COMBATTING THREAT

Paul Hicks *examines what can be done to protect airports from drones as well as revealing measures that can be actioned to prevent misuse*

Coronavirus aside, at this time of year airports would otherwise be relied upon by thousands of domestic and international passengers every day. In 2019, some of the UK's biggest such as London Heathrow – the second busiest airport worldwide – recorded their busiest years on record with 80.9-million passengers passing through. In addition to passenger numbers, UK airports handle more than 2-million tonnes of freight annually, as well as providing 960,000 jobs and contributing an estimated £52-billion gross value added to the economy.

Safety at airports is therefore paramount. Health and safety requirements are uniquely stringent given the type of vehicle and equipment operating near high concentrations of people and valuable cargo. Airport authorities, however, now face a new challenge with the growing prevalence of unmanned aerial vehicles (UAVs), or drones. Although used largely for legitimate purposes, high-profile incidents such as the infamous December 2018 Gatwick Airport drone situation highlight the potential for malicious drone usage to cause life-threatening and economic consequences.

The question for airport authorities, then, is what is the most effective way to prevent and defend against unauthorised drone usage in and around airports?

Drone usage has risen exponentially as UAV technology develops. This is driven by markets for both leisure and commercial use. PwC estimates there will be 76,000 commercially operated drones in the UK's skies by 2030, creating over half a million jobs in the process and injecting a £42-billion increase in UK gross domestic product.

As companies seek more efficient, innovative and ambitious methods in how they deliver services, drones offer an unparalleled option. Gathering data quickly and accurately from hard to reach places, they can create record data in real-time. This can make a crucial difference in managing costs, controlling risks, increasing safety, and influencing outcomes. Drones are increasingly being tried and tested across an array of industry sectors including, ports, agriculture, defence, mining, construction and the emergency services.

UAV technologies even have the potential to offer many benefits to airports and airlines. Drones can support airport operations by performing maintenance and inspection activities, including delivery and bird control. With the ability to cover a surface of more than 200 thousand square metres, they can create an extremely high-resolution image of the runway. Drones can also be used for observation or tactical planning. Therefore, their use has become very common in a wide range of applications, but despite technology advancements most of these systems still require a remote pilot to guide the aircraft.

However, as we're all too aware drone misuse, unintentional or otherwise, is rising as more people deploy them. Figures from the Civil Aviation Authority show that British consumers purchased 530,000 drones in 2014 and that over the Christmas period in 2017, a further 1.5 million were anticipated to have been sold. As sales continue growing exponentially, the requirements of infrastructures critical to the UK economy must be considered and their relevant authorities prepared.

> POLICE ARE RETICENT TO SIMPLY SHOOT DOWN DRONES BECAUSE IT'S NOT ESPECIALLY SAFE

Over the past few years, the number of invasive drone incidents in and around airports has risen. Whether accidentally or deliberately, unauthorised drone usage is a serious safety hazard that requires an appropriate and immediate response.

Between 19 and 21 December 2018, Gatwick Airport, and thousands of its customers, fell victim to the highest profile drone incident to date. Drone sightings close to the runway necessitated an immediate halt to flights from the airport, affecting approximately 140,000 passengers and 1,000 flights. The cost to the airport and airlines, due to damages and loss of earnings, totalled £50-million after the airport was closed for 30 hours at peak Christmas travel time.

During the incident, both the RAF and army were deployed to tackle the apparent threat to the airplanes operating on the runway. Supt Justin Burtenshaw, head of armed policing for Sussex and Surrey, described attempts to catch whoever was controlling the drones as "painstaking" because it was "a difficult and challenging thing to locate them". The policing operation during the disruption and subsequent investigation cost £790,000. At the time, questions were asked as to how a still-unidentified drone operator was able to cause so much disruption. Police are reticent to simply shoot down drones because it's not safe: stray bullets can end up anywhere. The industrial specifications of the drone used at Gatwick meant it was harder to track than a standard personal-use drone. Yet a commercial-sized drone is still unlikely to appear on radar detection. And with so many anti-drone options on the market, but no industry-wide consensus on the most effective yet feasible deterrent, a lack of uniform response enabled the perpetrator to cause so much disruption.

