

**DAVID RUBENS ASSOCIATES**

Reports and Articles

July 2010



DAVID RUBENS  
ASSOCIATES



## **David Rubens Associates**

**David Rubens Associates** is a specialist corporate security consultancy offering strategic security services to individuals and organisations across the world.

**DRA** has worked with government agencies, NGO's, international conglomerates and major global events, and brings a mixture of strategic vision, operational experience and academic research to all of its projects, however large or small.

**David Rubens**, DRA's founding director, holds an MSc in Security and Risk Management from Scarman Centre, Leicester University, is a Visiting Lecturer and Dissertation Supervisor on their Global Security and Policing MSc programme, and is currently a Visiting Fellow at the Security and Resilience Department, Cranfield University at the UK Defence Academy, specialising in Terrorism & Public Policy and Strategic Management & Leadership.

**These articles were originally issued** as regular monthly articles that are distributed to DRA's clients. They are designed to give readers an understanding of some of the security issues of the day in greater depth than can be gathered from normal media sources, but without going into the minutiae of academic research.

Comments and feedback are welcomed, and I will be happy to supply references for any of the assertions made, if required.

Please contact [post@davidrubens-associates.com](mailto:post@davidrubens-associates.com) if you would like to be added to the monthly mailing list.

For further copies of this report,  
or to discuss the contents,  
please contact  
David Rubens  
[david@davidrubens-associates.com](mailto:david@davidrubens-associates.com)

## **Contents**

<b>'War on Terror': What It Means For The Security Officer</b>	<b>March 2006</b>
<b>Information Gathering: The Key to Global Security?</b>	<b>January 2007</b>
<b>Profiling: A Good Tool Wrongly Used (Part 1)</b>	<b>March 2007</b>
<b>Profiling and Security (Part 2)</b>	<b>April 2007</b>
<b>Global War on Terror (Part 1): Al-Qaeda – Still A Threat?</b>	<b>September 2007</b>
<b>Global War on Terror (Part 2): The New Game Plan</b>	<b>October 2007</b>
<b>Effective Security – More Complex Than It Seems...</b>	<b>February 2008</b>
<b>Terrorism – Does It Work?</b>	<b>March 2008</b>
<b>It could be you...Countering Islamic Radicalisation</b>	<b>September 2008</b>
<b>National Security – The Israeli Way</b>	<b>March 2009</b>
<b>Umar Farouk Abdulmutallab: Why Can't We Learn.....?</b>	<b>January 2010</b>
<b>'Lions and Donkeys... ' – Still Getting It Wrong</b>	<b>July 2010</b>

## 'War on Terror' : What It Means For The Security Officer

March 2006

(This month's column looks at some 'models of security response' as they can be seen in the aftermath to 9/11. I realize that for many people these are very emotive issues, and my article is intended to raise awareness of some of the principles involved in choosing one set of tools over another in developing effective security responses, and is in no way intended to be a criticism of any of the models mentioned).

For many of you reading this, especially those of you involved in various 'sand pit' operations, the fall-out from the US declaration of a 'War on Terror' following 9/11 is the backdrop to your daily activities. There is no question that the decision to declare a 'War on Terror' has affected almost every aspect of our lives, including individual freedoms, the right to move money from our own accounts, the right to move freely from country to country, or even the right to fly on planes, yet it is in the area of 'security' that these assumptions are most stark.

In this article, I would like to look at some of the underlying assumptions involved in declaring a War on Terror, and how those assumptions affect us in all aspects of our role as security experts tasked, in whatever situation, with creating a 'secure' space in our society.

The first thing to realise is that the declaration of a war on terror was not an inevitable consequence of the 9/11 attacks, and that there were other equally if not more valid response options available. In London, for example, following the attacks on public underground facilities last July, the immediate reaction of all of the authorities was to treat the incidents as crime scenes. Police experts treated the situations as they would any other criminal case - they gathered evidence, took statements, looked for clues. They built a picture of the people that they were looking for, identified them, found them and then arrested them. They then built a case based on police work, and are now awaiting to bring those cases before a judge where, if found guilty, they will be sentenced to long periods of imprisonment.

This of course, is completely different to the American experience following 9/11, and I would like to look at the implications of those differences.

