TURBULENT TIMES: UNDERSTANDING THE ENDURING AND EVOLVING THREAT TO CIVIL AVIATION

Andy Blackwell, ISARR's Senior Risk and Security Advisor, reviews the disruptive events affecting civil aviation security over the past six months, identifies key trends, risks and vulnerabilities, and provides guidance on simple steps that organisations can take to enhance their security resilience.

BACKGROUND

The aviation sector is no stranger to crises, from lethal terrorist attacks against airports and aircraft in flight, to major safety issues, accidents and natural events such as volcanic ash clouds. The pandemic is the latest crisis to impact the sector and by far the most disruptive and challenging it has ever faced. COVID-19 is not only a deadly virus but a potent distraction risk. As this paper will reveal, conventional security threats remain and just as new viruses emerge and mutate, so do threats against the sector, with malicious actors demonstrating innovation and seeking to exploit weaknesses in aviation defences that could provide them with viable attack opportunities. This dangerous mix of risks requires careful management and constant review to maintain the integrity of aviation security.

THREAT LANDSCAPE

Despite the global pandemic, terrorists including the so-called Islamic State, al Qaeda and al Shabaab have called for renewed attacks, telling their followers that global jihad is to continue even as the virus spreads. These groups have previously included aviation in their target sets, and al Shabaab operatives have been linked to recent attacks and plots against the sector. The UN's Counter Terrorism Committee Virtual Open Briefing – *Threats to Civil Aviation* (Dec 2020) reported that there has been little change in the threat posed to civil aviation by malicious actors, at a time when COVID-19 has created new vulnerabilities including a displacement of focus from security to health protection. It is clear that terrorists retain their unhealthy interest in the sector and will repurpose themselves to exploit the crisis and our recovery from it.

In November 2020, Ed Butler, Chief Resilience Officer at Pool Re, said he fears a new terror spectacular in the next 12 months as the coronavirus crisis sees pressures build up, and that the key concern is the aviation sector which provides an iconic target for terrorists. Other malicious actors featuring on aviation security's radar during the reporting period

include cyber criminals, fraudsters, and the 'enemy within', hostile insiders.

TARGETING OF AIRCRAFT AND AIRPORTS

Al Shabaab, one of AQ's most dangerous affiliate, features significantly in threat reporting for the period in question. One of their operatives, Cholo Adbdi Abdullah, was recently charged with plotting a 9-11 style attack (aircraft used as a weapon). Abdullah is alleged to have been making preparations in the Philippines to hijack an aircraft and crash it into a building in the US. He is said to have received flight training and completed tests necessary to obtain his pilot's licence. Al Shabaab also claimed responsibility for an attack on a Turkish cargo aircraft landing in Diinsoor in Somalia, after 14 anti-aircraft projectiles were reported to have hit the Ethiopian occupied airstrip. There was no damage to the aircraft and it was able to make an emergency diversion to Aden Adde International Airport in Mogadishu. A second attack within a 48-hour period involved Al Shabaab fighters firing several rockets from a long-range anti-aircraft gun at an aircraft attempting to land at the same airstrip. The aircraft was not damaged and there were no casualties. Al Shabaab also attempted to take control of Dhusamareb Airport in Somalia by staging an unsuccessful attack using a mortar barrage. They were thwarted by AMISOM forces.

At the time of writing, the US Federal Aviation Authority, issued a warning about airspace security in Eastern Kenya, advising that al-Shabaab *'likely seeks to target Western civil aviation and possesses or has access to, a variety of weapons, including small arms; indirect fire weapons, such as mortars and rockets; and anti-aircraft-capable weapons, including man-portable air defence systems (MANPADS). Such weapons present a risk to civil aircraft operating at low altitudes*'.

The magnitude and frequency of these incidents highlights the unhealthy interest al Shabaab retains in attacking aviation assets and the danger they pose to the sector. Official sources report that Al Shabaab maintains

the capability to develop concealed IEDs and the intent to use them against civil aviation.

