wiley

ARTICLE

Is The US Ready For A 'Gatwick Drone' Scenario?

Law360
January 8, 2019

Over the holidays, as Vodafone debuted a seasonal and groundbreaking first drone delivery using 4G networks, drones in the United Kingdom made news for a different and darker reason. Rogue drone operators appeared to force the closure of Gatwick Airport, the second-largest airport in the U.K., by flying unidentified drones near the runway.

In the time since, this story has continued to evolve, with some news operations reporting that there may not ever have been any drones other than police drones, and other organizations suggesting that drones may have been a cover for closing the airport because of a cyber hack. The U.K. military ultimately deployed what has been described as Israeli counter-drone technology, though it is not clear if it was used — and it has now been withdrawn. The Sussex police force has been quoted as saying it was continuing to investigate "relevant sightings" from 115 witnesses, 93 of whom are "credible."

The U.S. has not experienced a disruption of this magnitude caused by a drone, although there have been documented instances of drones flying in dangerously close proximity to airports. Given the hazards inherent in small unmanned aircraft systems, or UAS, operating in close proximity to commercial airliners, an incident like the one at Gatwick raises questions about how well-prepared the United States is to handle the threat of rogue drones operating near airports.

Existing regulations are in place to limit flights near airports and provide mechanisms to enable lawful operation in airport-adjacent

Authors

Sara M. Baxenberg
Partner
202.719.3755
sbaxenberg@wiley.law

Joshua S. Turner
Partner
202.719.4807
jturner@wiley.law

Practice Areas

Uncrewed Aircraft Systems (UAS)

(Class B, C, D and E) airspace. Under the Federal Aviation Administration's Part 107 rules, commercial UAS operators are prohibited from operating in Class B, Class C or Class D airspace, or within the lateral boundaries of the surface area of Class E airspace, unless they have prior authorization from Air Traffic Control, or ATC.

Although the FAA initially handled airspace authorization requests through an online application process with a several-week processing window, the agency is in the process of deploying the Low Altitude Authorization and Notification Capability, or LAANC, which allows for near-real-time approvals to operate in restricted airspace. According to the FAA, LAANC is now available at nearly 300 air traffic facilities spanning 500 airports.

Hobbyist UAS users are also required to obtain prior approval to operate in airport-adjacent airspace. Although Part 101 of the FAA's rules requires only that a hobbyist provide ATC with prior notice of the operation, this regulation was based on Section 336 of the 2012 FAA Modernization and Reform Act. The 2018 FAA Reauthorization Act, signed into law in October, repeals Section 336 and imposes slightly different restrictions on hobbyists. One such restriction is that hobbyists now must "obtain[] prior authorization from the [FAA] or designee before operating" in airport-adjacent airspace. The FAA has not yet announced a streamlined LAANC-like mechanism for obtaining such authorization.

In addition to enhancing the restrictions on hobbyist operations near airports, the FAA Reauthorization Act also recognizes that "the unauthorized operation of [UAS] near airports presents a serious hazard to aviation safety," and encourages the FAA to "place particular priority on continuing measures ... to educate the public about the dangers ... of operating [UAS] near airports without the appropriate approvals or authorizations."

But even assuming hobbyists and commercial operators alike can obtain near-real-time authorizations to operate in restricted airspace nationwide, this only provides a mechanism for law-abiding drone users to utilize the airspace — it doesn't stop the rogue operators. That's one reason why in the U.S., the ability to remotely identify the operators of UAS in flight, known as Remote ID, is viewed as an essential component of the regulatory scheme, and is a key priority for the FAA. The Reauthorization Act provided a much-needed fix to a gap in existing law that prevented the FAA from applying Remote ID to hobbyists. With the regulatory authority to apply Remote ID to all aircraft, the FAA will be able to proceed with a rulemaking and adopt Remote ID rules over the next couple of years.

Even with the ability to identify UAS owners and operators, the question remains as to how drone threats can be mitigated, and who can conduct that mitigation. Here too, the FAA Reauthorization Act advances the ball, including as related to airport safety specifically. First, the act expanded the list of federal agencies authorized to undertake counter-UAS measures to protect certain assets and missions of the agency. This list now includes the Departments of Defense, Energy, Homeland Security and Justice.

