Pool Re SOLUTIONS
Building resilience against terrorism risk

Equitable House, 47 King William Street, London, EC4R 9AF
+44 (0) 20 7337 7170
poolre.co.uk

Sector Risk Report: Airports

Has the terrorist threat to airports changed post pandemic?

July 2022

Executive Summary

As key players within the UK economy and vital aspects of the UK's Critical National Infrastructure, it is unsurprising that airports remain high value targets for terrorist attacks. Traditionally malicious actors have primarily targeted aircraft however, significant security improvements and mitigations have shifted the threat onto airports themselves and in particular landside areas. While low complexity methods have dominated the terrorist threat landscape in the UK in recent years and would undoubtedly cause significant costs if used to target airports, the threat posed by terrorist use of explosives against airports remains. Despite strict airside security measures, landside areas are at an increased risk due to their status as Publicly Accessible Locations (PALs)[1] and increased crowding as a result of the current staffing crisis. Moreover, the staffing crisis has also caused an increased risk of insider threats resulting from mass recruitment to combat the crisis. As a result, it is assessed that there is a moderate terrorist threat towards airports in the UK. Despite the vital mitigations already in place within airports, there is space for improvement with regards to landside areas, particularly as the terrorist threat will remain in the long term.

[1] A publicly accessible location is defined as any place to which the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission. For more information, please visit: https://www.gov.uk/government/consultations/protect-duty

Key Findings

- As airside security measures within airports have become more stringent, malicious actors may target landside areas instead of traditional airside targets.
- Significant staff shortages at UK airports have resulted in shortened recruitment processes, possible lower recruitment standards due to increasing pressures, and a reduction in the required counter-terrorism training and background checks for new starters.
- Increased media attention surrounding airport staff shortages and significant queueing has exposed airports as PALs that may be exploited by malicious actors.
- Islamist actors have historically shown the greatest intent to target airports, however, attacks by environmental extremists or single-issue actors cannot be discounted.
- While Person Borne Improvised Explosive Devices (PBIED) attacks have been the primary mode of attack toward airports globally since 1980,[2] threat actors in the UK are statistically more likely to conduct a marauding attack using bladed weapons or Vehicles as Weapons (VaW). These low complexity methods have featured more prominently within recent UK attacks and require minimal skills and preparation. Such an attack would lead to considerable business interruption and loss of attraction as people avoid airports, which would further exacerbate the financial pressures on airports.
- On current trends, environmental extremists are likely to continue targeting airports with disruptive measures, causing little to no physical damage, but significant business interruption. It is unlikely these actors will act violently towards airports in the near future; however, more violent offshoots of existing groups cannot be ruled out. It is more likely that they will continue to disrupt operations through protests or the use of drones. While these actors do not currently fall under the definition of terrorism, adaptations in their behaviours may lead to terrorist proscription.
- Lower complexity methods or even hoaxes are the most likely tactic to be used by terrorists targeting airports and have the potential to cause a huge economic impact through non-damage business interruption (NDBI) and loss of attraction, regardless of physical damage.

Introduction

Civil aviation forms a significant part of the UK's Critical National Infrastructure (CNI) and contributes considerably to the British economy both directly and indirectly. In 2019, the air transport sector alone contributed £5.47 billion to the UK economy, and the entire aviation industry contributed almost £22 billion.[3] From the 1970s through to the 2000s,

[2] 'Designing Airports for Security: An Analysis of Proposed Changes at LAX', *RAND: Public Safety and Justice*, 2. https://www.rand.org/pubs/issue_papers/IP251.html
[3] UK aviation: reform for take-off, *UK Parliament – Transport Committee,* UK aviation: reform for take-off - Transport Committee (parliament.uk)

there has been a five-fold increase in UK air-travel[4] with UK airports handling almost 300 million passengers each year.[5][6] Furthermore, following the fall in passenger numbers as a result of the COVID-19 pandemic, the International Air Transport Association (IATA) expects global passenger numbers to reach four-billion in 2024, exceeding pre-pandemic levels. As key economic players and vital CNI sites, airports therefore make attractive targets for terrorists. The continuing terrorist threat to the UK combined with the recent staffing shortages and significant queueing witnessed at many of the UK's major airports, has further increased the threat to airports. This underlines the continuing importance of appropriate threat awareness, understanding of possible vulnerabilities, and implementation of risk mitigation measures to protect airports.