The first thing that is set when the decision to couch the response in terms of war, is that it will be generals who then take the decisions rather than policemen. This automatically puts one set of tools - police work, evidence gathering, judicial response as understood within normal political and social frameworks - back in the cupboard, and brings another set of tools onto the table. By definition, military responses do not deal with solving cases, but rather with defeating enemies. The tools to do that are invasion of territories, control of airspace, use of special forces, acceptance of 'collateral damage' (ie innocent civilian deaths), etc.

It is generally accepted that in order to have a 'good' war, two things need to be set out clearly from the start. Firstly, there needs to be a clearly defined 'enemy', and secondly, there needs to be a clearly-defined 'win position', whereby both sides will then know who has won and who has lost. It is generally accepted amongst historians that the last war to fulfil these two criteria was the second world war, which finished in 1945! Since then, rather than being 'won', wars are 'resolved', where both sides come to a negotiated settlement.

However, since 9/11, it is clear that one of the underlying weaknesses in the main responses to those attacks is that there has never been a clear definition of who the enemy is. This is not just a problem of political rhetoric, but has direct implications for everyone involved in developing and delivering an integrated security response to the threats that that war has created.

Security, in all its many forms, could be said to have two basic functions. Firstly, to deter potential attacks, whether shoplifting, kidnapping, burglary or suicide bombers, gas attacks or ICBM's. However, equally important in our role of security providers is to create a feeling in the minds of the people that we are protecting that they are living in (relative) safety. In London, as one example, there is a real feeling that having armed police walking round the streets, or being stopped for security checks as we come out of tube stations or enter shopping centers, creates as much a feeling of fear as it does of safety.

If we look at the basic ways that military response options differs from the police response options, then a number of identifiable patterns emerge. Military responses tend to be carried out away from the prying eyes of publicity; they develop a chain of command that rejects the idea of civilian oversight; they tend to demonise the enemy, and deny any possibility of dialogue; they tend to demand public and political support, and to term opposition to the military response in language of betrayal, or even treason. Police response to terrorist attacks, on the other hand, work within normative social and civilian controls - they tend to be carried out within the public eye; there is a clear operational and political oversight of response operations; they are targeted against specific criminals, rather than communities; they are limited in terms of what they are intended to achieve; there is a clear 'closure point' (ie. once an arrest has been made, though this will obviously lead into the next stage of criminal trial, sentencing and imprisonment). Perhaps most important of all, the difference between the military response option and the police response option is that the former almost demands that basic concepts that are central to our 'democratic' societies - judicial oversight, right to freedom from arbitrary arrest, right to freedom from torture, right of freedom of association - are seen to be not only unnecessary, but are in themselves a barrier to creating safety within our societies.

This is all very interesting, you might say, but how does that affect me as a private security officer. As a security officer of whatever sort, you will have, somewhere in your role, the concept of authority. This concept of authority can itself be seen as having two forms, in that

in can be either 'oppressive' or 'enabling'. Do you see yourself as working within a community, creating safety and security to everyone who moves within that community, or do you see your role as being oppressive, imposing rules and regulations on 'others'? Merely by choosing one self-image over another, you can create a situation where you are limiting yourself to the range of tools that you are likely to be using. Much has been made of the difference between the US military attitudes in Iraq and that of UK forces. US forces tend to be seen as being 'harder', in that they use armoured vehicles, full personal protection equipment, and often act as though they are in the middle of enemy territory at all times.

UK forces, on the other hand, are often characterised as using 'soft' techniques - foot patrols, berets rather than combat gear, often with a football to kick around with local kids. It is clear from these signs that the way they define their jobs are in themselves very different, and it is therefore no surprise that this has an immediate effect on the way that they interact with the people that they are, in the end, tasked with protecting.

Perhaps the central question at the heart of these choices remains 'Yes, but does it work?'. I will leave that to you to decide.

---

## Information Gathering: The Key to Global Security?

January 2007

For any student of international political and security activities, one of the most interesting debates over the last few years has concerned the claims by various governments (though mainly those of US and UK) that at the heart of their ability to create a winning strategy in the Global War on Terror is their right to gather ever more detailed information on every individual that they can.

Whilst it is true that at the heart of any security operation is the art and science of information gathering, modern technology has changed the nature and the role of information gathering due to the massive growth in the ability of various authorities to track us, and then record that data in increasingly centralized holding-banks. As with so much of modern technology the question has become one of 'Do we have the ability to do something?', rather than 'What benefit do we gain by doing so, even if we have the capability?'.

