The sky must have limits—counter-drone technology and regulation

20/02/2019

TMT analysis: In light of global drone attacks on airports and the recent introduction of new measures to combat drone misuse by the UK government, Ruhi Sethi-Smith, barrister at Forum Chambers, looks at the legal implications of counter-drone technology and regulation.

In the recent airport drone incidents, why didn't the police simply shoot the drones out of the sky?

While there have been a number of near misses at national airports prior to this incident, no drones have ever remained in such close proximity to airspace over an airport for a sustained period of time. Therefore, the police had to quickly consider a number of options for removing the threat to aircraft safety.

In the UK, the use of anti-drone or counter-drone technology is restricted to the military. Therefore, the police would have required special permission to be granted before such technology could be deployed. This does not appear to have been an option in this case. Another option considered by the police was to shoot the drones out of the sky, however, it was considered that there was a risk of stray bullets causing injury or death to members of the public in the vicinity of the airport.

The incident has highlighted the vulnerability of the UK's national airports to drone attacks from those intending to cause harm and/or disruption to large numbers of people and the need for greater technological and regulatory protection in order to prevent such incidents in the future.

What is counter-drone technology and how does it work?

There are a number of drone detection and counter-drone systems already available. Firstly, there are drone detectors which can detect the presence of rogue and unauthorised drones in protected airspaces. These detectors can provide tracking and monitoring of any such drones by using radar sensors, electro-optical sensors and infrared sensors. Some detectors use radio frequency to detect flight control signals (emitted from the ground control station to a drone) or video downloads (from the drone to the ground control station) to classify an emission as coming from a drone. Each system has different capabilities and limitations but, generally speaking, drone detectors allow detection at a greater range and can be more reliable than manual visual sightings. Drone detectors also provide security personnel further time to determine whether a drone poses a threat when compared with manual visual sighting and therefore can provide critical information to allow enforcement agencies to deploy a proportionate and effective response to any threats posed.

Secondly, there are electronic or physical effectors, also referred to as defenders, which disrupt or destroy the unmanned aircraft using a number of different methods. Electronic effectors such as 'jammers' or 'GPS spoofers' work in the following ways:

• jamming the command transmission from the control system to the drone and/or of the video transmissions from the drone to the control system which then overpowers a frequency band with noise

• jamming GPS or Sat Nav systems to disrupt drones flying on a pre-planned satellite navigation route

• offsetting the GPS receiver in the drone by simulating false satellite signals to divert the drone to a chosen location

• overpowering the drone's control system to induce the drone's failsafe mechanism or the return to origin setting

The advantage of these systems is that those who need to can respond to a rogue drone in a proportionate and timely manner by essentially preventing the drone pilot to complete the mission. The drone and its data would also remain intact, making it possible to arrest and prosecute the wrongdoer.

Physical effectors such as specially trained birds of prey, net guns, nets launched from other drones, missiles and guns work by physically bringing down or destroying the drone. The disadvantage with this option is that it could result in damage to the drone and its data which would inhibit the apprehension and prosecution of the wrongdoer.

What are the key legal issues arising in relation to the use of counter-drone technology?

The primary legal issue with drone detection technology is that of data handling. All data acquired by the detectors must be handled in accordance with the provisions of the Data Protection Act 1998. Therefore, licensed operators must ensure that they comply with these requirements as a failure to do so will result in fines from the Information Commissioner and/or privacy claims.

If the systems being used are not sophisticated enough to accurately target a rogue drone, the use of electronic and physical effectors could give rise to claims for damage to nearby drones which were not being used for nefarious means. There is also the question of potential personal injury to third parties and damage to property in the vicinity.

While damage or injury caused within a restricted air space could be argued to be necessary and proportionate following the completion of a satisfactory threat assessment, damage and injury claims could be brought by victims in the areas immediately surrounding the restricted air spaces, for example, close to airports. This could open up operators of counter-drone technology to civil claims for personal injury and damage to property. If businesses in the area are affected, operators could face claims for business interruption and consequential loss flowing from any damage caused by the use of counter-drone technology. The closure of Gatwick raises a number of potential insurance coverage issues and highlights how a small and relatively inexpensive consumer drone can have a far-reaching financial impact on global businesses. Accordingly, it is advisable for businesses to check their insurance policies and in particular the wording of exclusion clauses to check whether this type of loss would be covered should such an incident be repeated.

Are there any forthcoming legal developments which will assist in preventing the serious misuse of drones?

The UK Parliament is currently considering the draft Drones Bill. If the bill is adopted, the following changes could be included in new legislation:

• the mandatory use of an app which would publish flight plans, making pilots more traceable

• enhanced two-way communication between the pilot and the authorities if required

• the filing of pre-flight notifications if flights are planned at certain heights

• enhanced access to relevant information for police to assist with the apprehension of wrongdoers

• police powers to order pilots to land a drone, obtain warrants to search premises where there is a suspicion of a drone offence, to stop and search those suspected of drone crime and finally to seize and retain a drone and to access the digital data on it

• fixed penalty notices for those misusing drones in public, with suggested fines of £100 to £300 for those who cause harm, harassment, alarm or distress or disturbing public order

The above legislation will undoubtedly help in preventing drone attacks and potential business disruption. However, given that the bill has not yet been adopted, this is likely to take a number of months if not years before the relevant legislation is passed. In the meantime, those wishing to cause harm and disruption could develop digital methods of defeating the detection and effective technology.

Therefore, it is imperative that the government acts quickly to put the regulatory and legal framework in place to deal with the potential threats posed by the wrongful use of drones.

Interviewed by Andrew Muir.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.