LONDON, UK - 30 MAY, 2022. Hundreds of passengers in long queues at Heathrow Terminal 2 on May 30th. (Photo by: Mark Thomas/Alamy

Context

Historically, UK airports have witnessed plots carried out by a variety of actors, including the 1994 IRA mortar attacks at Heathrow airport. Security advances following the 9/11 attacks have made aviation security more stringent and attacks on aircraft more difficult. Consequently, the threat to airports' landside areas has increased as terrorist actors still seek high-value and high-profile targets of attack. The Glasgow airport attack in 2007[7] is perhaps the most well-known terrorist attack targeting an airport in the UK in the past 20 years; however, other malicious events such as cyber-attacks, environmental protests, and drone sightings have also caused significant disruption.

Airports are currently at a heightened risk in the UK as a result of a staffing crisis. As the media continues to report on understaffing and long queues at airport terminals, it is

[4] UK. Department for Transport (2003) The Future of Air Transport.
[5] United Kingdom: Value of Aviation, *IATA*, https://www.iata.org/en/iata-repository/publications/economic-reports/united-kingdom--value-of-aviation/
[6] Aviation Trends Q3 2018, *CAA*, https://www.caa.co.uk/Documents/Download/3156/83738415-f8e3-4e83-ae7b-703a8e594cc6/11
[7] See Case Study 2 in the annexe for more details about the 2007 Glasgow airport attack.

possible that malicious actors will seek to exploit airport deficiencies highlighted by the media in order to carry out an attack. Furthermore, the current fast-tracked recruitment to combat staff shortages increases the risk of lowered recruitment standards, and/or inadequate background checks and training - increasing the 'insider threat'.

Threat Assessment

The threat of a terrorist attack targeting an airport in the UK is currently assessed as moderate. Terrorist targeting of airports is powerful and symbolic with the potential for significant economic and societal consequences. The landside areas within airports also provide a publicly accessible alternative to targeting aircraft and highly secured airside areas, whilst inflicting a similar impact, as was seen in the Zaventum airport attack in Brussels.[8] Therefore, airports will remain a targeting priority for malicious actors in the long term.

Threat actors based in Great Britain, regardless of their ideological motives, have relatively limited capabilities. This is largely due to the difficulty in obtaining weaponry, ammunition, or explosive precursor materials as a result of strict regulations, purchase monitoring, and strong counter-terrorism capabilities within the security services. While airports remain a desirable target for threat actors, significant improvements to airport security have helped to mitigate the risk of a successful attack.

As a result of restrictions on weaponry and precursor materials, terrorists are most likely to use low complexity methods to target an airport such as attacks using bladed weapons or using Vehicles As a Weapon (VAW). While less likely, Islamist extremists continue to demonstrate a desire to employ Person-Borne Improvised Explosive Devices (PBIEDs)[9] which could cause mass casualties, property damage, business interruption and economic losses.

There is a realistic possibility that extremists will use cyber-attacks or drones within future plots. In the UK, we are yet to see a viable attempt at weaponising drones for destructive purposes; however, based on previous drone usage, it is more likely they will be used to disrupt airport operations or air travel. Environmental extremist groups and activists, though not yet officially designated as terrorist organisations, have demonstrated a desire to use drones disruptively towards airports in protest against the aviation industry's impact on climate change. While environmental extremists and activist groups are currently unlikely to cause significant property damage or cause mass casualties, this cannot be ruled out in the future, particularly when controversial decisions over runway expansions are made. Nevertheless, the disruption caused by such groups is likely to lead to sizeable business losses.

Tactics

Different tactics are explored that might be deployed against airports and outline their potential effects:

Person-Borne Improvised Explosive Devices (PBIED)

[8] See Case Study 1 in the annexe for more details about the 2016 Brussels attack.
[9] See Case Study 1 in the annexe for more details about the 2016 Brussels attack.

