Umar Farouk Abdulmutallab and the Christmas Day Attack: Why Aren't Lessons Learned?

December 2009

David Rubens

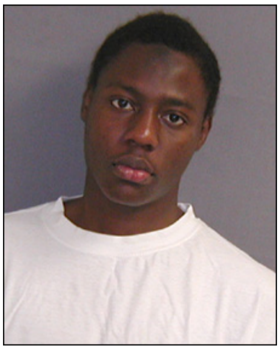
Meido Consultants Limited

The Arches,
Maygrove Road
London NW6 2EE
info@meidoconsultants.com
www.meidoconsultants.com

David Rubens is MD of Meido Consultants, a corporate security consultancy.
He holds an MSc in Security and Risk Management from Scarman Institute, Leicester University, and is currently a visiting lecturer there on their Global Security and Policing MSc programme, as well as being a visiting lecturer in the Security and Resilience Department at Cranfield University at the UK Defence Academy.

david@meidoconsultants.com

Umar Farouk Abdulmutallab and the Christmas Day Attack:
Why Aren't Lessons Learned?



Main Points:

- Effective security management is not merely an amalgamation of separate and unconnected protocols and guidelines, but is something that is (or at least, should be) constructed upon a seamlessly integrated culture of security which permeates every aspect of an organisation's culture and ethos

- Technology offers tools, not answers

- Profiling should be seen as a dynamic component that, in conjunction with other aspects of the security framework, will allow security managers to best identify potential 'persons of interest', rather than merely offering a pre-set list of personal qualities (often based on statistically insignificant pieces of personal information such as race, religion, colour, age, etc).

- Effective security management isn't created simply by the introduction of security protocols, but in the sustained determination to maintain standards of absolute excellence in all aspects of the application of these rules throughout the organisation, at every level and by every person.

- Every security manager knows that the vulnerabilities within their own systems are not caused by a lack of security reviews and guidelines, and that therefore the introduction of another review is not going to change things. The problems in security management stem from the inability to maintain a required standard of individual professional and personal responsibility on a long-term, sustained basis. It is in this area that most security management programmes fail.

- **'There is nothing that we can do to affect the motivation of the terrorists, but what we can control is the opportunity. If an attack is made, it is because something within our system allowed it to happen'.**

The news over the recent Christmas and New Year period was dominated by the reports that a successful attempt had been made by a lone attacker to carry a functional explosive device aboard an international airliner. Although he failed in his attempt to trigger the device, the case once again highlights major systemic weaknesses concerning the issue of airport and national security at every level of operation.

As is usually the case in such situations, authorities have responded by announcing a review into why the national and international security and intelligence communities were not able to pick up someone who by all accounts was already identified as high-possibility potential suspect (and one who had been specifically identified by name to the US authorities), and by highlighting increased use of security technology to prevent similar attacks in the future.

As the Prime Minister posted on his website, 'We now know that the would-be bomber used a small quantity of explosive that went undetected by standard airport security equipment. We need, therefore, to continually explore the most sophisticated devices capable of identifying explosives, guns, knives and other such items anywhere on the body. So - in cooperation with President Obama and the Americans - we will examine a range of new techniques to enhance airport security systems beyond the traditional measures, such as pat-down searches and sniffer dogs. These could include advancing our use of explosive trace technology, full body scanners and advanced x-ray technology. [1]

There have been no shortage of reviews into security failings since the attack on the World Trade Centre, including the exhaustive Congressional Report into the systemic weaknesses that allowed the 9/11 attackers to remain undetected [2]. Given that the those reviews have been widely circulated, coupled with the massive amount of money and research invested in the introduction of new-generation security technology at airports, it is questionable as to how significant one more review or an extra ten x-ray machines will be in preventing future attacks.

If the authorities are serious in wishing to develop a security strategy that will be able to offer a realistic possibility of preventing future tragedies (across society, and not just in airports), then they will need to acknowledge that effective security management is not merely an amalgamation of separate and unconnected protocols and guidelines, but is something that is (or at least, should be) constructed upon a seamlessly integrated culture of security which permeates every aspect of an organisations culture and ethos, from the CEO in the international HQ to the person sweeping the car park or cleaning the toilets.