The most deadly attack against civil aviation in this reporting period involved explosions at Aden Airport in Yemen, as members of the new government were disembarking from a commercial aircraft belonging to the national carrier Yemenia. 28 people were killed in the attack and 107 injured. Maeen Abdulmalik, Yemen's prime minister has accused the country's Shiite rebels and Iran for the fatal explosions.

The frequency of attacks highlight the attractiveness of aviation assets to terrorists and other extremists. The bulk of the incidents reported have occurred in conflict areas. The incidents are summarised as follows:

Yemeni Ansar Allah militants (Houthis) targeted Abha International Airport in Saudi Arabia using an unmanned aerial vehicle (UAV). The attack resulted in the puncturing and ignition of the left-hand aft fuselage of an Airbus A320 aircraft. The US State Department condemned the attack, which coincided with US Special Envoy Lenderking's first trip to the region and his efforts to bring a lasting peace to Yemen. A further weaponised drone attack a few days later was thwarted by Saudi air defences, although Houthis claimed that attack hit its target with 'high accuracy'.

Three rockets were fired at Baghdad International Airport, two landed outside the airport whilst the third hit a house in the Al-jihad neighbourhood, west of Baghdad. No casualties were reported and there was no claim of responsibility. The Tigray People's Liberation Front (TPLF) carried out missile attacks on Asmara Airport in Eritrea and Bahir Dar and Gondar airports in Ethiopia. Islamic State in Khorasan Province (ISKP) claimed responsibility for an attack on Kabul International Airport using rockets that killed one civilian, injured another and slightly damaged a Kam Air aircraft on the ground. Bagram Airport was also targeted by rockets for the first time since the signing of a peace agreement with the US.

A Mission Aviation Fellowship (MAF) aircraft was set on fire by a group claiming to be part of the West Papua National Liberation Army. The seven passengers and crew survived the incident after being ordered off the aircraft by armed men who fired a warning shot in the air shortly after it landed at an airstrip in Intan Jaya Regency, Papua, Indonesia. In a related incident in Mimika, Papua province, Free Papua Movement rebels opened fire on a helicopter conducting a survey. A bullet was found on the helicopter's fuselage, but it landed safely and there were no injuries.

It is not only aviation assets in conflict zones that terrorists and other malicious actors are interested in targeting though. During judicial proceedings in Ireland involving a woman accused of being a high ranking member of the New IRA, the court were told of an alleged plot to attack Shannon Airport, to show support for Arab terrorists because of the use of Shannon Airport for the transporting of American troops. Sikhs for Justice, a US-based fundamentalist/pro-Khalistani group, threatened that it would not allow two flights from Delhi's Indira Gandhi International Airport to reach London (on a specified date), resulting in the airport being placed on alert. Mumbai Airport increased their security posture after intelligence inputs warned that terrorist organisations may target the airport on a given date. Additional security measures were implemented at Chennai Airport in India after an intelligence report warned of a possible terror attack on Republic Day. Security was also enhanced at Barcelona Airport following arrests of Islamic State suspects in the capital, a precautionary measure but one that indicates concerns about the possible targeting of aviation assets there.

OVERFLIGHT SECURITY

The decision to allow overflying of particular conflict zones in whole or part, requires careful risk management by states, civil aviation authorities, and airlines if state approval is granted. The risk assessment process is dynamic and much dependent on access to reliable intelligence and information, appropriately shared.

Overflight security linked reporting for the period included: A Russian Interstate Aviation Committee warning over the potential risk to civil aircraft due to the resurgence of hostilities in the disputed Nagorno-Karabakh region of the Caucasus. The committee expressed concerns about the use of missiles and other weapons and the possible threat posed to international flights, despite the NOTAM measures in place. Azerbaijan issued an airspace warning advising that Armenia has been using long-range missiles to target civilian interests throughout the territory.

BOMB THREATS AND HOAXES

The high level of hoax threat messaging continued to disrupt the sector's operational activities, and all the linked incidents reported in our monthly Insight reports were subsequently deemed to be non-credible threats. Threat messages were received via a multitude of sources including: direct from airline passengers, written threats found on board aircraft, via telephone, fax, social media (including a YouTube video), email, and one of particular note being broadcast as a digitised voice on an air traffic control frequency. In addition, placed 'hoax' items also featured in our reporting.

