Willis Towers Watson

Drone disruption at airports

A risk mitigation and insurance response

ARC

Airport Risk Community

Connecting | Sharing | Delivering

Drone attacks: An overview

Industry concerns are rising with regard to potential disruption caused by drones due to the serious consequences for airports, passengers, airlines and the wider aviation ecosystem.

Increased use and improved technology

Airports are facing an increasing threat from unauthorised and sometimes malicious use of drones in and around their premises. Personal drones are not only readily available but also becoming more powerful. Perpetrators are now able to orchestrate disruption some distance from the potential target with minimal risk or threat of discovery.

Militarily drones are also increasing in sophistication and can be used for a number of functions such as passive information collection or in a kinetic attack at an airport.

The use of drones in the delivery of small scale munitions can appeal to terrorists, insurgents and other militant non-state actors. Likewise unmanned aircraft appeal to states since they are largely inexpensive and provide a means to attack a target with a low risk to personnel and the perpetrator(s).

Whether the origin of the disruption is anarchical, terrorist motivated or even militarily strategic, airports must prepare themselves for increased levels of drone-based disruption in the future.

2018 Gatwick drone incident

In late December 2018, operations at London Gatwick airport were interrupted by a series of drone sightings over a 48-hour period, temporarily closing the airport. In all, Gatwick's COO estimated that about 120,000 passengers suffered flight disruption. The perpetrators of the attack remain unknown but in April 2019 Gatwick confirmed they had reason to believe that inside knowledge may have contributed to the attack. The type of drone used could have been specifically selected to avoid detection based on Gatwick's existing technologies. Gatwick also had reason to believe that whoever was piloting the drone may have either had sightlines to the runway and/or an ability to eavesdrop on internal radio communications within the airport.

Escalating frequency

According to the UK Airprox Board[1] over the past eight years approximately 330 'near miss collisions' have been identified between drones and aircraft. Of the 330, almost 130 occurred in 2018 alone[2]. These statistics show an alarming escalation in the number of drone-related occurrences, elevating calls from the public and private sectors for regulators to enforce stricter controls on the use of drones around commercial aviation hubs.

Regulatory response

In March 2019 the UK Civil Aviation Authority responded by issuing Air Navigation Amendment Order 2019 (CAP1763), which widened drone-exclusion zones around airports to five kilometres long and one kilometre wide from the runway[3]. Questions remain whether this will be sufficient to discourage individuals intent on disruption.

Thus far, the aviation industry has avoided incidents resulting in injury or loss of life. However, it is important to recognise the dramatic increase in drone-related incidents in recent years, demonstrated by an approximate 730% increase in airport incidents[4]. This has lead to some important questions being raised around the risks to airports caused by drone use.

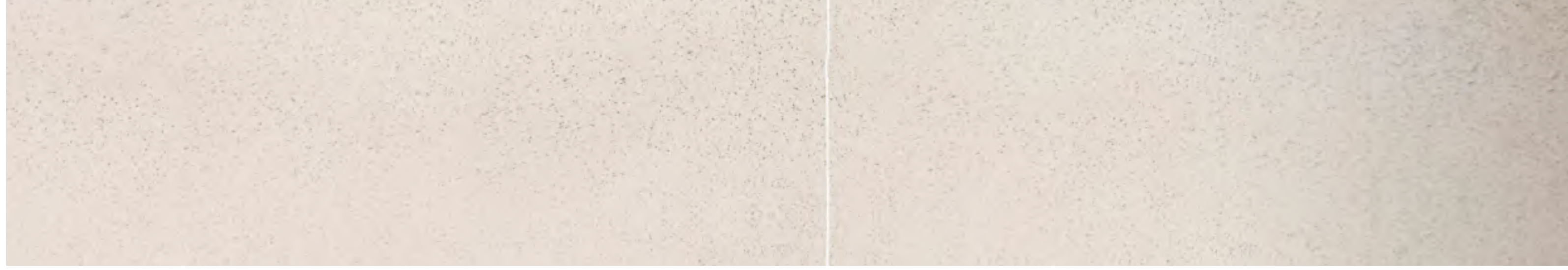
> *According to the most recent Drone Airprox Count and Information, the number of incidents has gone from approximately 35 between 2013-2015 to nearly 290 from 2016-2018 in the UK alone[4].*