Research based upon the RAND-MIPT Terrorism Incident Database found portable explosives to be the most frequent and deadly mode of attack from a sample of 75 airport attacks worldwide since 1980.[10] Terrorist use of PBIEDs in attacks against UK airports remains a realistic possibility in the medium term, with passengers in check-in zones and landside areas being the likely targets. The damage caused by such an attack is likely to increase if there are multiple transport hubs within a single location, such as a bus station, train/tube station and airport. This was seen in the Brussels Airport attack in 2016[11] where members of the Brussels Islamic State terror cell conducted a coordinated PBIED attack which killed 32 civilians and injured over 300 other people. Following the attack, the airport was closed for over a month while local hotels, public transport and airport businesses reported heavy losses. A foiled PBIED plot in 2017 in Manchester airport demonstrates the threat posed by this tactic in the UK.[12] Any PBIED attack would require a high level of planning, access to explosive materials and a level of reconnaissance at the intended target site. This tactic, if successfully deployed, would be likely to result in both significant casualties and costly property damage and significant long-term business interruption.

Low Complexity Methods (Bladed Weapons or Vehicle As a Weapon (VAW))

With experts estimating that there will be approximately six billion aviation passengers annually by 2030,[13] airports increasingly present crowded places. As PALs with large volumes of people, this presents an opportunity for terrorists to employ lower complexity methods successfully.

GLASGOW, UK - 01 JULY, 2007. Failed car bomb attack on Glasgow Airport (Photo by: Andrew Milligan/Alamy Live News)

[10] 'Designing Airports for Security: An Analysis of Proposed Changes at LAX', *RAND: Public Safety and Justice*, 2. https://www.rand.org/pubs/issue_papers/IP251.html
[11] See Case Study 1 in the annexe for more details about the 2016 Brussels attack.
[12] See Case Study 3 in the annexe for more details about the foiled plot in Manchester airport.
[13] 'The Threat Among Us: Insiders Intensify Aviation Terrorism', *US Department of Energy*, p. 7. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-25689.pdf

A bladed weapons attack would require minimal prior planning or preparation and could easily target landside areas, including airport check-in and arrival zones. Despite the panic and hysteria this method would cause, these attacks would likely result in relatively few casualties and limited to no property damage or long-term business interruption. Equally, a VAW attack requires minimal planning and capability but has the ability to cause significant human casualties, high levels of property damage and business interruption. The 2007 Glasgow airport attack[14] demonstrates terrorist intent to use VAW to target airports and with excessive crowds being recently documented queuing outside airports, the potential for mass casualties as a result of a VAW attack is increasingly concerning.

Drones

In the recent past, concerns have been expressed about the potential use of drones - either accidentally or maliciously – to disrupt airports. It is most likely that drones will be used non-violently to disrupt business activity and bring airports to a stand-still. Although not designated an act of terrorism, in 2018, Gatwick Airport was closed for two days following reports of drone sightings close to the runway causing estimated losses of over £100 million. The use of multi-drone displays has been recently seen in celebrations such as the Queen's platinum jubilee. It is therefore possible that terrorists could be inspired by these displays and attempt to use drone swarms for disruptive purposes or to target aircraft. As drone technology becomes more advanced, drones are likely to feature within attack plans with increasing severity. Whilst evidence is yet to be seen of the ability to arm drones with explosives within the UK, this cannot be ruled out in the long term.

Cyber Threat

Much of the aviation industry – particularly airports – rely on technology in managing access, screening, verification, and communications. As airport security becomes more advanced and on-site attacks less achievable, is it possible that threat actors may aspire to use cyber-attacks to target airports for disruption, or to manipulate systems to enable a physical attack. Cyber-attacks have previously impacted the day-to-day business of airports, bringing flights to a stand-still and causing severe disruptions. However, the threat of terrorist groups conducting a large-scale cyber-attack on an airport is considered low, given current deficiencies in cyber-capability and the lack of intent of malicious actors to develop these.

