# AVIATION TERRORISM

**Mark Brace** *examines the increasing use of on-board improvised explosive devices on commercial flights*

**Aviation continues to be a high-impact, media-spectacular target for terrorist groups globally. While a range of methods have been employed by such groups – from firearms attacks at airports, through hijacking and using the aircraft itself as a weapon, to surface-to-air fire against aircraft in-flight – the weapon of choice has remained the on-board improvised explosive device. In the most recent high-profile incident, the so-called Islamic State attempted to get an IED on board a flight from Australia to the UAE in July 2017. That it failed appears to be primarily down to luck – the luggage containing the IED was apparently too heavy, so was taken home by the perpetrator. But it was yet another example of a concealed IED – this time within a meat grinder. It followed the two most recent 'successful' terrorist attacks against airliners: the downing of Russian airline Metrojet Flight 9268 by Islamic State's affiliate in Sinai, Egypt, in October 2015; and the explosion on board Daallo Airlines Flight 159 perpetrated by al-Qaeda affiliate al-Shabaab in Somalia in February 2016. These also used concealed IEDs – in a soda can and a laptop respectively – but were likely facilitated by 'insider' assistance in both cases.**

Al-Qaeda (AQ) didn't invent aviation terrorism – individuals, crime groups, governments and their proxies, and extremist groups with a range of motivations have attempted, often successfully, to bring down airliners with IEDs almost since the dawn of commercial aviation. However, prior to the rise of the Islamic State (IS) group, AQ had the pedigree for targeting the sector, particularly in the development of concealed IEDs. Following the 9/11 attacks in 2001, AQ and its regional affiliate al-Qaeda in the Arabian Peninsula (AQAP) attempted a series of attacks using increasingly sophisticated concealed IEDs designed to defeat aviation security measures. These included:

- **December 2001:** Richard Reid, the 'shoe bomber', attempted to detonate a device made up of plastic explosives packed into the sole of a shoe. A second shoe bomber, Saajid Badat, chose not to go through with the plot, but was only arrested – and his bomb discovered – in 2003 in the UK.
- **August 2006:** The liquid explosives plot. Component liquids disguised as soft drinks were to be assembled into an IED and detonated on board multiple transatlantic flights from the UK to North America.
- **December 2009:** The 'underpants bomb'. A failed attempt to detonate a non-metallic device concealed within a pair of underpants and worn by the operative, on a flight from Amsterdam to Detroit. A further attempt in 2012 using a similar, enhanced device was reportedly thwarted due to the operative being an agent working for government intelligence agencies.
- **October 2010:** The printer bomb plot, in which an IED was concealed to resemble the inner workings of a printer. Two of these printer devices were sent from Yemen to the USA and were only discovered after an intelligence tip-off and extensive, repeated examination of the printers in which they were concealed.

These devices demonstrated ingenuity and a continual adaptation to the security measures of the day, and latterly reflected the work of AQAP's master bombmaker, Ibrahim al-Asiri. None of these attacks was executed as intended, through a combination of disruption by the security and intelligence services, operative error and luck. However, they defeated aviation security measures in each case, and caused massive disruption to air travel, with the lasting effect of changes to aviation security regimes worldwide.

## INSIDER ASSISTANCE

Before the July 2017 attempted attack in Australia, IS had previously targeted aviation – the 2015 Metrojet attack and the 2016 attacks against airports in Brussels and Istanbul. The Metrojet airliner was downed by an IED facilitated onto the aircraft, likely with insider assistance at Sharm el-Sheikh International Airport, from where the flight departed (no one has ever been charged with carrying out the attack). IS' Sinai Branch claimed responsibility for the attack, and IS provided images of what it claimed was the device in an edition of its online magazine *Dabiq* in November 2015 – a relatively simple device consisting of explosives concealed in a soda can. This would not be considered a sophisticated concealment – but it did not need to be, as insider assistance can mitigate the shortcomings of a rudimentary or poorly concealed device, as it appears to have done so in this case.

However, the Australian plot marked a significant uplift in IS capability to strike away from the battlefield in Syria/Iraq. The component parts of the device – including high explosives – had been sent via air cargo from Turkey to Australia. While it remains unclear whether the meat grinder IED would have defeated security in this instance – it did not get that far at the airport – authorities in a number of countries affected by the plot have indicated that it likely would have done. Regardless of this, IS now knows it can send IEDs or component parts through air cargo potentially anywhere in the world, either to target aircraft or to enable operatives to carry out attacks in their home countries. As IS continues to be squeezed in Syria/Iraq, this kind of approach could provide the remnants of the group with an element of resilience, as it does not require large numbers of personnel. In order to detect such a device or its components, changes would be necessary to the level of scrutiny that air cargo and parcels undergo, and the parameters and sensitivity of any detection equipment would need to address the size and nature of component parts of such a device.