[1] UK Airprox Board (UKAB) Responsibilities https://www.airproxboard.org.uk/Learn-more/About-us/

[2] Wilde, C., & Bellamy, A. (2019, January 26). More than 300 near misses between drones and aircraft across the UK recorded. Retrieved from https://www.yorkshirepost.co.uk/news/crime/more-than-300-near-misses-between-drones-and-aircraft-across-the-uk-recorded-1-9558792

[3] Civil Aviation Authority. (2019, February 28). Retrieved from http://publicapps.caa.co.uk/docs/33/CAP1763%20New%20UAS%20guidance%20Feb%202019.pdf

[4] Forward, S. (2019, April 9). Current Drone Airprox Count and Information. Retrieved from https://www.airproxboard.org.uk/Topical-issues-and-themes/Drones/

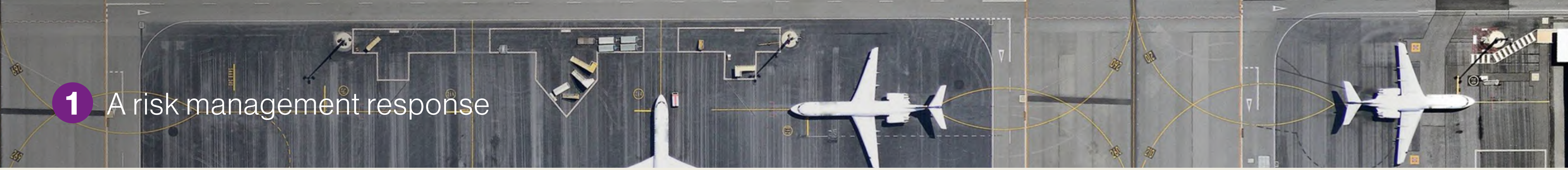


Questions being raised by the industry

In the context of increasing drone activity, it's appropriate that airports are actively considering the extensive risk implications.

Discussions within the Willis Towers Watson Airport Risk Community (ARC) have highlighted some key areas of concern, which we will outline in the following report:

1. What risk management measures can be taken to minimise disruption and damage caused by a drone incident?
2. How might a drone incident affect the reputation of the airport among its stakeholders?
3. Insurance market response:
   - Damage to physical assets caused by a drone
   - Interruption to business and loss of revenue as a result of drone disruption
   - Actions taken against airport operators by third parties?



1 A risk management response

There are four main steps that airport operators should consider when dealing with a drone disruption:

Assess and locate

Reports of drone activity can come from a number of sources such as aircraft crews, members of the public outside the airfield boundary and airfield employees or passengers inside the airport. These reports could be well-intentioned, or made maliciously to disrupt flight operations for a criminal purpose.

A clear decision-making process should be in place to allow the airport operator to make the most appropriate decision based on what is known (or not known). Clearly, safety is the priority. Any decisions should be appropriate, proportionate and necessary, with documentation of when it was made, by whom, and the rationale for making it.

Operators should also consider whether to invest in enhanced technology to locate drones; this technology should allow airfield managers to identify and track suspicious drone activity and inform the decision-making process.

It is imperative to understand which part of a facility's airspace has been infringed upon and where the drone is at all times during the incursion.

Identify

The identification phase is vital to any mitigation efforts, especially if the airfield operator is considering investing in bespoke technology.

It is important that the type of device causing the disruption is identified. This should include when and where it was first seen in as much detail as possible (size, colour, number of rotors, direction of travel, etc.). Identifying the drone will provide information on likely endurance time, and which disruption tool (if any) is best suited for response.

The airfield operator may be able to utilise existing CCTV systems, especially if they are located high up (e.g., in the air traffic control tower). This information will inform subsequent criminal investigations.

Long-distance photographic surveillance equipment is already widely used within many military organisations. Obtaining equivalent technology on the ground could be crucial to allow early identification and minimise disruption. With airports forming part of key national infrastructure perhaps government has a role to play in funding such technology?

It is important to understand the type of drone being used, what threat it poses to the operator (or other businesses) and what mitigation options are available.