This paper will attempt to give a brief overview of the current state of some of the main issues in international security, will identify what went wrong in the run up to the most recent incident, and will offer a number of suggestions concerning Best Practice Indicators (BPI) that will be relevant to policy makers and security managers, whatever area of security they are involved in.

International Security Management since 9/11

'Strategic security management is about creating safety, NOT merely reacting to danger'

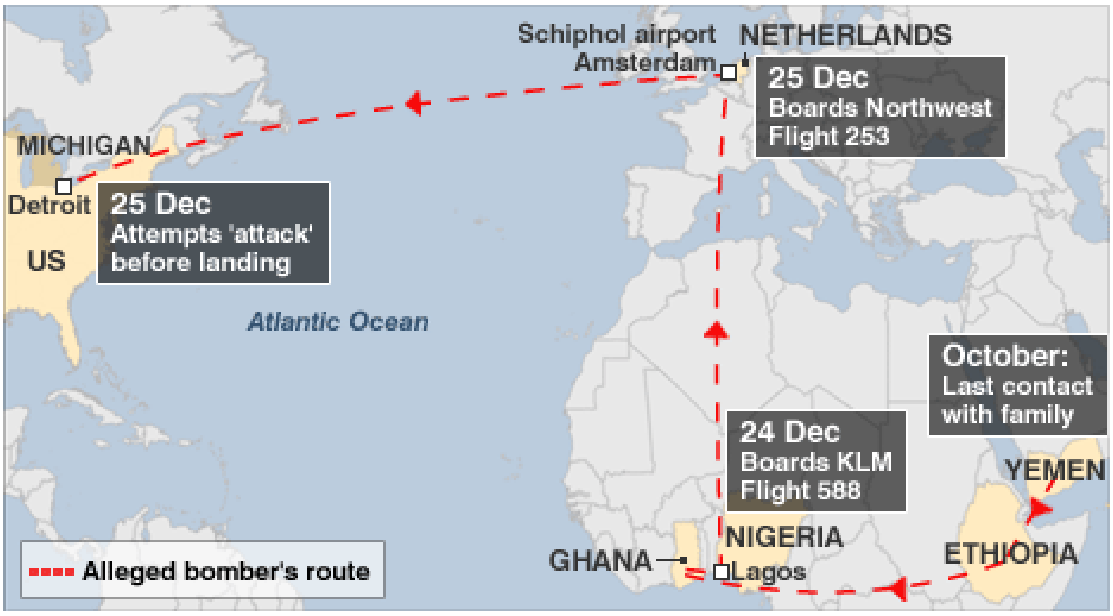
The multiple-attacks against the US that took place in September 2001 changed the face of security management to a degree that had never been experienced before. Over and above the classical three-fold process of traditional security management, namely the use of risk assessment to identify potential threats; the development of security protocols to prevent those risks from occurring, or to minimise their impact in the event that they did occur; and the development of an on-going management programme to integrate those protocols into the normal running of the company or operation - there was now the need to plan for 'unthinkable' attacks, one-offs that did not correspond to any previous patterns and which therefore could not be predicted in any meaningful way.

In the US military, this evolution in strategic thinking was introduced through a paradigm-changing Revolution in Military Affairs (RMA), predicated upon the simple fact that future conflicts would be fast-developing, unpredictable and difficult to plan for. RMA in its simplest form called for a organisational change from focusing on the 'threat' (which was unknowable and out of our control), to focusing on 'capability' (which was manageable and responsive to our own guidance).

In the commercial world, despite the fact that the nature of security management has changed so drastically, the basic perspective of security managers has not evolved to a comparative degree. This can be seen in the fact that policy makers are still focused on the idea of stopping a specific threat (and even more so, a specific style of attack, determined by the headlines describing the latest high-profile attempt at terrorism. The announcement that in future toilets will be closed on planes one hour before landing, and passengers will not be allowed to have blankets on their laps is unlikely to strike fear into the hearts of terrorist organisations.), when in fact they should be more concerned about 'creating safety'.