The amount of information that we give out about ourselves is so all-pervading that it many senses we have become completely unaware of it.. Every time you use a mobile phone or credit card, every time you log onto the internet or send an e-mail, every time you pay a bill or register with a utility company, that information is logged, recorded and then fitted into an ever-growing matrix of inter-connected data banks.

What I would like to do over this and next month's column is to look at how we, as security personnel, should be looking at this new information gathering capability, and whether in fact it is an effective tool in the war on terrorism.

### Information Gathering

Both the US and UK governments have made a clear claim that the ability to gather and store information about people, whether their own citizens or not, is at the heart of a successful Global War on Terror (GWOT). They are prepared to declare that the need to gather and store this data overrides almost every other civil and legal right that has been developed in the western world over the last thousand years (even before the introduction of the Magna Carta in England in 1215). In matters of computer privacy and the buying of airline tickets (even to flights not landing in US territory), US authorities have been prepared to say that those countries that are not prepared to give up such information on their own citizens are looking at being excluded from the ability to have trading relationships with the US. You may be interested to know that in order to board a plane that will land in the US, the number of different information boxes that you will be required to fill currently stands at thirty-six, though the US Department of State has reserved the right to increase that at their own discretion, without having to enter into negotiations with partner countries.

(The speed with which the desire to use this technology spreads can be seen by the fact that officials at the US Centers for Disease Control and Prevention have proposed new federal regulations that will require all passengers to supply additional items of information over and above that required by US flight regulations. This will then be used to electronically track more than 600 million U.S. airline passengers a year travelling on more than 7 million flights through 67 hub airports).

The obvious question, therefore, would seem to be whether this global gathering of information actually make us safer.

For any student of basic system management, one fact stands out above all others in this debate, and that concerns the difference between 'information' and 'intelligence'. Information does not turn into intelligence until it is assessed and given context. Information without assessment and context are just facts, and facts alone do not make us safe. In fact, what is increasingly clear is that information gathering, rather than intelligence gathering, may actually be putting us in more danger, because the relatively rare nuggets of real intelligence that may be the signifiers of serious potential attack are lost in the tens of thousands of non-relevant information nuggets that have also been gathered. As the official Congressional Report into 9/11 stated, the problem was not that there was so little information on Al Qaeda and its activities, but rather that 'the possibility of a suicide hijacking would have been just one more speculative theory amongst many, hard to spot since the volumes of warning about al Qaeda threats and other terrorist threats was in the tens of thousands, probably hundreds of thousands'. (1).

More recently, and in an atmosphere of heightened security awareness, it was still possible for the head of MI6 to categorically state to a meeting of MP's the day before the London bombings took place on 7th July 2006 (which killed 52 people in four separate but coordinated attacks on public transport) that there was no imminent threat of a terrorist attack in the UK, despite the fact that all of the London bombers were known to the intelligence services, and had in some cases been actively tracked by them.

It has also been recently reported (2) that UK security services are gathering information on every British Muslim who travels to Mecca for the Haj. Given that this is over 100,000 people each year, and the justification for this given by the intelligence authorities is that two of the London bombers had visited Mecca, it is questionable how much usable intelligence can be trawled from the life facts of one hundred thousand people. Intelligence authorities in the UK have already publicly stated that they do not have the resources or capabilities to track the two hundred potential terrorist plots that they are already aware of, so how this additional information will be integrated, assessed and utilised is hard to know.

There are a number of basic problems with information gathering on this scale, some of which I will go into in greater depth in next month's column, but some of the main ones which stand out are as follows.

Firstly, the level of intelligence produced can only ever be as good as the information that has been gathered, and then input into the system. As anyone who has ever worked in an office knows, the main problem with the information on the system is that so much of it is wrong. Names are mis-spelt, e-mail addresses and phone numbers wrongly input, duplicate files are opened, information from one file incorrectly cross-referenced with information from another file. It is no different in the super-data systems of the government. The simple fact is that whilst they may have the most up-to-date information crunching super-computers in the world, the actual work of inputting that information is little different from offices across the world. This in itself creates two major problems. Because that information is increasingly being handled by private companies, they are under pressure to cut costs as much as possible, and therefore are increasingly likely to sub-contract the actual information in-putting process to further private companies, often in India. Thus we already have two of the major precursors of disaster inbuilt into the system, namely increasing complexity and no clear chain of responsibility.

