Planes, drones and the Internet of Things

As the global village meets the shrinking world, technology is increasing the range of potential risks for aviation underwriters, says **Suki Basi**

The term "global village" – coined in the previous century by cultural historian Marshall McLuhan – describes the world as being closely connected by modern telecommunications and economically, socially and politically interdependent.

Since the term was invented it has become easier and quicker to cross from one side of the village to the other, while 21st century communications have evolved to the point where they are instant. This has brought advantages and disadvantages.

The world of aerospace, which has played a central part in bringing the global village closer together, is imperilled by a new wave of hazards caused by technologies that have ostensibly been created to make life easier for us all.

In this article we discuss how two of those potential hazards – drones and the Internet of Things (IoT) – have the potential to pose problems for aviation underwriters.

Drones in airspace

Within a week of Russell Group releasing its "Ground Accumulation Hazards" white paper in January 2016 it was reported that drones almost collided with planes near major UK airports in four separate recent incidents. They included one near-miss in September 2015 with a passenger jet taking off from London Stansted.

The pilot of the Boeing 737 passenger jet said a six foot (two metre)-long remote-controlled plane passed less than 15 feet above its path, at 4,000 feet, in controlled airspace where any drone flight is illegal. Nine days later, the pilot of a Boeing 777 airliner taking off from Heathrow saw a small drone passing "less than a wingspan" away from the plane.

The UK Airprox Board investigated seven incidents in December 2015 involving drones, four of which were classified as being in the most serious bracket, according to *The Guardian* newspaper.

Steve Landells, a flight safety specialist at the British Airline Pilots Association (Balpa), said at the time: "The reports that UK Airprox gets are the ones that are seen. But when you're flying at more than 100mph, the chances of seeing a typical, 18-inch wide drone are small.

"We don't know if this is the tip of the iceberg. With the massive increase in drone sales, we fear we might see a dramatic rise in close calls."

The Guardian story from 29 January mirrors an equally worrying report in the same newspaper from a few weeks previously. It explained how commercially available drones have the potential to be converted into flying bombs capable of hitting targets such as nuclear power stations, the prime minister's car, or, of course, airports and airlines.

"Drones are a game changer in the wrong hands," warned the lead author of a report by the Oxford Research Group's Remote Control project.

Continued on page 60

Planes, drones and the IoT continued from page 59

The January 2016 report, "The Hostile Use of Drones by Non-State Actors Against British Targets", highlights concerns that "drones will be used as simple, affordable and effective airborne improvised explosive devices".

Taking the threat to another level, it appears that "Islamic State [Isis] is reportedly obsessed with launching a synchronised multi-drone attack on large numbers of people in order to recreate the horrors of 9/11".

Chiming with warnings in previous Russell Group white papers on the aviation and airport war and terror threat, there are now reports of the Lebanese militant group Hezbollah violating Israeli airspace with drones that are part of a fleet of an estimated 200 unmanned aerial vehicles.

Whales and airports

Meanwhile, further advances in technology – particularly the internet – have drawn increasing attention to social networks and human interconnectedness, and the ability of individuals, organisations, terrorists and even states to create disruption.

More and more things are connected whether or not we like it – or know it. That's why it was interesting to read a recent report which outlined how the hunting of whales far out at sea could directly lead to the shutdown and disruption of a major inland airport.

Hacktivist group Anonymous claimed responsibility for a cyberattack on the website of Tokyo's Narita Airport, which went offline between 22 and 23 January after a distributed denial of service attack caused it to collapse under the strain of too much traffic. But why would Anonymous do that, you ask?

According to *The Independent* newspaper, Twitter accounts associated with Anonymous claimed the cyberattack was in retaliation for the detention of Ric O'Barry, an American dolphin trainer turned animal rights activist, who has been a vocal critic of Japanese whale and dolphin hunting.

In our January white paper "Post Tripoli", Russell Group focused on airport ground accumulation hazards and risks, which we believe are rising significantly due to a range of emerging social, environmental, economic and political factors. The Anonymous cyberattack in retaliation for a whale hunt covers all four of these factors.

Underwriters could be forgiven for thinking: "Well I could hardly have factored whale hunting into my airport safety risk management system!" However, the episode highlights a central point of globally connected risks and hazards today, which is that airport risk management, for example, is not simply about the measurement of "micro" or "on the ground" risks such as hanger collapse, wing tip collisions or other aircraft accidents.

A modern, holistic underwriting approach needs to factor in political risks (such as the Tripoli airport attacks), as well as environmental (floods, and maybe whales!), social (the IoT, cyber) and economic (inequality or corruption, for example) perils. Two recent episodes highlight the social factor – the IoT and cyber hazards.

The shrinking world

The first episode – news that hackers allegedly stole $55mn from a Boeing supplier – has potential ramifications for aviation underwriters that are concerned for their cyber and supply chain exposures.

Aerospace parts manufacturer FACC reported on 19 January this year that its financial accounting department had been attacked by hackers. The financial markets responded badly to the news and FACC's stock price closed 17 percent lower by the end of the day's trading.

The news is a reminder that in today's connected cyber environment it is incumbent on companies to keep a closer eye on their suppliers' digital vulnerabilities, as well as their own.

Increasingly, however, the airlines themselves are coming under attack as our second example, Ryanair, discovered to its cost in 2015.

The airline reportedly fell victim to hackers who managed to steal EUR4.6mn (almost $5mn) via a fraudulent electronic transfer to a Chinese bank. However, it seems that the money was subsequently recovered.

While there was a relatively successful conclusion to this particular cyber episode, it is still hard to put an estimate on the cost of the man hours lost and the fees paid to recover the sum, not to mention the reputational damage incurred.

The Hungarian author Frigyes Karinthy believed that the modern world was "shrinking" due to the ever-increasing connectedness of human beings. He posited that despite the great physical distances between the globe's individuals, the growing density of human networks made the actual social distance far smaller.

Underwriters could draw similar conclusions to the connected nature of risk in 2016. So as our "virtual" world merges with the "real" world today, it is becoming increasingly important that the insurance community absorbs these abstract concepts and turns them into measurable analysis that can mitigate the risks between things.

Suki Basi is managing director of Russell Group