A stark example of how concentrating on one specific aspect of terrorism does not necessarily increase the general level of public safety is demonstrated by the fact that in October 2006, when the UK was at its highest security level in its 'War on Terror', and therefore concentrating on 'Islamic terrorism', a Russian assassin was able to fly to the UK from Hamburg, land at Heathrow Airport, clear customs and then walk around London, the whole time leaving a trail of radiation from the Polonium-210 nuclear material that he was going to use to poison Russian dissident Alexander Litvenko. This was the first ever documented case of nuclear terrorism, and it had calmly moved undetected through the entire security system of some of the world's busiest airports [3].

The facts as we know them at the moment concerning the Christmas attack are that a Nigerian passport holder, Umar Farouk Abdulmutallab, boarded a plane in Ghana, changed planes in Lagos, Nigeria, and then changed planes again in Amsterdam, where he went through normal security procedures at Schipol Airport before being allowed to board a Delta plane for the US. Sometime just before the plane went into its landing procedures, he went to the toilet, where he stayed sometime, and then when he returned to his seat he attempted to detonate an explosive device that he had brought aboard the plane inside his clothes, before being subdued by passengers and crew.



It later turned out that there were a number of significant factors that would have been expected to have flagged him as a high-risk potential 'person of interest', both in background reports and in his actual behaviour in preparing for the flight.

His father had approached both the Nigerian security forces and the US Embassy in Lagos to inform them of his suspicions concerning his son's radicalization during his stay in Yemen, a centre of global jihadism, (and as a senior member of Nigeria's banking community, and one of the richest individuals in the country, it could be expected that he would be given a more respectful hearing than an ordinary person coming in off the streets). Abdulmutallab had also been previously refused a visa to return to the UK (though this was because the college that he had listed as his academic institution was not recognised as such for the purposes of gaining a UK visa, though having been refused a visa he would then have automatically been added to the data-base of 'persons of interest'). Perhaps most damning of all, his own personal behaviour, which is always recognised as being the most trustworthy of indications of potential terrorist activity, was both highly significant and totally overlooked. The fact that he bought his ticket in cash, and then turned up to the airport for a two week stay away with only one piece of hand luggage, should have been enough for someone in the system to look up, pay attention, and decide 'This is not normal, its probably worth having a quick chat with him'.

The first two public reactions from senior policy makers following the incident were both entirely predictable, but also worryingly wrong.

The first announcement from a senior US official concerning what was clearly a major breakdown in airport security management was from Janet Napolitano, US Director of Homeland Security, who is personally responsible for ensuring the safety of the US homeland and US citizens from terrorist attack. Her immediate response was that 'Our security protocols worked effectively', though that assessment was soon retracted and she admitted (as did her boss, President Obama), that there had been major breakdowns in the system that had allowed someone to get through all of the various layers of security checks, until he succeeded in getting to a position where he could actually deliver a fatal attack.

The second response was that the reason that Abdulmutallab had got through the security system was because there was not enough technology in place, and that if they had had whole-body scanners (that are currently not used as they show the human body under the clothes, and are therefore perceived of as being intrusive), as well as explosive 'sniffers' that could have identified the PETN explosive material that he was carrying, then the incident would never have occurred.

Technology - A False Messiah

It is said of military dogma that it can basically be boiled down to one simple concept: 'If you haven't achieved your aims using mindless aggression - then you obviously haven't used enough'. Much the same can be said for technology. It seems hard to believe that given all of the technological capability that we have at our disposal at the beginning of the 21st century, together with the massive private and governmental financial and manpower resources that have been thrown at the issue of airport security in the last ten years, that if we only had one more machine - iris identification programme, 3-D x-ray spectrometers, biometric ID cards - then our problems would be solved. Whilst it is certainly true that technology has a part to play in creating an effective anti-terrorist security management strategy, it is also true that the role that technology plays is actually quite limited, and in fact an over-reliance on technology, as well as a belief in its superiority to actual human interaction, in itself creates weakness and vulnerabilities within our systems that are both easily identifiable by the potential attacker, as well as being easy to manipulate to their advantage.