Chemical, Biological, Radiological (CBR)

While the use of CBR materials by terrorists in an airport attack would have a very detrimental impact, both directly and due to the consequent business-closure for clean-up, the likelihood remains very low. In March 2021, the Secretary of State for Defence stated that the UK could see a successful CBR incident before 2030. It is more likely that an airport could see a low sophistication hoax or threat to conduct a CBR attack as opposed to actually experiencing a successful attack due to the difficulty in obtaining CBR material. The likelihood of a hoax still remains fairly low, however, the NBDI costs of

[14] See Case Study 2 in the annexe for more details about the 2007 Glasgow airport attack.

evacuating the area for an extended period of time to ensure it is safe could still be considerable.

Potential Impact (disruption/destruction/NDBI)

A terrorist attack on an airport would likely result in economic losses and business interruption. Higher complexity terrorist attacks would likely cause moderate to significant physical damage dependent on the tactic used. However, lower complexity methods or even hoaxes have the potential to cause a huge economic impact through non-damage business interruption (NDBI), regardless of any physical damage.

Low complexity attacks or incidents which can be contained to small areas of the airport would undoubtedly lead to significant NDBI costs and consequent financial impacts due to loss of attraction following an attack. However, the resultant costs would be minimal in comparison to the effects of more complex attack methods or attempts that would trigger a full terminal evacuation. Regardless of the whether there is a successful attack or an undetonated IED is identified, the evacuation, cordoning and post-attack clean-up process is likely to have considerable negative economic effects.

Following discussions with senior security officials at several UK airports it is estimated the NDBI costs could amount to between £125,000 and £600,000 for a 7-hour evacuation, irrespective of the cause of the evacuation. These costs would obviously be dependent on the time of day, time of the year, passenger profile, and airport size. Following a successful attack requiring longer periods of evacuation and site closure, NDBI costs alone could reach millions of pounds.

Mitigation

The airport industry is highly regulated across the globe. The International Civil Aviation Organization (ICAO) have international baseline standards for areas - including design and security regulations - which airports across the globe are required to follow. Internationally aligned standards and regulations help to mitigate the terrorist threat to airports. Most nations also have their own additional standards alongside the requirements outlined by the ICAO. In the UK these are set by the Civil Aviation Authority (CAA), whose standards are more stringent than those set by ICAO and place the UK as one of the most proficiently regulated bodies with regards to airport regulation, safety, and security.

The Aviation Security in Airport Development (ASIAD) guidance was implemented by the UK Department for Transport in 1996 and revised in 2018 to mandate particular design elements and standards that will improve resistance to bomb blasts; including multi-laminated glass and post-blast retained structural barriers to protect against physical attacks. ASIAD requires those planning, designing and developing airports and terminals to mitigate the impact of a large-scale terrorist attack on airport infrastructure. Its scope includes all airport infrastructure, not just security facilities, however this does not account for unprotected queues outside airport buildings. As such it is important to consider how best to protect these areas in the case that significant queueing continues. Given that recent attacks have now featured lower complexity tactics such as the use of bladed

weapons, and ASIAD was developed with a main focus on bomb blasts, a re-consideration of the guidance which takes into account other methods may be beneficial.

UK airports also require all airside staff to carry out General Security Awareness Training (GSAT), with some airports including this requirement for landside staff. While this is the baseline training required, airports typically provide bespoke in-house training to their staff to ensure specific airport security standards are maintained. Given the increased threat to landside areas due to their relative lack of security measures, increased rollout of GSAT to all airport staff would help to further mitigate the threat or terrorism targeting airports.

The forthcoming Protect Duty legislation will further enhance the requirement to protect the public at airports; airport operators will need to demonstrate they have proportionate mitigation measures in place. However, potential issues about standards of staff training, missed or skipped procedures due to crowd pressures, insider threats from inadequate vetting or failure to protect crowds queueing in more vulnerable areas, including outside terminals, could raise questions over liability where insurance cover is traditionally lower for terrorism than other forms of liability such as health and safety.

Enduring Issues

Despite the mitigations in place, there are a several enduring issues which require further attention to reduce the risks they pose.

Insider Threat

The insider threat to airports comes from an individual with authorised access to information, facilities, people or resources within the airport. An insider threat could include the use of access to facilitate an act of violence, cybercrime, sabotage, or destruction of property. The insider threat to airports is consistently a concern to airport security officials with the current staffing crisis emphasising the risk. As airports attempt to re-establish sufficient workforces, it is possible that malicious actors could gain employment as recruitment standards are relaxed to meet demand.