Mitigate

There are a number of technological solutions on the commercial market. Airfield operators must remain within the law when using disruptive technologies, and the risks on the wider community should be fully assessed and understood.

Efforts to identify methods that will protect airspace using virtual technologies are ongoing. These options include geofencing along with other safe ways to disable a drone so that it can be identified and its operator sanctioned.

It is recommended that airfield operators establish communication channels with security agencies – such as the police, military and the Civil Aviation Authority – before an incident occurs. If a drone falls within the airfield boundary, the operator should consider consulting with the police before approaching it, as it may contain vital forensic and digital evidence that could be used in an investigation.

One way to understand the full risks and community impact of any incursion would be to practice a potential scenario as part of a multi-agency drill before investing in any disruptive technology.

It is also recommended that airfield operators seek regular updates from police on the threat to the local aviation sector from drones; this should be regular practice as part of the airport multi-agency group meetings.

Adopted mitigation options must be legal, proportionate and properly risk assessed.

Assure

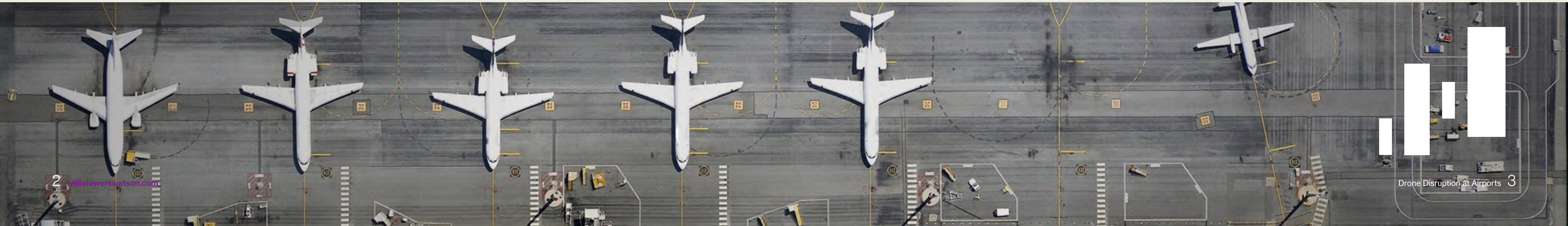
The final stage is to ensure that the drone has left the operator's airspace; this will satisfy the operator's security concerns, as well as those of the user airlines, passengers and, in some cases, the Civil Aviation Authority, while operations return to normal.

To resume flight operations, the operator will need to confirm that: the airspace is clear; the drone no longer poses a threat to the airfield; and it is safe for operations to restart.

Drone disruption action plan:

When planning a drone disruption response airport operators may consider the following:

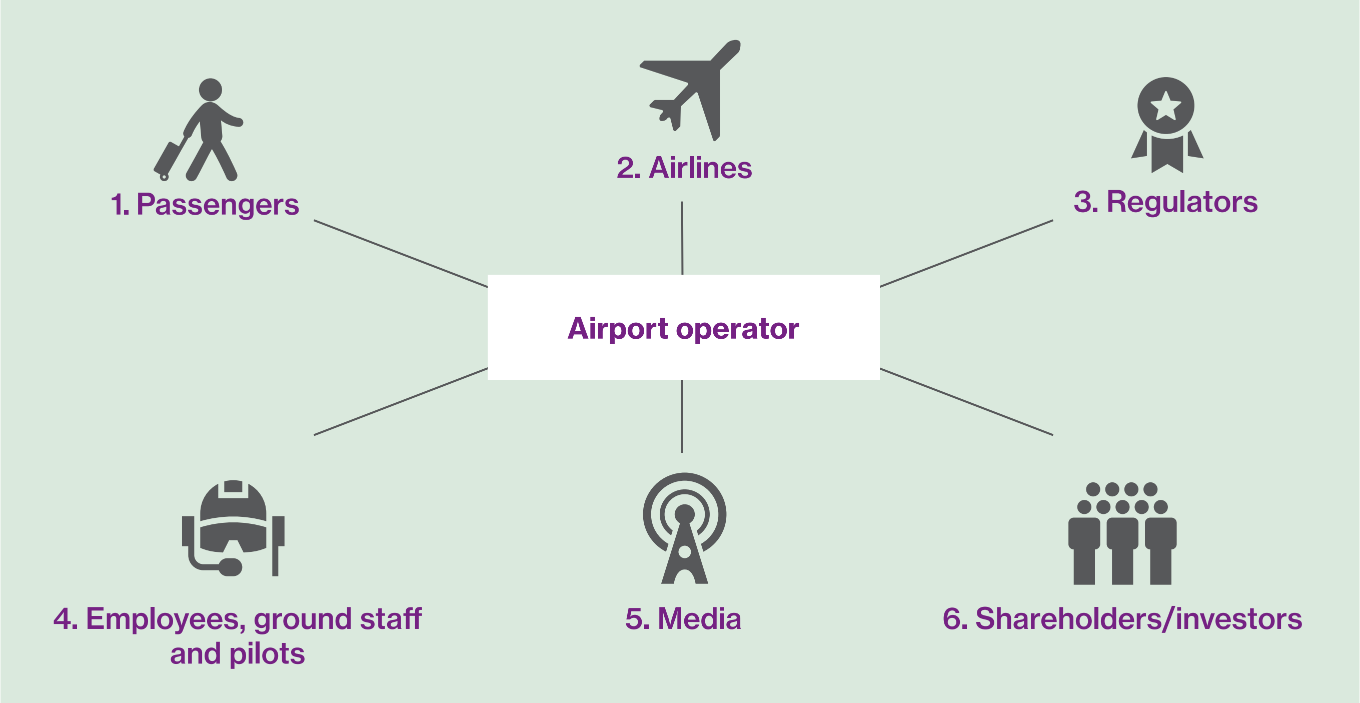
- A single internal reporting point for drone sightings
- Pre-planned decision making channels
- Early liaison with multi-agency partners
- Assessing the potential insider threat
- Ensure your business continuity plan considers this type of disruption
- In the absence of technology, consider deploying staff to act as spotters
- Assess the media response (keeping passengers and stakeholders informed)
- Early engagement with airline operators during initial stages of a drone sighting
- Exercise this scenario regularly in a multi-agency drill



2 Potential reputational damage

Reputational damage is an obvious outcome from the associated disruption. London Gatwick airport reported that 120,000 passengers were disrupted when planes were grounded for more than 30 hours.

Long-term reputational harm to airports is difficult to quantify but should not prevent operators from considering the potential impact on a range of stakeholders:


1. Passengers
2. Airlines
3. Regulators
Airport operator
4. Employees, ground staff and pilots
5. Media
6. Shareholders/investors

1. Passengers

A loss of confidence in the airport operator's ability to deal effectively with the threat of a drone can seriously damage passengers' use of the airport. If transportation alternatives or competing airports are viable transit options, the long term damage can be significant.

2. Airlines

Airlines, whilst reliant upon airports, are ultimately customers. A decision from a key carrier to move to an alternative airport may be more attractive if disruption becomes more frequent and losses escalate.

3. Regulators

The closure of any airport – particularly at major hub locations – is not well received by regulators and politicians, unless there is clear justification, for example, if the safety of passengers is at risk. While the Gatwick incident fulfilled this criterion, any repetition will attract regulator and political scrutiny, which in turn can damage reputations.

4. Employees, ground staff and pilots

As well as passengers, airports owe a duty of care to the vast network of personnel that help them function. Repeated drone incursions would endanger ground staff and put huge pressure on the operation team trying to resolve the issue. Pilots are ultimately responsible for the in-flight safety of their passengers and may even refuse to operate from an airport.

5. Media

Airport management needs to react quickly and effectively to what is likely to be a media storm. This requires a strong, clear, honest and where possible transparent appraisal of the situation and steps to resolution. Concise, direct messaging to the media will give reduced bandwidth for speculation and unfair criticism of the airport.

6. Shareholders/investors

Airports are an attractive investment vehicle. Recent years have seen several expansions of airport groups, merger and acquisition activity and development of existing infrastructure. An airport's perceived inability to manage drone threats could jeopardise future investment opportunities.