The leading magazine in this field, Aviation Security International Magazine (www.asi-mag.com) carried a major article on this subject in its December 2009 issue [(4)], looking specifically at the role that new generation technology could play in identifying liquids and other similar potentially suspect materials. The unanimous assessment by all the authorities quoted, including one ex-head of security for the British Airports Authority, was that technology by itself would have only limited impact on increasing passenger safety, unless it was seen as one component to be integrated into a larger security management programme. **Remember, technology offers tools, not answers.**

The other aspect of cutting-edge technology that needs to be considered is that it often comes up against popular or moral objections. The Aircraft Passenger Whole-Body Imaging Limitations Act of 2009 was passed in the US House of Representatives on June 4th 2009 [(5)], limiting the use of such equipment to a secondary role only (when other methods had highlighted the possibility of suspect materials being carried by a particular person), and even then that person would need to be given the option of a physical pat-down in place of the full-body imaging process. As the Representative who proposed the bill so memorably put it, 'Nobody needs to see my wife and kids naked to secure an airplane' [(6).]

'Intelligence-Led' Security

Intelligence-led security is another buzz-word that is popular with specialist police directorates as well as government security spokesmen. In its simplest terms, it gives the security services the opportunity to use intelligence in order to be pro-active in disrupting potential security risks, rather than waiting to respond to attacks that have already happened. It has been used in the UK to justify the arrest of (Muslim) Manchester United fans who were suspected of wanting to blow up Old Trafford [7], the 'Plane Bomb plot' that was said to have been initiated in Pakistan, (and which similarly to Abdulmutallab's plan was alleged to have also involved the use of peroxide-based components that would have been recombined using syringes and Tang drinks), and which led to the introduction of the ban on carrying liquids onto planes that is still in place today [8], and the arrest of twelve Pakistani students in what the Prime Minister Gordon Brown called 'a major terrorist plot' [9], though all the suspects were later released without charge.

It is intelligence-led security that has been the rallying cry for supporters of measures such as the national database, the biometric ID cards and the gathering of information through a myriad of means on as many people as possible. The problem with this is that there has been a simple and yet profound misunderstanding concerning the difference between 'information' and 'intelligence'. It is certainly easy, in the present day and age, to gather a massive amount of information on a massive amount of people. However, that cannot be considered to be 'intelligence' until each piece of information has been classified, assessed, and put into a wider context. The mere fact that one can gather information on most of the population has no significance in preventing terrorism unless there is a method for identifying from the tens of millions of facts on file, which ones are actually significant.

In fact, the gathering of so much information can in itself (as in this case) actively lessen the likelihood of successfully identifying which one piece of information is of potential value.

This is a lesson that has not been learnt since 2001. The official Congressional Report on the intelligence failures that led to 9/11 clearly identified the fact that there was so much unassessed information in the system, that there was no way of knowing what was significant and what was not [10]. Similarly, for the FBI to claim that there are currently 500,000 people on their 'terrorist watch' list, and therefore they were not able to identify Abdulmutallab as someone of being beyond normal interest, is clearly a systemic breakdown that demonstrates that its attempts to gather more information on more people in order to try and make itself more effective has actually increased the likelihood of an intelligence failure.

The other known systemic weakness identified post-9/11, and one which is clearly a factor in this case, was the lack of coordination between various intelligence agencies, and even between various divisions of the individual agencies themselves.

These problems are still unresolved. A recent (September 2009) Congressional Report on intelligence issues made it clear that 'In the wake of the September 2001 attacks, the FBI was strongly criticized for failing to focus on the terrorist threat, for failing to collect and strategically analyze intelligence, and for failing to share intelligence with other intelligence agencies (as well as among various FBI components).....Congress has expressed concern about the overall effectiveness of these reforms [introduced post 9/11] and with the FBI's widely criticized information technology acquisition efforts' (11).

Photo courtesy of BBC

Profiling

Although profiling has also become a favourite word in the lexicon of security policy-makers, it is another basic concept that is often fundamentally misunderstood, and therefore misused, in terms of both its operation and its purpose. As with any other aspect of the over-all security management programme, profiling should be seen as a dynamic component that, in conjunction with other aspects of the security framework, will allow security managers to best identify potential 'persons of interest', rather than merely offering a pre-set list of personal qualities (often based on statistically insignificant pieces of personal information such as race, religion, colour, age, etc).