A leaked letter from the UK aviation minister in April this year revealed the Government's plans to relax vetting rules, permitting new employees to access landside areas and begin their training before security checks are completed. Our interviews with those in the sector revealed this practice had already begun for landside workers, although access to airside remains prohibited until vetting is completed. Allowing un-vetted individuals into the airport together with issues regarding access to training increases the risk of these processes being exploited by insider threats. In 2011, in the UK, a former British Airways employee with links to Al Qaeda was convicted of offering to help damage airline computer systems,[15] and in 2015 two Egyptian baggage handlers successfully took down an aircraft by smuggling a bomb on board at Sharm El Sheikh airport. The mass recruitment of individuals, disaffected or uninterested in their jobs, also potentially presents terrorists with a pool of more easily impressionable airport employees who may

[15] See Case Study 4 in the annexe for more details about the BA insider threat conviction.

be willing to share inside information in exchange for monetary rewards.[16] Therefore, sacrificing the wait for completion of security checks prior to training so as to counter the backlog of vetting poses a significant risk to airport security.

Consequential impact of the terrorist threat to aircraft

Evidence of prior terrorist attacks indicates a desire to target aircrafts in-flight as opposed to directly targeting an airport. However, a consequence of stringent security measures within airports with regards to accessing airside and aircraft is to transfer risk from aircraft to airports. Threat actors wishing to target aircraft may be prevented from accessing airside areas of the airport and instead the threat to the airport itself increases as terrorists make a last resort effort to conduct an attack. The time-consuming check-in and security processes within an airport also present an opportunity during which a device intended for an aircraft could prematurely detonate or activate.

A further consequential threat to airports comes from an attack on an aircraft taking place shortly after take-off or before landing whilst the aircraft is above the airport footprint. Though this is less likely to take place than a mid-flight attack, based on evidence from previous in-flight attacks, this indirect threat can be mitigated through in-airport security measures preventing the individual from accessing the aircraft with an IED, weapon or other attack materials.

Endnote

In researching and composing this airport sector risk report, Pool Re Solutions gained and is sharing a more comprehensive understanding of the evolving threat landscape surrounding airports, their possible vulnerabilities, and the current risk mitigation measures put in place to protect against them.

As security measures within airports have become more stringent, malicious actors may target landside airport areas instead of traditional airside targets, with the potential for significant social and economic consequences.

Airports are currently at a heightened risk in the UK as a result of a staffing crisis which has led to unprecedented levels of queuing both inside and outside of the UK's major airports, as well as a relaxation of background checks for new employees. Furthermore, as emerging threats such as drones and cyber-attacks become more advanced, malicious actors are likely to feature such tactics with increasing frequency in their attack plans. Adapting security measures to account for the changing threat landscape in the UK and the developing vulnerabilities within airports are, therefore, vital to ensure the safety and security of all airports, staff and their customers.

[16] This concern was expressed to us during interviews with senior security officials from UK airports.

ANNEXE

Case Studies

Case Study 1: Brussels airport attack 2016

Event description:	On 22 March 2016 three coordinated attacks targeting Brussels airport and Metro occurred. At the airport, two suicide bombers detonated explosives in the check-in area. A third device was found by police during a search of the airport following the initial blasts.
Methods/Tactics:	Improvised explosive devices hidden in luggage were packed with nails, designed to act as shrapnel in the blast.
Actor:	Islamic State claimed responsibility for the attack. Five attackers were involved; three were killed in suicide explosions and the remaining two arrested. All five attackers were involved in the planning of the Paris attacks in 2015.
Casualties:	16 people were killed in the airport bombings, with hundreds injured.
Impact:	In the immediate aftermath of the bombing all rail transport to the airport was stopped and road closures were also put in place. Air traffic was also halted, and the airport did not reopen until 03 April. The country raised its threat level to the highest level within 90 minutes of the attack. The airport, as well as businesses nearby, including hotels and car rental companies, were badly affected by physical damage and/or business interruption. Brussels airport received a €50 million pay out[17] to cover damage to infrastructure and operating losses and several reports indicate the Belgium economy lost almost €1 billion. An economic impact report by the Belgium government indicated the capital suffered significant losses in both sales and tax revenue in the capital[18].