3 Insurance market response

There are three primary areas in which a drone attack could cause financial loss to an airport:

- Damage to physical assets caused by a drone
- Interruption to business and loss of revenue as a result of drone disruption
- Actions taken against airport operators by third parties

Property damage insurance

Property damage insurance is black and white when it comes to drone activity. If a drone hits a building and causes damage, a property damage policy would typically respond to indemnify the value of the damage, whether for replacement, repair or rebuild, depending on the circumstances.

Currently, most drones are small, lightweight and not likely to cause extensive damage. However, as drones increase in size and scope, the risk of significant property damage rises.

Nonetheless, it is important to note that there is a key exclusion in a standard property damage policy. If the drone has explosives or some sort of device attached, it becomes a terrorism issue. A standard policy would exclude such an event, but can be insured via a variety of available terrorism products.

Terrorism insurance

A property damage policy typically excludes damage caused by a terrorist/malicious attack, whereas a traditional terrorism policy will fill this gap. It will cover the cost to rebuild, repair or replace as long as the cause of loss was a terrorist/malicious attack.

Some terrorism policies – such as an active assailant policy – will provide support for the costs associated with a crisis-management response and certain expenses such as the cost of medical care or consultation with public relations experts. Also available in the market are nuclear, chemical, biological and radiological policies, which provide coverage for reparation and demolition/decontamination clean up of property (subject to certain exclusions, such as war). A drone incident of this type has yet to occur but, in principle, the coverage is available.

It should be noted that terrorism policies distinguish 'malicious' attacks from 'terrorist' attacks and it is important to check that any terrorism policy addresses both perils.

3 Insurance market response

Business Interruption

Interruption to business and loss of revenue is a much more complex issue. For business interruption coverage to take effect, it must be as a result of property damage. This would apply to both Property Damage & Business Interruption (PDBI) and Terrorism policies.

Moreover, the business interruption usually must be as a direct consequence of the damage caused; for example, if a drone crashed into a fence – and operations could have continued – and the airport is shut down because the authorities are fearful of a second event, insurers might restrict or deny indemnity. This might then be "bought back" if the wording has a denial of access/ingress and egress/ civil or military authority extension. These provisions are often sub-limited, though, and always require physical damage.

If, as was the case at Gatwick, disruption occurs but there is no property damage, the business interruption would fall outside the scope of standard cover. For the business interruption coverage to be triggered, the airport must sustain property damage.

If the sole intention of the Gatwick perpetrators was to create maximum disruption, there is little appetite from insurers to cover what is perceived to be a societal problem: currently very few restrictions to individuals obtaining a drone exist and there are limited controls to prevent them entering airspace.

Insurers also would point to a lack of fortuity, upon which much of the traditional insurance market is based. There are a small number of insurers who will entertain providing some type of cover for this kind of event, but it is far from a developed market at this point.

What some insurers will provide is 'efficacy' cover, a type of 'sleep easy' arrangement. Such a policy relies on the airport having preventative measures in place. For example using anti-drone defensive technologies to prevent illegal flights near the airport; this arrangement would be paid for by the airport and the companies that provide the defences.

Another recent development in the terrorist market is a "Threat of a Malicious Act" policy. Through this arrangement, coverage can be provided for business interruptions such as a lockdown, evacuation or 'invacuation' of an airport after a civil or military order (or agreement/subsequent "certification", if initiated by the insured) resulting from the threat of a malicious act. This coverage may also include any costs incurred in taking reasonable precautions due to the sighting of a drone, which later turns out to be a hoax, accidental flight, misreport, or an activity of innocent intent.

Again, it applies only if the civil or military authority agrees that the precaution taken was reasonable and proportionate.

As well as traditional insurance policies, the last few years has seen the rise of "parametric solutions". In such contracts, payments by insurers are not triggered by a single identifiable occurrence. Instead, the policy responds if a metric is triggered relative to a pre-agreed index. In many cases, the index is weather based (e.g. if an airport is affected by an unusually high number of snow days), but solutions are also available for a decline in footfall.

Parametric solutions are customised to each insured and, in principle, could be adapted for drone-related perils.

There is no easy solution as a current lack of related data is inhibiting product development for insurers. What are the good risks and what are the bad ones? Without this information, it is easy to understand the lack of appetite amongst insurance carriers.