Picture credit: Getty

**Debris of the Russian airliner after the plane crashed in Egypt's Sinai Peninsula**

The group's targeting of aviation contrasts with the general trend for low-sophistication attacks by lone actors or small groups. As well as recognising the value of aviation as a target for terrorist attacks, IS may have learned from AQ aviation successes in the past – AQAP has shared some details of its aviation attack methodology through its *Inspire* publication, for example step-by-step instructions provided in December 2014 to make a version of its non-metallic IED used by the 'underpants bomber'. However, IS has undoubtedly benefited from a permissive operating space in Syria/Iraq, where it has been able to research, develop and perfect IEDs and concealments – as AQAP previously did in Yemen.

The use of an aviation insider – an individual who uses their legitimate privileged access to an airport or airline, knowingly or unwittingly, to facilitate an attack against an aviation target – is not an attack methodology in its own right. It's an attack facilitator. But it's a key ingredient of IED attacks that can be prevented.

## ON-BOARD IEDS

The two most recent successful terrorist attacks against commercial aircraft – Metrojet and Daallo Airlines – involved the use of on-board IEDs. However, crucial to the success of both was the likely use of insider assistance to facilitate these IEDs through security at the airports from which the attacks were launched (Sharm el-Sheikh in Egypt and Mogadishu in Somalia). In the Daallo Airlines case, a senior security figure at Mogadishu Airport was involved in facilitating the IED through security and into the hands of the suicide operative who took it on board the flight. The IED itself was concealed within a laptop; the laptop passed through security x-ray scanners, and images of these x-rays have subsequently shown that the IED could not be considered a high-tech, sophisticated concealment, and should have been detected by competent, trained security operatives. What we do not know, however, is whether the security operatives lacked training, were colluding with the senior insider, or did not subject him to the same level of scrutiny due to his position.

For some observers, it might be easy to dismiss these incidents as happening in corrupt corners of Africa with lax security procedures. However, it can also be a problem closer to home, as exemplified by the British Airways software engineer Rajib Karim, jailed for 30 years in 2011 in the UK for plotting to use his access to assist key AQAP figure Anwar al-Awlaki in carrying out a terrorist attack.

▶

While effective training of security staff is obviously of paramount importance, personnel security is just as key. The insider threat is not a problem unique to the aviation industry, but it is particularly at risk given the priority that terrorist groups attach to targeting aviation. As security measures improve, the use of insiders will become increasingly important to terrorist groups, which will likely take a more proactive and systematic approach to the recruitment and placement of insiders within the industry. While the threat can never be completely mitigated, organisations can maximise their chances of discovering and disrupting insiders without having to depend on a well-resourced government security agency. Fostering an appropriate security culture and developing robust personnel and cyber/IT security policies can be enhanced with materials and tools available in the public domain.

## THE KNOCK-ON EFFECT

The human cost of any successful terrorist attack – not just against aviation – is obvious. But even an unsuccessful attack that doesn't reach fruition has a magnified effect on the industry. Security responses to plots in recent years remain with us – limits on liquids in hand luggage, removing shoes at security – and increase with every reported or alleged plan to bring down an aircraft. In 2014, limits and checks on personal electronic devices like mobile phones, tablets and laptops were introduced, reportedly in response to intelligence indicating the so-called Khorasan Group, a collective of AQ veterans in Syria, which was plotting to attack aviation using explosives concealed in such devices. More recently, the US and other governments implemented further measures in relation to laptops on aircraft in early 2017, this time reportedly in response to an alleged IS plot against aviation. The industry is affected in other ways too: following the Metrojet attack, Russia stopped flights to Egypt, and the UK banned flights to Sharm el-Sheikh. Egyptian tourism revenues slumped. This is exactly the kind of impact terrorist groups want. Russia eventually recommenced flights to Egypt in April 2018, but only to Cairo; the UK ban on Sharm el-Sheikh flights remains in place.

Responding to each attack as it happens is impractical and unsustainable in the long term. Security measures are only as effective as the people doing them – standards vary the world over. And it's a safe bet that terrorists will be seeking to find a way round new measures as soon as they're introduced. There have been some incredible intelligence-led successes in stopping terrorist plots targeting aviation worldwide; the kind of international cooperation that facilitates this will continue. However, there will always be some that slip through the net. While other disruptive options are possible, such as direct kinetic military activity, governments know they cannot just drone-strike their way out of the problem. There is a need for holistic, longer-term, future-proof technological solutions as part of an international collaborative effort between governments, regulators and the industry.

Emboldened and encouraged by perceived successes, terrorist groups are likely to continue to target commercial aviation through developing ever-more sophisticated concealments for their IEDs. They are likely to look beyond, to 'non-traditional' IEDs capable of incorporating chemical, biological and radiological agents. The threat is not just evolving – it's broadening. Every method and technique that has been tried by terrorist groups to target aviation is still available to them, and could be used by branches, affiliates, cells and individuals in different parts of the world previously unaffected by these issues – wherever extremists have the reach.

These groups aren't going away any time soon. Governments and the aviation industry will need to stay one step ahead of them or come up with a more comprehensive, longer-term solution to the problem. Preferably both ●

**Mark Brace** – Aviation Security Analyst at Osprey Flight Solutions – has many years' experience in the public sector as a senior aviation security intelligence analyst in the UK government.

**The shoes used in the failed attempt to blow up a plane by shoe bomber Richard Reid back in 2001**

Picture credit: Getty