The second in-built problem is that of basic security. With all of this so-called high level security information being passed around, often to the lowest bidder, it is clear that the potential for security violations is ever-present.

The second major problem that needs to be publicly discussed (but rarely is) is the simple fact that the technology for the holding and cross referencing of so much information does not yet exist. This is especially true when we are talking about the issue of biometric recording, that is retinas, fingerprints, face recognition, etc. Whilst it is true that it is possible to run this on small scale operations, it is not yet possible to capture and collate that information to any meaningful level on the scales that are being talked about by government departments. You only have to read the papers each morning to see how large-scale projects using developing technology are seemingly doomed to failure, and yet much of the information gathering technology that will be introduced on an almost global scale has yet to be proven to work in even local trials.

As anyone involved will tell you, the most sensitive and effective information gathering and security equipment yet invented is the human eyeball attached to the human brain. There is always a tendency to make use of new technology, whether it is appropriate or not, and once introduced that technology then tends to be used on an ever-increasing scale, whether effective or not.

The question that should always be asked, and which needs to be asked here, is the simple one of whether this will actually do the job that it has been tasked with, ie identifying potential terrorists and allowing the authorities to disrupt their operations. I will come back to that next month, but as always I welcome feedback and comments from readers.

## Profiling: A Good Tool Wrongly Used (Part 1)

March 2007

One of the buzz words for the last couple of years across the security spectrum but especially in the GWOT (Global War on Terror) has been 'Profiling'. As is so often the case, what was originally seen as a highly specialised tool that could make a specific contribution to the identification of people with a higher-than-normal likelihood of propensity to terrorist or other undesirable activities has been taken over so that it is now used in ways and situations that are completely out of keeping with its original remit.

In this article I would like to look at what Profiling is, what value it offers to the security professional, and some of the ways in which it has been abused by non-professional security policy-makers.

Profiling, in its broadest sense, means to look at large groups of population and to try and discover indicators of likely or predictable behaviour. For example, an advertising agency will profile the potential buyers of new cars and build their advertising campaign around the research that tells them that the potential buyers of small cheap cars will respond to a certain sort of advertising (young, funky parties, driving along a Californian beach waving to people), whilst potential drivers of high-range executive cars are more attracted to images of power, freedom and being away from the kids.

The science of profiling is a mathematical based model that says that whilst individual behaviour is in itself unpredictable, the actions of groups of people are more likely to fall into recognisable patterns. Thus whilst not all football hooligans are skinheads, a group of skinheads walking down a high street on a Saturday afternoon are more likely to be identified as being a potential for trouble.

Given that potential problems are infinite, and we usually have less resources than we require, within the security role profiling should allow us to be able to concentrate most of our energies on those people who are most likely to pose a potential threat to whatever it is we are safeguarding. This is done by studying general patterns of behaviour and then trying to concentrate that information in order to be able to predict similar patterns of behaviour in increasingly small groups of people.

Profiling can basically be divided in pre-incident and post-incident analyses. Pre-incident analyses gives us an indication of what sort of people are most likely to be involved in any particular activity, so that, for example, in a shopping centre the security team will spend more time monitoring the behaviour of the three skater-kids rather than the middle-aged white lady, and the immigration team at the airport will spend more time questioning a black male from Nigeria than they will a white person from South Africa.

Post-incident use of profiling takes the known facts from any incident and then tries to build a picture of the person who committed that crime. The use of profiling in this manner is probably older than most people realise. Dr Thomas Bond, the police surgeon who examined the victims of Jack the Ripper in London in the 1880's suggested that investigators look for a quiet inoffensive looking man, probably middle aged and neatly dressed.

Obviously, the more information the profiler has on a particular person, and the longer they have to study them, the more personal and specific the information they will be able to infer.

In a famous case from the 1980's, James Brussels, a New York psychiatrist, had letters that the New York Bomber had sent over a sixteen year period, as well as evidence from over thirty explosive packages that he had left across New York City over an eight-year period. He eventually suggested that the bomber would be "...a heavy man. Middle aged. Foreign Born. Roman Catholic. Single. Lives with a brother or sister....When you find him, chances are he will be wearing a double breasted suit. Buttoned". Brussels was so close in his assessment that when he was finally arrested, the arresting officers found him in a double-breasted suit that was buttoned.

