Securing our airports

The unauthorised intrusion of a drone over Gatwick airport has triggered calls for more effective counter measures. By **Neil Tyler**

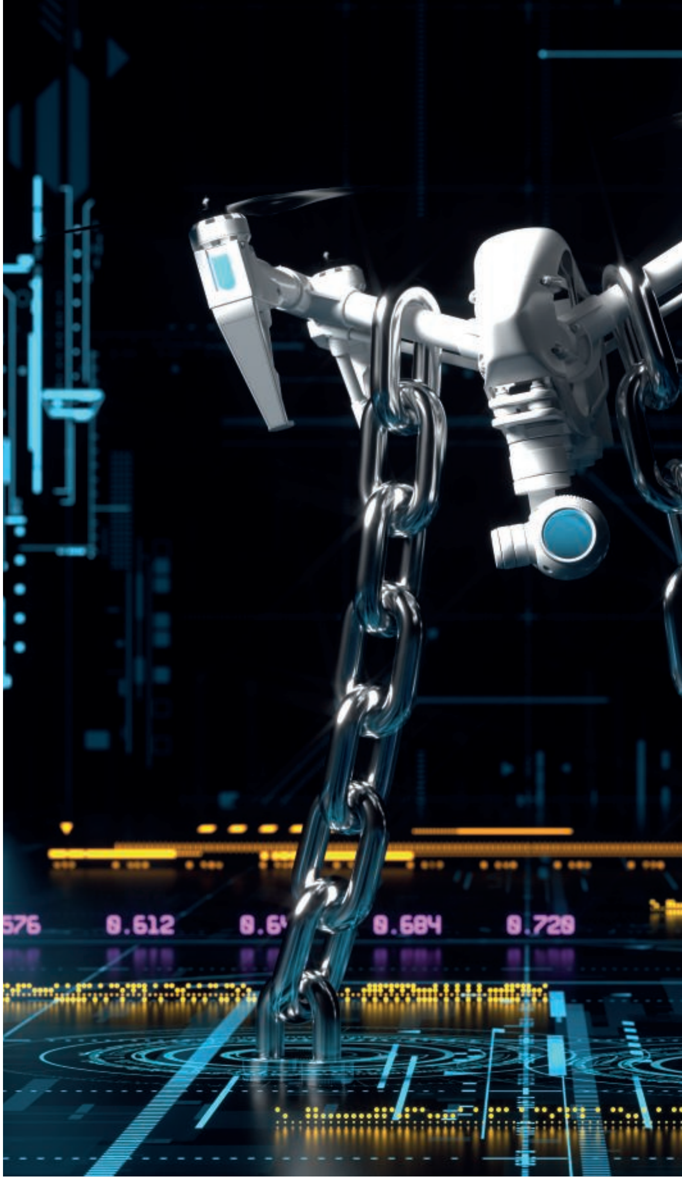

Illustration: Oliver Burston

At the end of 2018 Gatwick airport and the UK authorities were forced to bring in military teams, using advanced techniques developed on the battlefield, to search for an unauthorised drone buzzing the airport's runway.

Although no drone or pilot was found, the impact on the airport was serious and Gatwick was closed for an unprecedented 33-hours.

The economic impact only came to light in January when the budget airline easyjet said that 80,000 passengers had been caught up in the 'mayhem' and that it had to cancel over 400 flights, at a cost to the airline of over £15million.

In total 1,000 flights were disrupted with over 140,000 passengers inconvenienced, suggesting the total cost to the airport and industry was anywhere between £50-100million.

The Chief Executive of easyjet, Johan Lundgren, described the closure as a "wake-up call to airport operators around the world."

According to Geoff Moore, business development manager at Blighter Surveillance Systems, "The events at Gatwick really didn't come as a surprise. The industry has been talking about this kind of event for some time.

"Airports are a commercial operation and most of the regulations concerning them are not mandatory, there is nothing currently in place to defend airports against drones."

Richard Gill, CEO of Drone Defence added, "All airports face various demands on limited resources when it comes to mitigating risk. Up until easyjet's impact assessment, which worked out at around £1.5million per hour, the industry didn't have a benchmark figure to work with. Now with actual figures they can start to create a realistic budget to counter this threat and invest accordingly."

Moore said, "Managing an airport is about managing risk and now we can put a cost on disruption caused by drones."

