

SLIPPING THROUGH THE NET

Tony Kingham examines how airports are trying to ensure that terrorists aren't able to smuggle explosive devices onto airplanes

The ban on laptops and tablets in cabin baggage on flights from some countries in the Middle East and North Africa to the US and UK has once again thrust airline security into the limelight.

Nine airlines from eight countries are covered by the US ban: Turkey, Morocco, Jordan, Egypt, the United Arab Emirates, Qatar, Saudi Arabia and Kuwait, while the UK ban affects all flights out of Egypt, Turkey, Jordan, Saudi Arabia, Tunisia and Lebanon. So, what lies behind this ban?

The US Department for Homeland Security has cited attacks on planes and airports over the past two years as the reason for the ban and UK sources reported that the ban was not connected to any specific threat intelligence.

RAMAN SPECTROSCOPY IS ONE TECHNOLOGY THAT HAS SHOWN A GREAT DEAL OF PROMISE

However, the cloud of mystery surrounding the ban is doing nothing to quell speculation. The fact that other countries have failed to follow suit with bans of their own would suggest that no specific threat intelligence does exist.

What is most likely is that there is sufficient chatter being monitored over the airways, internet etc. to prompt both the US and UK to implement a ban as a precautionary measure until more concrete intelligence is known.

What is a fact, however, is that holes in airline security exist and terrorist organisations are determined to exploit them. Why do they bother, when attacks like the recent one on Westminster in London attracts just as much publicity? One answer may be that attacks on airliners are considered "spectaculars" by terrorists in general and by al-Qaida in the Arabian Peninsula (AQAP) in particular. Which is why AQAP is the most likely suspect to be the principle motivation for the ban. AQAP has a long history of attacking airliners and is known to possess a

good deal of technical know-how or trade craft when it comes to smuggling bombs on aircraft including the underwear bombers and using bombs hidden in computer printers.

The inconvenience of security screening queues at airports is one of the most obvious ways in which terrorism has permanently changed our way of doing things and a reminder to all of us every time we get a flight that al-Qaida is out there trying to do us harm.

There may also be another reason why it persists in targeting airliners. In the warped world of terrorist politics, influence and recruiting, ISIS has rather cornered the market in barbarism, brutality and as a result it has dominated media headlines and thus, recruitment in recent years. As we have seen from recent attacks, although the Westminster attack has gone unclaimed, most of the so-called lone wolf attacks have been on behalf of ISIS despite the fact that many of the attackers have never even been to Iraq or Syria and have not been directly recruited.

So, in a sick form of brand differentiation AQAP might be trying to demonstrate that it is a more sophisticated organisation and try and recapture the heady days of post 9/11 when it dominated the terrorist agenda. Whatever the motivation, it knows and we know that there are holes in aviation security and they are working towards exploiting them.

So, what of this latest threat? It has been widely reported that the ban is the result of the discovery of a plot to hide a bomb in an iPad, according to a report that seems to have first appeared in the UK's *Guardian* newspaper.

LAPTOPS LOSE OUT

Whether the report is true remains unconfirmed, but it would seem highly likely given that the attack on last year on a Somali airliner was also suspected to have been hidden in a laptop.

So why given that we have invested so much in security in recent years is a ban on laptops in cabin baggage, the only answer to this particular threat? The problem is that we still do not have a way of detecting explosives as they pass through the conveyor belt scanners that we are all familiar with at airports, secure buildings, events etc. These are



A Kuwaiti traveller puts his laptop inside his suitcase at Kuwait International Airport before boarding a flight to the United States

X-ray scanners and they can detect some substances by looking at the density of the items being examined, but when it comes to a bomb disguised inside a laptop or other electronic device for all practical purposes, it is impossible.

Explosives can be detected by a variety of equipment using technologies such as ion mobility spectrometry (IMS) like the Smiths Detection IONSCAN 500DT, which uses a wand-like device to detect trace substances that can then be analysed in the machine in a few seconds.