For example, the fact that Abdulmutallab paid cash for his ticket should definitely have been a trigger for someone to note that his behaviour did not fit the normal profile of people making preparations for an intercontinental flight. That in itself should have been enough to have brought him out from the background of the tens of thousands of other people who had bought their tickets in the 'normal' manner, and which would have triggered a check against relevant government and security databases. However, even if the complexity of such international inter-agency cooperation was beyond present capabilities, if that information had been logged onto the ticketing system, the fact that he then turned up at the airport with no more than hand luggage should have certainly pushed him into the 'Inform the security team' bracket. This simple example demonstrates that profiling is not something that is based on pre-set plan, but is rather a tool that can be used to identify anyone whose own behaviour sets them out as different from the vast majority of people who are going through the same system and using the same services.

As I was taught over thirty years ago, on my very first day of training, **'There are only two possibilities: Either someone is behaving naturally, or they are trying to pretend to behave naturally - and our success depends on our ability to spot the difference'.**

How it should be done....

There is undoubtedly one organisation that has proven over many years (decades) that it is in fact possible to create safety in a public-access mass-transit environment, and that is El Al, the Israeli national airline. El Al was targeted for the first ever political hijacking, which took place on an El Al flight from Rome to Tel Aviv in July 1968, a year after the end of the 6-Day War, and was the first attempt by the Palestinian Liberation Organisation (PLO) to use political terrorism, and hijacking in particular, to project their cause across the world's media. Following that attack (which involved a hostage situation lasting five weeks), and a further successful hijack in October the same year, the terrorists were then limited to attacking El Al planes on the run-way, which they did in 1969 and 1970, and attacking Lod Airport in Tel Aviv, during which 26 bystanders were killed. Since that time, Israeli political and security leaders made one simple promise: 'This will not happen again'. And the proof of the effectiveness of their strategies and protocols has been that in the more than forty years since the Lod airport attack, not only has there not been a successful attack on an El Al plane, (during periods when the PLO was both the most active and most successful terrorist organisation in the world), but that, as far as we know, no attempt has even come close to making a successful attack.

There is no 'magic pill' that the Israeli's have developed, and there is nothing hidden or secret about their methods. Their security strategy is extremely simple, costs almost no money to develop, and can be introduced within hours of someone understanding the underlying concepts. The skill comes not in the introduction of these security protocols, but in the sustained determination to maintain standards of absolute excellence in all aspects of the application of these rules throughout the organisation, at every level and by every person.

One of the main difference between El Al security activity and the majority of security protocols that have been put in place in airports around the world is that rather than institutionalising 'security by disruption' that is focused around a specific event - the security search - El Al integrates security into every aspect of its operations, from first contact through to the moment when that person leaves El Al territory at the end of their journey.

The following Best Practice Indicators (BPI), against which all security managers can measure their own operational effectiveness, will be readily understandable to anyone involved in security management, and it is hoped that their effectiveness coupled with their simplicity will strike a chord of recognition, and will perhaps inspire those reading this report to review their own security practices with a view to implementing some of the lessons learned.

The Foundation of Security is the Study of Human Behaviour

As has been noted above, although there is a place for technology in security management, the most effective and sophisticated security resource still remains the human eye-ball attached to the human brain. The purpose of all security, whatever its field, is to search for the anomalous, that which doesn't fit, the tiny clue, however insignificant, that would set off some trigger in an experienced security operator and make them think 'That's not right'. Once that awareness has been triggered, it will then be possible to raise the level of interest in that particular person, from out of the tens of thousands of people who might be around them, so they can be then treated with a higher level of circumspection.

The problem in normal security operations is that there is also almost no effective interaction between the airline personnel and the passenger, and that which does take place is so formulaic that is has almost no significance from a security point of view. The person asking the security questions is bored and looking at their booking screens, and the passenger can give one word answers that they have given every other time that they have flown.

When the passenger does go to the actual security process - walking through a metal detector and then possibly having a pat-down if an alarm has been triggered, all of the attention of the security personnel standing around is focused on the security machinery, and not on the people passing through it.