As drones become more popular more are now being fitted out with high quality photo/video sensors and can operate with considerable power reserves, giving them a much wider field of action.

"While the number of commercial flights in the air at any one time totals around 15,000, there are millions of drones in operation," said Moore, "and as more piloted and semi-autonomous drones enter our air space so there will be more accidents or near misses."

British and US authorities have recorded a growing number of collision alerts but, while the risk of collision may be growing, of greater concern is the payload capabilities of certain drones which could be used for terrorist activities.

As a result, securing airports against unauthorised intrusions by drones is now being taken more seriously.

"To counter the threat of drones you need to look at a range of counter drone technologies. You need to invest in a significant amount of equipment - radio frequency spectrum analysers, direction finding antennas, radar and video, all have a part to play. Different detection systems have different capabilities," Moore explained. "To effectively counter drones you need to deploy a combination of these technologies to be effective and that will be expensive."

Much of the focus with anti-drone technology tends to be on specialist radar and thermal imaging techniques - the aim being to detect, track

and then identify the drone and its operator.

As Moore explained, “You can use a simple acoustic device, a microphone, to track a drone which will have its own unique acoustic profile. But then you have to manage background noise problems.

“Video is another solution, but the sky is a big place and it’s not easy to track a small device with an optical camera. It’s best to deploy thermal management techniques but thermal cameras are not only very expensive but provide only limited resolution – video tends not to be an appropriate solution when combating drones.

“You can use radio frequency monitoring, but that only works if the drone is being piloted,” Moore continued.

With drones that are operated by radio waves it is possible to use a direction-finder to locate and challenge the drone’s pilot and then use jamming in all its forms (directional, omnidirectional, variable frequency ranges, etc.) to interrupt the flow of data between the drone and its ground station as well as the GPS-guiding system. Jamming the video can also stop the drone from transmitting its images, so making the intrusion pointless.

Jamming implementations

Drone Defence has developed a range of solutions to combat drones that target radio communications.

“We focus on the link between the drone and its pilot,” said Gill. “We have developed a RF detection system and can offer real-time awareness and, where required, we can enhance the system with other sensing technologies like radar, cameras and acoustics.”

The company has developed SkyFence, an electronic countermeasures system which prevents drones from flying into or close to a protected location by disrupting its command and navigation radio transmissions.

“We can use multiple low-powered radio transmitters which are strategically placed around a protected site – for example, on the perimeter fence of an airport. These devices would be placed every 40 feet along a fence and when activated would transmit a signal which is designed to overwhelm the drone’s radio transmissions. This breaks the control and video link between the drone and its operator,” explained Gill.

Jamming signals can be transmitted on GPS to force the remote pilot to navigate the drone themselves, provide the aircraft with an incorrect GPS solution (forcing it off course), disrupt communications which removes control from the remote pilot and possibly force the drone into a controlled landing.

The limiting factor on these types of counter-drone systems is that many countries have laws in place that restrict the use of jamming capabilities and jamming may only be undertaken with express permission from specific agencies.

Drone deterrence and detection is being affected by the growth in autonomous drones that, “Don’t’ transmit much because they can be pre-programmed. As a result, there’s little traffic between the pilot and the drone,” explained Moore.

Detection, at present, is primarily achieved by using radar, said Moore.

“The B400 from Blighter was designed to provide long range ground surveillance and can detect moving vehicles and people over a wide area.

“It uses Blighter’s passive electronically scanned array (PESA) radar technology which uses digital beam forming on both transmit and receive to help reduce unwanted detections from clutter, so reducing the number of false alarms which is crucial when you’re dealing with what is a very cluttered environment like an airport,” Moore said.

The company’s Anti UAV Defence System (AUDS) was developed to detect drones up to 10km away using electronic scanning radar and uses precision infrared and daylight cameras and specialist video tracking software to track the device before disrupting the flight using an inhibitor to block the radio signals that control it.

“This detect, track, disrupt, defeat process is very quick and typically takes less than 15s,” explained Moore.

The ideal solution, however, would be to use all relevant systems in a given area and merge the data to isolate the identified non-problematic drones from more dangerous intruders

The ease of obtaining drones or unmanned aerial vehicles (UAVs) has bred a vast associated industry, and many industries are using drones owing to their ease of use, availability, cost savings and their ability to perform dangerous tasks.