It's estimated that there will be 76,000 commercially operated drones in the UK's skies by 2030

The incident at Gatwick prompted reactions from the top of the Government, with then Prime Minister Theresa May issuing a statement condemning malicious usage. Other senior political figures called for tougher legislation. Additional police powers were granted, and legislation was rushed through by the Government. In 2019, legislation was introduced by the Civil Aviation Authority – the UK regulator – requiring drone users to take an online test and pay a £9 annual fee or face a £1,000 fine. On 13 March 2019, new restrictions on use near airports were introduced with the risk of charges for a criminal offence for those who choose to flout them. Drone users are also strongly encouraged to familiarise themselves with the Drone Code, which emphasises safe usage.

Legislation and guidelines can only do so much, however. Practical detection and defence systems are necessary. Since the Gatwick incident, the drone issue, if it wasn't already, has become a priority for airport safety decision makers. The incident highlighted the potential risks and challenges the UK's, as well as worldwide, airports are faced with. Both Heathrow and Gatwick invested millions to install military-grade anti-drone apparatus following the December 2018 incident. The fact that the army had to deploy its own defence system during the incident – allowing operators to jam radio signals and allow safe landing– is indicative that airports weren't ready to deal with malicious invasions.

The question for them now is: what drone mitigation solution is the most effective, safe and cost-efficient?

Varying solutions have been developed to tackle invasive drones. A giant gun-like device has been developed which can supposedly jam 2.4 and 5.8GHz frequencies used for their remote control, meaning that jamming will not interfere with manned aircraft, mobile phones or other radio bands and can shoot down the device from 2km away. Another method is GPS geofencing. This means a drone's software will prevent it from entering certain geographical areas that have been listed as prohibited. There's a 30-nautical mile radius around the Ronald Reagan Washington National Airport where drones aren't able to fly, for example. The idea of net cannons mounted onto other drones has also been explored. In 2016, Dutch police were experimenting with training eagles to swoop and pluck rouge drones out of the air like prey. Organisations and businesses must begin combatting unauthorised usage effectively now, rather than later. To avoid the scenario of unexpected incidents, akin to the Gatwick one, a solution that can provide adequate protection needs to be adopted. By not putting measures in place, drone attacks could cause major disruption to national infrastructure and, in a worst-case scenario, cost lives.

UNAUTHORISED DRONE USE IS A SERIOUS SAFETY HAZARD REQUIRING AN APPROPRIATE RESPONSE

Developed in response to the significant rise in drone incidents, telent and Digital Global Systems (DGS) CLEARSKY have come together to deliver a Drone Threat Management System (DTMS). This has the ability to protect stadiums, large public venues, airports and utility facilities from the unpredictable threat of unauthorised and malicious drone usage.

With the capability to detect drone activity from up to 2km away, any associated potential threats can be easily and appropriately responded to. What's more, it can also locate the drone operator, monitor the flight path that the drone is undertaking and identify the type of drone. The system doesn't require hours of training for the controller and allows ground teams to rapidly deploy it.

The DTMS uses passive radio frequency (RF) monitoring rather than radar, which means it does not interfere with other equipment and radio-based services. It monitors a wide range of spectrum from 50MHz to 6GHz, to monitor both the commercial drone frequencies and outside the normal range to detect modified models. This patented technology also automatically captures, interprets, locates and alerts on rogue wireless signals, preventing unauthorised personnel from stealing key information. This ensures users are able to capture and store threat data quickly so the authorities can also use it effectively as evidence for any legal proceedings that may arise.

When it comes to tackling unauthorised or malicious drone flights, the instant reaction is to bring it down immediately, but in most situations, it is illegal to interfere with a drone's flight path. More so, by doing this it can also present safety risks to people on the ground. What's even more complicated are swarming drones, which cooperate and communicate with one another as they go on the attack.

In circumstances like this, the best response is detection. This means organisations need to ensure they have the right tools in place to protect their assets from the unpredictable threat of unauthorised and malicious drone usage. Looking ahead, as the devices become more commonly used, stadiums, large public venues and airports need to start investing in drone management technologies, before they find themselves at the forefront of an attack.

As technologies and artificial intelligence continue to move forward, having the right strategy in place to protect your organisation is crucial. Whether used for good or bad intentions, drone usage means they will be increasingly more prevalent on both the runway and in everyday life ●

Paul Hicks, Head of Wireless at telent Technology Services, joined telent Technology Services as Wireless Head of Sales in 2012 and is responsible for developing new business within the wireless sector.

A commercial drone is unlikely to appear on radar detection

Picture credit: Getty