However, the problem is when there is a heightened threat, as we appear to have at present where to scan every laptop or device would mean every person and every device being scanned every time instead of on a targeted basis as it is now. And this would cause unacceptable delays and security screening chaos.

So, for the authorities faced with a tangible threat, a blanket ban is really the only short-term answer. After all, if an aircraft were attacked and destroyed and it became known that the authorities knew about

the threat and failed to act there would be justifiable outrage. Better inconvenience, than more innocent terror victims.

The technological answer to this particular problem (ie a standoff explosive detection technology that can be incorporated into the security screening line) is a long time coming and has seen many false dawns. Including the so-called puffer machines, which promised much but proved far too unreliable to work in a busy airport environment.

Raman spectroscopy (RS) is one technology that has shown a great deal of promise. It identifies potential explosives by detecting changes of vibrational energy level states in response to laser illumination, providing a repeatable spectral response. In this way, it is able to identify the specific response from a database of known substances and identify a wide range of explosives or drugs.

Another promising technology is being developed by Dutch start-up company Stage Gate 11 (SG11).

This uses Hyper-Spectral Differential Reflectometry – again using reflected light – from which it has developed the Delta R shoe scanner. It's not yet in production, but has been extensively tested with good results. If it can work for shoes, then why not for laptops?

Laptops and tablet devices are not the only thing we need to be concerned about when it comes to airline security. While laptop bans focuses attention on one potential weakness in the system, terrorists have the luxury of simply switching target or *modus operandi* until the fuss dies down as it will inevitably will and simply return to it later. In the meantime, what else should we be concerned about? One niggling worry for me is the body cavity bomber.

With practice, drug mules regularly carry anything up to two kilos of illicit drugs swallowed in

EXPLOSIVES CAN BE DETECTED BY A VARIETY OF EQUIPMENT USING ION MOBILITY SPECTROMETRY

capsules in their stomach. It is also possible to carry significant quantities in the rectum.

This is not new, nor is it some weird James Bond film plot. Twice that we know of, terrorists have attempted assassinations of leading figures in the world of security using this method.

In August 2009, the attempted assassination of Prince Mohammed bin Nayef, the Saudi Interior Minister, was the first time that this method of attack was first reported. The terrorist was able to pass through two airport security screenings and the Prince's own security before detonating a device that used a mobile phone card and a half-kilo of explosives that had been inserted in his rectum.

In December 2012, another assassination attempt

was made on Afghanistan's intelligence chief, Asadullah Khalid, using a bomb carried concealed inside the suicide bomber's body cavity, which evaded all security measures surrounding such a high-profile target. Mr Khalid was not killed, but suffered serious enough injuries as a result.

The possibility that the same method could be used to smuggle explosives on board an aircraft is obvious. At present, none of the technology currently employed in departures will identify explosives hidden inside a body cavity.

Back scatter and millimetre wave scanners are whole-body imaging devices and are commonly seen at almost every airport. They will pick up objects carried on the body such as organic materials and liquids, as well as non-organic materials such as plastics and metal, but not inside of it.

However, there is a technology that is already in daily use at airports that will detect any object carried internally, and that is the Through Body X-Ray scanner. These machines are already widely used by custom officials at airports around the world for detecting drugs and contraband smugglers. But as far as we know, there are none currently deployed in departures specifically to counter the cavity bomber threat.

Jan Steven Van Wingerden, CEO of ODSecurity in the Netherlands and manufacturer of the Soter RS Body X-Ray scanner says: "These scans are simple, quick, non-intrusive and safe and will identify any foreign objects, either hidden in body cavities, ingested or indeed carried on the body. Our machines are not for mass scanning purposes, but can be used in support of professional airport security staff as a part of their regular screening process".

The game of cat and mouse between the terrorist and the security community is set to continue and technology will eventually provide an answer to the laptop threat. But where there are already obvious gaps and we already have the technology to fill it, should we not act immediately before we learn the hard way? ●

Tony Kingham is a freelance journalist and publisher of www.WorldSecurity-index.com, specialising in information and public relations within the defence and security markets.



The Soter RS Body X-Ray scanner is able to identify foreign objects hidden in body cavities