A re-emerging trend that dates back to 2018 is the *'Bitcoin extortion bomb threat'* which takes the form of an email or faxed threat message demanding that a specified sum of money be paid into a named bitcoin account, or a remote bomb would be activated at the airport or on an aircraft. The criminals behind these extortion bomb threats (and linked 'sextortion' threats) are said to be making $1.2m per year.

Responses to the threat messages and *placed items* resulted in airport and runway closures, evacuation of buildings and aircraft, and additional searches of aircraft, passengers, cargo and baggage. The level of disruption resulting from bomb and other threats made against aviation assets highlights the importance of having trained and experienced

threat assessors available 24/7, to avoid unnecessary 'abundance of caution' approaches.

INTERFERENCE WITH AIR TRAFFIC CONTROL

A 32-year old male in Germany was arrested for using two-way radios to interfere with air traffic. For a period of six months he attempted to redirect aircraft, including police helicopters. His arrest came after he made contact with a police helicopter dispatched specifically to catch him. The male contacted the police helicopter and police were able to locate him shortly afterwards. A search of the subject's home resulted in the discovery of a pair of radios capable of broadcasting on aircraft frequencies. The male's motives are not currently known.

AVIATION-RELATED CYBERCRIME

The Aviation-ISAC, an international cyber-threat sharing organisation providing aviation-specific threat information to the aviation community, reported seeing a 'tremendous increase' in ransomware attacks on airports and they continue to find a growing inventory of airport credentials being sold on the dark web. Mention was made that hackers on the dark web were selling access to the networks of Pakistani International Airlines, Kuwait Airways, Thai Airways and the Brazilian Department of Airspace Control. Hackers also attacked the Automated Weather Observing system (AWOS) at an airport in Canada, and computer scientists reported that next-generation collision avoidance systems (ACAS-X) appear to be just as vulnerable to signal spoofing attacks as older equipment. Cyber attacks are also reported to be increasing in the freight transport sector, and a ransomware attack on Forward Air's operational and informational technology systems caused shipping delays for its customers.

IndiGo Airlines advised that a data server breach may have compromised some passenger data, and Chinese hackers are gathering passenger details from airlines across the world to track high-value targets' movements. The perpetrators targeted airline companies in different

geographical areas, with hackers reportedly scraping user data from the RAM of flight booking servers.

A new advanced persistent threat group using the name LazyScriptor is reported to be using remote access trojans to target the International Air Transport Association (IATA), multiple airlines, and individuals planning to emigrate to Canada on government job-related programs. LazyScriptor was first discovered in December, but appears to have been active since 2018.

INSIDER THREAT MANAGEMENT

The need for effective personnel security and insider threat management is highlighted by the volume of 'insider' cases reported in the past six months. Linked job roles include directors, front-line workers, civil aviation authority officers (PK), an airport police officer, immigration officers, an air traffic control officer, pilots and cabin crew. The range of alleged unlawful activities include money laundering, smuggling, corruption, complex thefts, immigration fraud, fraudulently obtaining pilots' licenses, criminal damage to ATC communications equipment,the placing of a fake bomb, misuse of drugs, sexual offences, and impersonating police. The significant number of staff in the sector who have been made redundant or been furloughed, and those working remotely introduces additional personnel security challenges.

IMPACT OF EXTERNAL EVENTS ON AVIATION SECURITY AND RESILIENCE

The credible warnings of violence from extremists before the US presidential elections provide us with a recent example of the impacts external events can have on the safety and security of the aviation sector, and reinforces the need for security/risk directors to take a broad view of external threats and risks that could prove disruptive for the sector. In another example, an intentional explosion in a camper vehicle parked outside a building housing AT&T network equipment in Nashville halted

flights out of the airport there due to telecommunications issues. 911 emergency systems up to 180 miles away were incapacitated.

COVID-19

INTERPOL warned of the organised crime threat to COVID-19 vaccines and issued a global alert to law enforcement authorities for them to prepare for such unlawful activities. Ensuring the safety of the COVID-19 vaccine supply chain is essential, and the International Air Cargo Association and Pharma.Aero released a report outlining recommended practices and insights for effective COVID-19 vaccine air transportation and handling. The report advised that airports may want to consider additional security and mitigating measures, and encouraged air cargo stakeholders to conduct internal risk and threat assessment for external, insider and cyber threats to ensure the timely rectification of any deficiencies.

