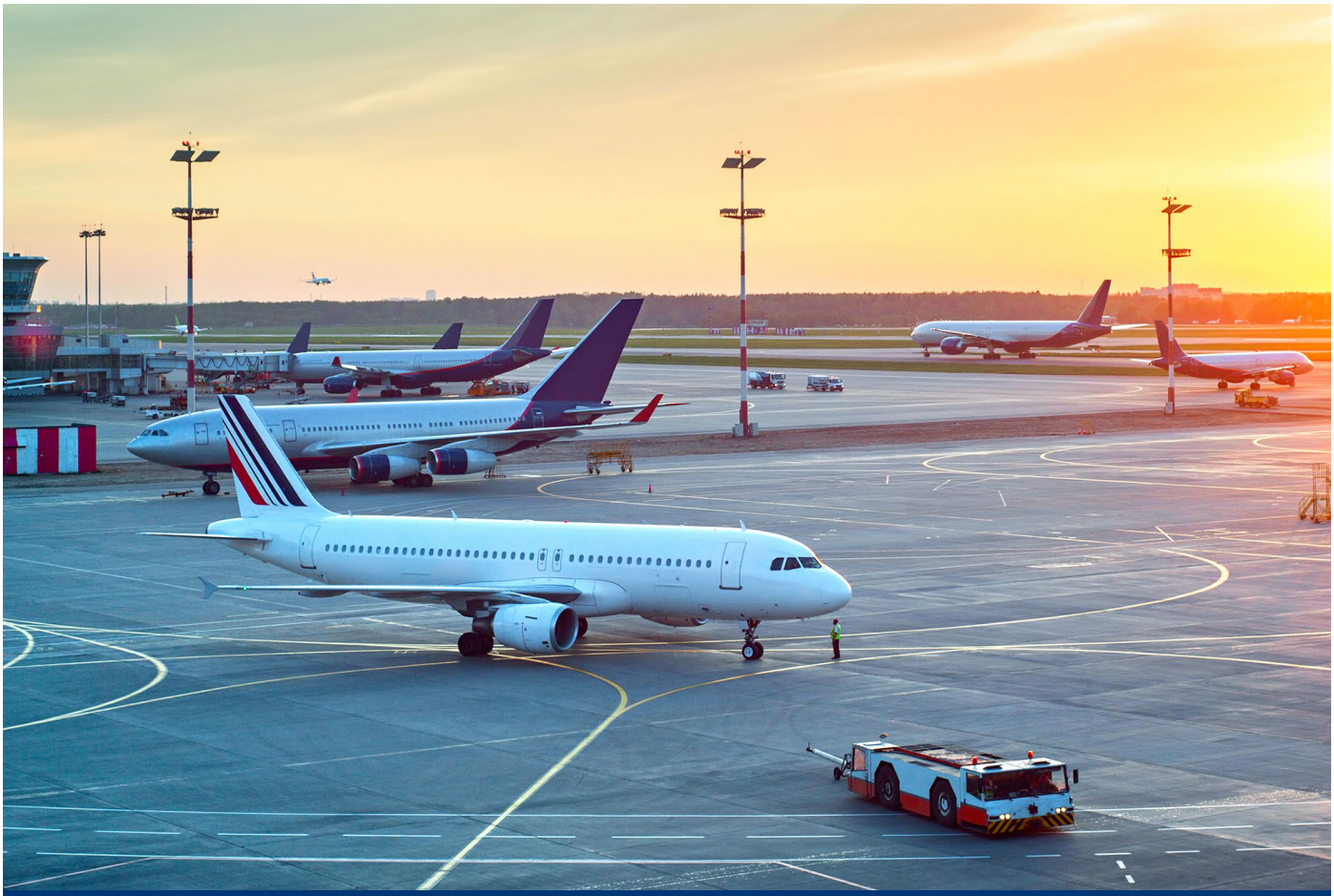
With all good actors participating in the UTM system, aviation authorities can visualise, monitor, and track real-time manned and unmanned aircraft telemetry for deconfliction. Participating drone operators can be remotely identified by their aircraft, flight path, and/or registration details and can be contacted directly for risk mitigation.

Step 3: Combine UTM with counter-UAS (C-UAS) system for a complete picture of an airspace operating environment.

Intentional bad actors may hack their drones, unlocking geofencing, or spoofing their location.

In these instances, the integration of counter-UAS (C-UAS) technology into the UTM system provides the ability to identify all aircraft movements within the controlled airspace. Information related to any aircraft detected by C-UAS is exchanged with the UTM system and remotely identified as either collaborative (registered) or non-collaborative, requiring intervention.

Much of the reaction to the Gatwick incident has centred on C-UAS technology as the answer to all illegal drone operations. But as drone operations near airports increase with enterprise demand, C-UAS alone will not be sufficient in determining whether a drone operation requires intervention because not all drone operations at airports are unlawful. Detection must be coupled with UTM intelligence to adequately inform and ensure the safety and smooth operations of all airports.



Credit: AirMap

The right UTM system will enable airspace authorities to grant permission-based access to drone operators in controlled airspace.