In the El Al model, anyone entering the airport has to go through a number of checks even before they get into the terminal, all of which are low-key and non-intrusive, but which do give the trained security people an opportunity to spot 'non-normative behaviour' at the earliest possible stage. The fact that this process is repeated at every stage of their progress puts added pressure on anyone who is feeling insecure, whether it is because they have not paid their road tax, are going for an illicit meeting, are carrying pornography in their bag or any of the other hundred and one reasons that make most of us nervous (and tell lies) when stopped by a policeman.

The purpose of the security technology is to create non-normal behaviour in the bad guy, which will then be picked up by the personnel within that area, who can then pass that information on to the security team. The important stage in identifying the person carrying an illicit substance is not the moment they pass through the metal detector, but rather the period during their approach to the security area where their behaviour will almost certainly be in some ways different from that of the other people around them.

Principle 1: Total Control of your Territory

Once you have decided what is the extent of the territory that you wish to take responsibility for (and in Ben Gurion airport in Tel Aviv that starts over 2 kms from the actual terminal), then the first principle of security management is that within that territory there is no un-owned space that an outsider can simply wander through. In most organisations there are areas which are unclaimed, such as back stairways, areas behind the kitchens, car parks, or any other similar 'lost space'. Effective security management will ensure that that cannot be allowed to happen. Wherever it might be within your organisational territory, if someone unknown is there then a member of the staff should feel comfortable about looking up, approaching and saying 'Can I help you?'. In this way, they are showing ownership and authority, and it is at that moment that basic responses within the potential transgressor are likely to be triggered, alerting the 'owner' of the territory that something is not quite right (12).

Principle 2: Everyone is Responsible for Security

The simple fact of security management is that we will not have sufficient security resources to cover every area of our territory. Therefore, it is not the core role of the security people to spot the potential transgressor. The likelihood is that who ever does spot the tell-tale sign will be relatively low in the food-chain - cleaners, kitchen workers, road sweepers, car park attendants. The objective of the security management programme is to ensure that those people understand the importance of their role in the security programme, and are completely comfortable about passing that information on to the specialist security teams.

Principle 3: Maintaining Standards - Today, Tomorrow, For Ever

Every security manager knows that the vulnerabilities within their own systems are not caused by a lack of security reviews and guidelines, and that therefore the introduction of another review is not going to change things. The problems in security management stem from the inability to maintain a required standard of individual professional and personal responsibility on a long-term, sustained basis. It is in this area that most security management programmes fail.

Within El Al, every single person has a security consciousness that is constantly monitoring their area. This does not lead to paranoia, aggression or a breakdown in effective customer relations (one only has to look at the large number of Arab passengers, families and friends wandering freely around Ben Gurion airport). There is also the understanding that getting worried about something that is not a risk will only decrease the likelihood of identifying that which could be a risk.

However, at the root of their security awareness is an underlying commitment: each person takes personal responsibility for ensuring that **any** non-normative behaviour, or any behaviour that could indicate a possible attack, will not pass unnoticed within their own territory. In this way, the possibility of any non-normative behaviour being unseen, ignored or not recognised is reduced to almost zero.

Conclusions

We have repeatedly seen that the threats we are facing are not from some super-powered international criminal conspiracy, but from ordinary people acting with extremely low-levels of infrastructure, technology and sophistication, as was demonstrated in the series of terrorist attacks in London, in the case of the Shoe Bomber Richard Reid (13) or even the racist Brixton Bomber David Copeland (14). Whilst it is natural for governments and security agencies to want to put their faith (and budgets) into cutting-edge technology, even if new-generation technology is introduced then the terrorist will simply find another way to deliver their attacks. What will not change will be their intention, and their human behaviour.

There is no magic pill that will create safety and security in our public places. However, effective security management can be just that - effective. The methodologies outlined above have a proven history of creating safe, welcoming spaces without disrupting the normal flow of people and events. Treating everyone as a suspect does not create security, and can actively reduce the likelihood of us spotting the potential attacker out of the tens of thousands of people moving through our territory.

The final word should go to the underlying principle that was at the heart of every briefing that we held over thirty years ago, and which is still relevant today:

'There is nothing that we can do to affect the motivation of the terrorists, but what we can control is the opportunity. If an attack is made, it is because something within our system allowed it to happen'.