Third parties' actions against airport operators

Most airports will have an Aviation Liability insurance policy designed specifically for owners and operators. Aviation liability policies tend to be extremely broad in the scope of their coverage and will respond to a range of incidents – landside or airside, incidental or malicious in intent - and can be made available to the benefit of contractors operating in or near the airport.

Although there are various terms and conditions, the three key requirements to trigger coverage under the policy are as follows:

1. The need for "an occurrence", as defined in the policy
2. The occurrence must result in bodily injury or property damage to a third party
3. The airport must be fully or partially liable for the damage sustained by the third party

In many cases, disruption caused by a drone would fit the criteria for a valid claim under the aviation liability policy. For example, if a drone damaged a third party's parked car and the airport was found to be responsible, or if a drone seriously injured a third party whilst at the airport.

There are even instances whereby a witness to such an event could make a claim against the airport based on a definition of bodily injury that included, for example, mental trauma. So there are plenty of occasions and scenarios in which an aviation liability policy would provide cover.

However, just like the standard response of the PDBI policy, an incident with characteristics similar to the Gatwick airport attack may become more difficult due to the lack of an identifiable occurrence that resulted in bodily injury and/or property damage – if a drone was simply sighted, disrupting operations, disappeared, re-appeared etc. Was there identifiable bodily injury or property damage? Was there even proof it was a drone?

Notwithstanding an airport's "terms of use" agreements, there is nothing to prevent severely delayed passengers from taking an action against an airport or the airline, or indeed to prevent an airline from seeking compensation from the airport for the disruption.

Despite commercial pressures to settle such claims, airports may find that they are beyond the scope of coverage that insurers are prepared to afford under an airport liability policy.

The traditional limitations of coverage in an airport liability policy could lead to the unusual situation in which a drone entering the airspace of an airport – or the flight path of an aircraft – causes disruption that would be outside the scope of cover, unless it resulted in a collision that caused damage to the aircraft (no matter how superficial), in which case it may be sufficient to activate coverage.

It almost seems arbitrary, but it provides an opportunity to aviation insurers to address this potential vulnerability in their client's programmes.

In summary

Drone-related incidents at airports may be a recent phenomenon, but they are expected to increase in frequency, complexity and severity as drones become larger and more powerful.

Airports need to prepare for potential attacks through effective risk management and there are a number of steps that airports can take to prepare for these scenarios.

Appropriate responses taken by operators during and immediately after any incident - as outlined in the drone disruption action plan - can minimise the impact on key stakeholders. Airports should also be calling on better support and co-ordination from government, security services, the military and industry partners.

Damage to reputation can be difficult to manage and mitigate. Organisations are now offering analytical tools which can help quantify the risk to reputation – recognising the direct link between reputation and your balance sheet.

Unfortunately, even with a range of measures in place, there remains significant scope for the airport to suffer financial loss by way of property damage, business interruption and legal liability. The insurance market's response in many circumstances will protect airports from financial losses. There are, however, some key policy triggers that may not be met in some circumstances, so it is essential that airports are aware of these limitations.