[17] https://www.brusselstimes.com/41630/brussels-attacks-one-year-on-cost-to-brussels-airport-of-march-22nd-attacks-40-million

[18] https://www.politico.eu/article/brussels-terror-attacks-cost-belgian-economy-almost-e1-billion-report/#:~:text=Czech%20EU%20Presidency-,Brussels%20terror%20attacks%20cost%20Belgian%20economy%20almost%20%E2%82%AC1%20billion,that%20killed%2032%20in%20March.&text=The%20Belgian%20economy%20lost%20close,new%20report%2C%20local%20media%20reports.

Case Study 2: Glasgow airport attack 2007

Event description:	On 30 June 2007 a Jeep was driven into glass doors at a Glasgow airport terminal. The two suspects were arrested following the incident, which was linked to a failed attempt to detonate car bombs in London the previous day.
Methods/Tactics:	The vehicular impact attack involved a Jeep loaded with propane cylinders which was driven into the airport doors. The vehicle did not explode and as a result one suspect threw petrol bombs while the other used petrol to set himself on fire.
Actor:	Two men carried out the attack, however several others were arrested following the incident. This included the brother of one attacker, who had links to terrorist group Al-Qaeda.
Casualties:	No one was killed in the attack however five people were injured either in the attack or while attempting to detain the suspects.
Impact:	In the immediate aftermath of the attack the terminal was closed for 24 hours. Surprisingly, there was little disruption to flights; although a small number of flights were cancelled, the cancellations were within expected levels during summer periods. Other UK airports, including Manchester and Birmingham, closed roads close to terminals, while other airports, including London airports, moved taxi ranks and parking areas further away from buildings. Many airports subsequently installed steel bollards outside terminals, which remain in place today, to prevent further attacks.

Case Study 3: Manchester Airport Foiled Bomb Plot

Event description:	On 30 January 2017, a man tried to smuggle a pipe bomb onto a plane from Manchester to Italy with the intent of detonating the device onboard a Ryanair flight.
Methods/Tactics:	Improvised explosive device found in the lining of a pencil case. The device made from batteries, tape, a marker pen, pins, and roughly 10 grams of gunpowder.
Actor:	One man was arrested following the incident and later sentenced to 18 years in prison. Due to absence of evidence of motivation, the man could not be prosecuted for terrorism offences.
Casualties:	None, however, it is estimated that the device would have caused considerable injury to people close to the device. The device would have posed the greatest threat to the person operating it.

Probable Impact:	Police were called to Terminal 3 of Manchester Airport at 8:50am. An evacuation of the terminal then took place as airport staff removed passengers from planes at the terminal. Bomb disposal experts then carried out a series of controlled explosions. If the device had been successfully detonated, it could have caused considerable injury to those nearby and possible infrastructure damage.

Case Study 4: British Airways Insider Threat Foiled Plot

Event description:	In 2011, a former British Airways (BA) employee plotted to blow up an aircraft while acting under the orders of Anwar Al-Awlaki, a radical Islamist cleric. Rajib Karim used his position as an IT expert at BA to plot attacks against the West and supply terrorists with confidential information. Karim also offered to help stage financial or disruptive attacks.
Methods/Tactics:	Access to British Airways computer systems and airport security protocols.
Actor:	One man was arrested with links to Al-Qaeda and Jammat-ul Mujahideen Bangladesh (JMB).
Probable Impact:	Had Karim successfully provided enough information and planning to Al-Awlaki, the attack would have likely caused a devastating number of human casualties. Al-Awlaki was aiming to target the US through either a person or a package onboard an outbound flight from the UK, and would have likely targeted a high priority target, causing significant structural and possible business damages. Alternatively, BA witnesses said that the airline would lose roughly £20 million a day if its IT systems collapsed, illustrating the possible business losses had Karim staged successful disruptive attacks.

Disclaimer