“The spectrum of adversaries is broad. From the inadvertent actor to those with malicious intent, they are the ones we need to locate, identify and bring down.”
Richard Gill

As a result, drones are becoming an increasing threat to aviation and in the United Kingdom, in the second half of 2017, there were 35 drone-related incidents reported to the authorities. These occurred up to an altitude of 12,000ft but some consumer level drones have a service ceiling of as high as 20,000ft.

So, what are the consequences of an aircraft impacting a drone in flight?

Research conducted by BALPA, in conjunction with the Military Aviation Authority and the UK's Department for Transport, found by using computer simulations that an impact with the windscreen of an aircraft could result in catastrophic damage.

"The smaller hobby drones are not a risk, they are made primarily of plastic. It's when you move to the larger commercial drones," suggested Moore, "those with large titanium cameras could cause a lot of damage."

According to the British Civil Aviation Authority (CAA) all major engine manufactures claim that their engines have been designed to contain engine fragments so that penetration by engine debris of the fuselage, fuel tanks and other critical areas is extremely limited.

Tests undertaken at the Virginia Tech University in the US found that a 3.5kg drone would severely damage the fan blades of a three-metre diameter turbofan engine in 1/200th of a second with drone debris within the engine reaching speeds of 1150kmh.

Whatever the impact drones must be seen as posing a real danger to commercial aircraft.

So, what role can drone manufacturers play in securing drones? China's DJI Innovations, which is the largest drone manufacturer in the world, has included geo-fencing within the app that controls their drones, and this prevents them being operated in areas where aviation safety or national security may be affected.

A website has also been produced by DJI that shows no-fly areas as well as additional safety information that drone pilots can check and the company has also introduced a nine-question knowledge-based quiz on local regulations.

"The spectrum of adversaries is broad. From the inadvertent actor, who simply doesn't know the rules and has no malicious intent, and that's most drone operators, to those with malicious intent, and its those that we not only have to be able to locate and identify but bring down where possible," said Gill.

Currently, counter-drone systems are under development with over 155 companies involved worldwide.

"There are a lot of companies coming into the drone detection space," said Gill, "but many only have a limited risk management background."

Drone regulation

Commenting on the Gatwick incident Russell Haworth, CEO of Nominet said: "Events at Gatwick have highlighted the urgent need for greater regulation of drones. A UK wide drone registry could go far beyond a mere list of registrations - a database could be created to authorise flights in real time, meaning all flights would need explicit permission before they can take off.

He continued, "The upcoming government's Drone bill will hopefully start to tackle this, as well as exploring other options such as geo-fenced 'no-fly' zones that can communicate with a drone's in-built GPS. But progress may need to accelerate to prevent highly disruptive events being repeated."

While Haworth appears to be in favour of greater regulation Gill is concerned that this focus on regulation overlooks the benefits of the technology. A too heavy-handed approach to regulation could seriously impact the industry.

"We shouldn't demonise drone technology, but rather focus on those will malicious intent," Gill warned.

"At present it is possible to access open source drone projects, download designs, buy components from ebay, source code for a drone and, if I want to, I can delete restrictions and spoof the identity of a drone. All of which means that there's obviously a lot the industry will need to do to operate securely in this space.

"However, I think in time the industry will become self-regulating. We'll ultimately see the development of standard Unmanned Traffic Management (UTM) systems. These will provide flight planning, conflict avoidance and manage how drones enter and leave specific air corridors," said Gill.

UTM systems are being developed for low-altitude airspace allowing for safer and more efficient low-altitude operations without requiring human operators.

"Both manufacturers and operators will be happy to develop products that automatically integrate into a national UTM system – hobby drones will be registered and able to talk automatically to those UTM systems."

When it comes to combating drones i.e actually shooting them down, the law remains opaque.

"Current regulations are likely to be relaxed. At present a decision to bring down a drone needs to be authorised by the Home Office, in the UK," explained Moore.

"I think those regulations are likely to be relaxed and police involvement is likely to be increased, but that will require new legislation and a better understanding of how to use anti-drone technology," added Gill.

"Airports need guidance from their regulators as to how to counter the growing threat of drones.

"When is it legitimate to apply jamming technology? What will be the rules of engagement and how will you mitigate any threat?"

"Events at Gatwick have highlighted the urgent need for greater regulation of drones."
Russell Haworth