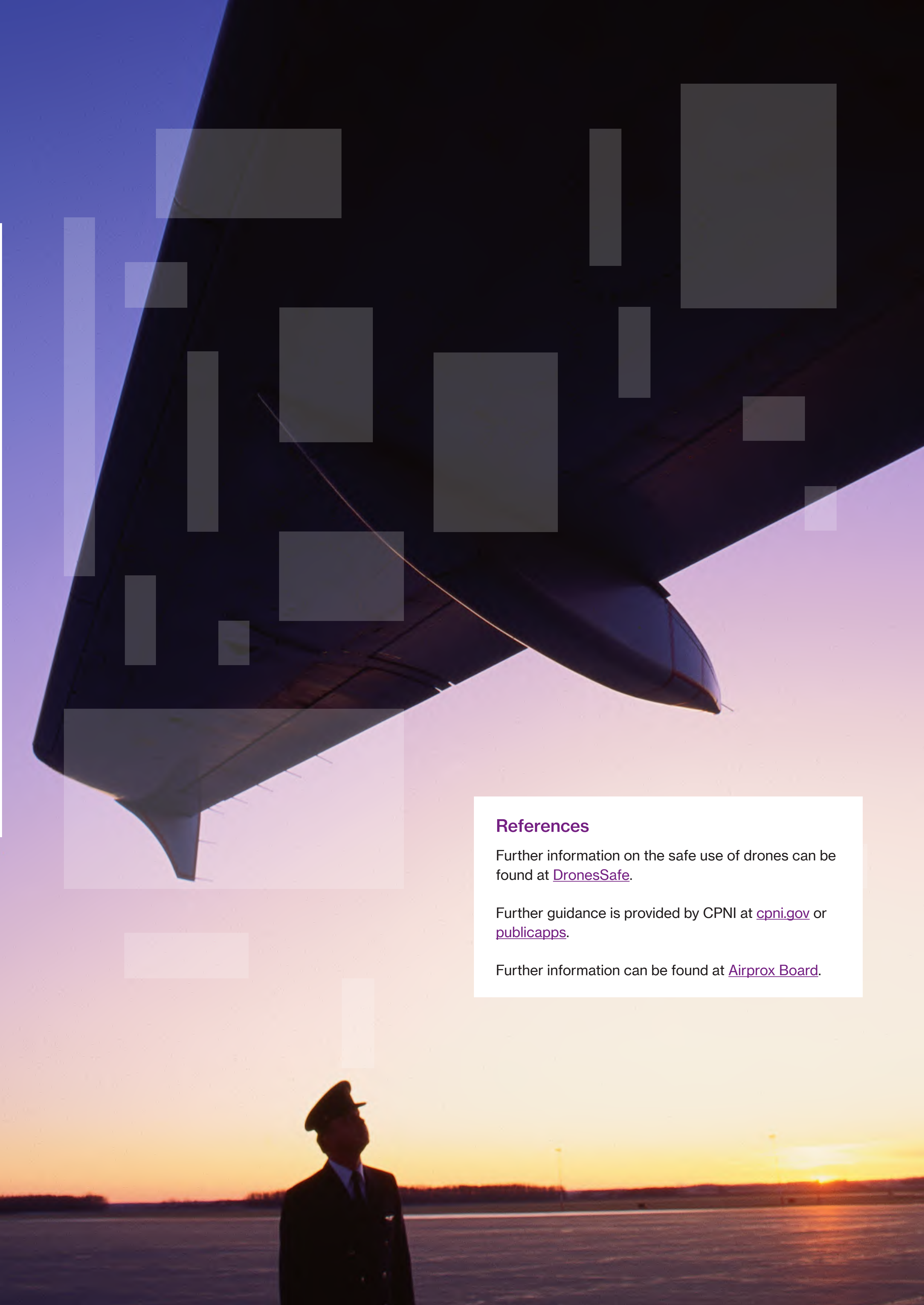
New products such as parametric solutions are on the horizon and the insurance market is actively looking at ways to enhance the range of products available to address drone incidents at airports. Innovation takes time and is best achieved through partnership and collaboration with the aviation community.

We welcome the opportunity to discuss any of the topics raised in this article.

Contacts

Robin Milan
Executive Director, Global Aerospace
D: +44 (0)1473 207127
Robin.Milan@WillisTowersWatson.com

Karen Larbey
Director of Strategy & Planning, Transportation Industry
D: +44 (0)20 3124 7606
Karen.Larbey@WillisTowersWatson.com



References

Further information on the safe use of drones can be found at DronesSafe.

Further guidance is provided by CPNI at cpni.gov or publicapps.

Further information can be found at Airprox Board.

This publication offers a general overview of its subject matter. It does not necessarily address every aspect of its subject or every product available in the market. It is not intended to be, and should not be, used to replace specific advice relating to individual situations and we do not offer, and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this publication may be compiled from third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such. The information given in this publication is believed to be accurate at the date of publication shown at the top of this document. This information may have subsequently changed or have been superseded, and should not be relied upon to be accurate or suitable after this date. The views expressed are not necessarily those of Willis Towers Watson. Copyright Willis Limited 2019. All rights reserved.

Willis Towers Watson is a trading name of Willis Limited, Registered number: 181116 England and Wales. Registered address: 51 Lime Street, London, EC3M 7DQ. A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority for its general insurance mediation activities only.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

FPS538/WTW247025/06/2019

willistowerswatson.com

Willis Towers Watson