The act further requires the FAA to develop a plan for certifying, authorizing and deploying counter-UAS

systems, and requires the FAA to charter an aviation rulemaking committee to make recommendations related to this plan. With respect to airport safety, the act requires the FAA to test and evaluate counter-UAS technologies by deploying a counter-UAS pilot program at five airports, one of which must rank in the top 10 most frequented airports.

Notably, the act does not give any express counter-UAS authority to state or local governments (including airport authorities), and the proper balance of the role between state and federal authorities raises complex questions in the context of UAS enforcement. While the federal government rightly enjoys broad regulatory authority over the national airspace, air navigation and aircraft safety standards, the FAA has limited means to enforce its regulations. It is generally understood that state and local law enforcement have a role to play in ensuring the safety of the airspace, particularly with the proliferation of small UAS.

To this end, the FAA Reauthorization Act requires the FAA to establish a pilot program to utilize Remote ID technology "for safety oversight, including enforcement actions against operators of UAS that are not in compliance with applicable Federal aviation laws." This pilot program must include a mechanism for the public as well as federal, state and local law enforcement to report a suspected unlawful operation. The act also requires the FAA to develop a "comprehensive strategy to provide outreach to State and local governments and provide guidance for local law enforcement agencies and first responders" on identifying and responding to public safety threats posed by UAS.

Importantly, the means available to state and local law enforcement to mitigate UAS threats do not, and cannot, include signal jamming. As we have previously explained, this type of interference with radio spectrum intrudes on the exclusive authority of the Federal Communications Commission and implicates a host of laws, including federal criminal statutes — prohibitions which extend to state and local law enforcement.

Penalties also have a role in protecting airport-adjacent airspace. FAA regulations already prohibit the reckless operation of UAS and require UAS to give way to manned aircraft, and the U.S. criminal code already prohibits damaging, destroying, disabling or wrecking aircraft. That same provision also bars "interference" with a person operating an aircraft, either in a way designed to cause harm or in a way that is reckless. And while that latter provision seems like it could be used in a Gatwick-style incident, the FAA Reauthorization Act adds a new provision that removes any doubt: it is now a federal crime to use a UAS to knowingly or recklessly interfere with or disrupt the operation of an aircraft carrying passengers "in a manner that poses an imminent safety hazard" to the passengers, or to (as the Gatwick operators appear to be doing) knowingly operate a UAS in a runway exclusion zone without proper authorization.

Penalties for the new criminal provisions include fine or imprisonment, with maximum prison terms of one year (committing the prohibited operations without causing any bodily injury), 10 years (causing serious bodily injury or death by recklessly operating near other aircraft) or life (causing, or attempting or conspiring to cause, serious bodily injury or death by knowingly operating near aircraft or in a runway exclusion zone).

In sum, while under current law it is possible for the U.S. to experience a Gatwick-style drone disruption, efforts are underway at all levels of government to reduce the risk and mitigate the threat of such an event, and these efforts are being facilitated considerably by multiple provisions in the FAA Reauthorization Act. Notably, the federal government has recognized the need for a multifaceted approach that includes deterring airport interference by UAS operators, providing mechanisms for lawful use of aircraft-adjacent airspace, identifying rogue drone operators, taking countermeasures against the drones and punishing bad actors.

One final take-away from the Gatwick incident has become clear over the past few days: Just finding out what is actually happening can sometimes be an epic challenge. Eyewitnesses — even credible ones — may not be able to reliably identify drone operations, or to distinguish what are permitted drone operations from those that are not. This can lead to confusion, which in turn can result in even more disruption. Remote ID systems will assist with this, but communication and coordination between law enforcement will be critical in making sure that responders on the ground have situational awareness in which they can be confident.

While the FAA Reauthorization Act recognizes the importance of coordination between law enforcement, the Gatwick incident raises new and potentially unanticipated challenges. This highlights the value of regulatory flexibility, and the value that pilot programs like those in the FAA Reauthorization Act can have for emerging technologies and the policy issues they raise.