Europol issued a recent warning about an Irish gang trading fake Covid-19 certificates. The *Rathkeale Rovers* operate throughout Europe, and have been producing false test results for people travelling throughout the continent who need a negative result upon arrival into countries. Other detections of people selling false coronavirus test results to passengers were made at Paris Charles de Gaulle Airport and London Luton Airport.

Several reports were received of passengers presenting false coronavirus test results, one notable case involved a senior police officer assigned to the Philippine National Police Laboratory. Whilst such activities are not aviation security matters per se, they do threaten passenger/public health efforts, and introduce criminality into the aviation environment.

FINDINGS

The key trends, risks and vulnerabilities identified during this review are:

- Established terrorist groups retain their unhealthy interest in the sector and will repurpose themselves to exploit the crisis and our recovery from it

- Al Shabaab possesses or has access to weaponry that presents a risk to civil aviation operating at low altitudes. The group maintains the capability to develop concealed IEDs and the intent to use them against civil aviation. Al Shabaab has been the most active against aviation during this reporting period
- Malicious actors still regard 9-11-style hijacking attacks (using aircraft as weapons) as viable
- Mortars, rockets and weaponised drones are increasingly being used to target aviation assets in conflict areas
- Many responses to bomb/threat calls and messages appear to be taken out of an unnecessary abundance of caution, despite a lack of threat credibility
- The *Bitcoin Extortion Bomb Threat* first seen in 2018 is circulating again
- Cyber criminals have increased their targeting of the aviation sector. *LazyScriptor*, a new persistent threat group identified in December 2020, has been active since 2018
- COVID-19 / health protection activities risk detracting focus from security
- *Rathkeale Rovers*, an Irish crime gang operating across Europe, has been producing false COVID-19 test results for people travelling throughout the continent
- The level of insider threat activity impacting the sector reinforces the need for robust insider threat management plans

SIMPLE STEPS TO ENHANCE SECURITY RESILIENCE

- Adopt a Security Management Systems (SeMS) approach to ensure the integrity of aviation security and demonstrate robust oversight in a dynamic environment, far beyond what compliance alone provides
- Ensure the 24/7 availability of trained and experienced Threat Assessors
- Avoid ‘fixed’ thinking by continually reviewing the ever-changing risks and instituting new and changed measures accordingly. External threats and risks that could prove disruptive for the sector should be included in the ‘search for risks’
- Review Insider Threat Management Plans and adapt as necessary
- Enhance collaboration between physical and cybersecurity teams to reduce the risk of missed *warning signals* and encourage a unified

approach to risk management
- Strive for the appropriate balance between security and health protection measures and ensure that security investment is not compromised
- Encourage active collaboration between physical and cyber security teams, and other corporate risk managers

CONCLUSIONS

As the phoenix rises from the ashes, the sector needs to be mindful that terrorists and other malicious actors retain their unhealthy interest in civil aviation. They are innovative in their approach, not only deploying previously used techniques, but also seeking to devise and deploy new methods to target aviation assets. Weaknesses in civil aviation security will create potential attack opportunities for our adversaries.

Whilst our vision may have been clouded by the devastating impacts of the pandemic, the need to have a clear view of the threats and risks facing our organisations is key, together with robust mitigation and response strategies. A properly implemented SeMS will produce assurance beyond compliance under a simple framework that makes best use of an organisation's resources, policies, systems and tools. In this way, the industry frees itself from unnecessary 'abundance of caution' responses and the inefficiencies and costs they create. Getting the balance right between public health measures and security will be key. Underinvesting in security will come at a great cost.

Get in Touch

Please contact us if you have any questions or would like to discuss the platform and arrange a demonstration

CONTACT US

Location

85 Great Portland Street, First Floor, London W1W 7LT

Office Number 0203 4750 753

Subscribe

Subscribe to our newsletter to stay up to date with our most recent articles and updates.

SUBSCRIBE