Notes

(1). **'Vigilance key to tackling terrorist threat - PM'**
http://www.number10.gov.uk/Page21950
1st January, 2010

(2) **The 9-11 Commission Report:**

Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition

http://www.gpoaccess.gov/911/Index.html

(3) **Litvinenko Plutonium-210 Incident**
http://en.wikipedia.org/wiki/Alexander_Litvinenko_poisoning

(4) **Searching for the X-factor: Screening Liquids, Aerosols and Gels (Richard Corfield)**
Aviation Security International Magazine, December 2009
http://www.asi-mag.com

(5) The Aircraft Passenger Whole-Body Imaging Limitations Act of 2009 (HR 2027)
Library of Congress
http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.2027.IH:

(6) Congressman Jason Chaffetz
http://chaffetz.house.gov/services/

(7) **Old Trafford Plot**
Over 400 policemen were used in an operation to arrest 8 people in the Manchester area (including a woman and a 16 year old youth), based on intelligence that they were planning to make an attack on Old Trafford, Manchester United football stadium. They were later released without charge. It was widely reported that this was an example of 'policing through disruption', a tactic involving arresting people whom it was known had no connection with terrorism in order to create confusion and disruption for other terrorist-related groups operating within the Moslem community.
http://www.guardian.co.uk/news/2004/may/02/uknews

(8) **UK Terror Plane Bombs Plot**
http://en.wikipedia.org/wiki/2006_transatlantic_aircraft_plot

The UK government claimed that it had infiltrated a Pakistan-UK plot to blow up ten planes in a simultaneous terrorist attack. The arrests were made on the report that the operation was ready to go live, though later reports seemed to imply that actually the operation was only in its early planning stage (if that), and that there was no actual threat to any planes at that time. This was also justified by government spokesmen under the guise of 'disruption', though alternative reports have strongly suggested that the arrests were made for domestic political purposes.

For an alternative view to the official versions, see

http://www.craigmurray.org.uk/archives/2006/08/the_uk_terror_p.html
('The UK Terror plot: What's really going on?')

(9) **April 2009 UK terror plot**
http://www.guardian.co.uk/uk/2009/apr/10/student-visa-terror-arrests-link

PM Gordon Brown claimed that police had foiled a 'very big terrorist plot', and intelligence sources briefed that there was an 'imminent and large-scale plot', though all twelve suspects (11 Pakistanis and one British citizen) were subsequently released without charge. This incident was given even further coverage when the senior police official responsible for counter-terrorism was photographed going into No 10 Downing Street carrying papers which clearly identified details of the police operation, leading to his resignation.

(10) **Intelligence Issues for Congress** (page 18)
September, 2009
Richard A Best Jr
Congressional Research Service
http://www.fas.org/sgp/crs/intel/RL33539.pdf

(11) In the Presidential Daily Briefings (PDB's) given to the President every morning by the CIA Director, Bin Laden was mentioned over forty times between January 29th and September 10th 2001 and was clearly identified as having both the intention and capability to deliver a large-scale mass-casualty attack against the US sometime in late 2001 (The 9-11 Congressional Report Chapter 8: 'The system was blinking red')

(12) 'Territorial Imperative' is one of the great under-developed areas of security management theory, and yet potentially is one of our most powerful tools in understanding how to create a welcoming yet secure environment. The bible of this subject is ‘The Territorial Imperative: A Personal Inquiry into the Animal Origins of Property and Nations’ (Kodansha Globe) (Paperback) by Robert Ardrey.

(13) **Richard Reid** ('The Shoe Bomber) hid components of an explosive device in his shoe and attempted to detonate the device in mid-air. The device failed to explode, and he was restrained by passengers and cabin crew.

(14) **David Copeland** exploded three bombs in London in 1999, the first in a street market in Brixton, considered a centre of the black community, the second in Brick Lane, home to a large Moslem Community, and the third at The Admiral Duncan, a popular gay pub in the centre of London’s night-life district.

For more articles by David Rubens – Meido Consultants please visit
www.meidoconsultants.com