So far, so good. The question now becomes, of what use can this be to the operational security manager? The typical way in which it is used will be along the pattern of 'The likelihood is that the terrorist bomber on a plane will be young, Muslim, radical, and probably wearing a beard'. The security team will then identify people who fit that profile, and concentrate their energies on that sub-section of people identified as being potentially high-risk. (This is obviously a simplification – but not by much). There are a number of problems with this system. The obvious one is that it labels a whole sub-section of society as being potentially high-risk offenders, and creates a pre-set range of interactions that are specifically aimed at that general group of people, irrespective of their own specific individual behaviour. The 'Sus [Stop-and-Search / 'Suspicious Behaviour'] Laws of the 1980's are a good example of this sort of stereotyping. The law was based on the Vagrancy act of 1824, which meant that it was illegal for a suspected person to be in a public place with intent to commit an arrestable offence, and basically gave the police the freedom to stop and search anyone they chose on the grounds that they thought that there might be a suspicion that they might commit a crime. This soon became seen as a symbol of abuse of police powers, and was widely seen as a means for the Metropolitan police to target and harass young black men. The Sus Laws were seen as a direct cause of the inner-city riots that took place across the UK in the early 1980's.

Besides the political and social implications of the above, there are two specifically operational considerations that are also important to consider. The first, which is technically the more challenging, states that the whole science /art / voodoo magic of profiling is based on probability and likelihood. 'It is likely that seven out of ten shoplifters fit this profile, and that by concentrating on these sub groups it is likely that we will cut out eighty per cent of shop-lifting attempts'. A seventy per cent success rate would be considered spectacularly good hen

trying to minimise incidents of shoplifting in city centre shopping centres – it would not be a particularly good success rate when trying to stop terrorist bombers!

The second problem is that once the potential terrorist is aware of the suspected profile that the authorities are looking for, they can simply change the sort of people that they use. The success of Israeli security forces in preventing young men from committing acts of suicide terrorism was directly linked to the previously unheard of pattern of the use of Palestinian women and youths to carry suicide bombs into Israeli cities. Radical Islamic suicide bombers have recently included white males ('Shoe Bomber' Richard Reid), black males (Ramzi Mohammed, one of the London 21/07 bombers) and white females (Muriel Degauque, a 38-year old Belgian woman who set off a suicide bomb in Iraq in November 2005).

It is clear that profiling would not have identified these people as high-likelihood suicide bombers, and they would have quite successfully walked through any security team that was looking for a specific sort of 'typical' suicide bomber.

This also means that the people who do not fit the profiling bill and are equally as likely to commit the crime will be even more successful as they are not identified as high-likelihood transgressors. In the examples I gave earlier in the article, statistics tell us that the white South African youth is as likely to be infringing visa regulations as a black African counter-part, and the white middle-aged female shopper is as likely to be apprehended as the skateboarding youths – but the attention that they are given by the respective security teams, whether shopping centre security personnel or immigration officials at the airport, are not in proportion to the reality of their likelihood of offending. Thus, the ineffective use of profiling can actually encourage the growth of offending by other, non-targeted sections of society.

Having highlighted some of the problems associated with the over-reliance on profiling, next month I will give examples of how, if used correctly, profiling can be integrated as an effective tool in helping create more effective security systems.

---

## Profiling and Security (Part 2)

April 2007

Last month I looked at some of the ideas that are involved in the security tool known as 'Profiling', and I pointed out that what was originally seen as a very sophisticated method of allowing us to identify potential high-risk transgressors (whether as in football hooliganism, shop lifting or suicide terrorist attacks), has degenerated into what is now often seen as a simplistic methods that allows us to target large sections of the community with little or no understanding of how profiling needs to be fitted into a wider range of security responses in order to be effective.

In fact, as we have seen by the growth of 'non normal' transgressors, such as non-Muslim, non-Arabic suicide bombers, the over-dependence of security teams on profiling can let other people, who are not identified as being of 'high-risk' by the profiling model, slip easily through the net.

One example of this is at a recent conference, a senior 'expert' on police use of profiling stated that as far as he knew, no suicide bomber on a plane had ever flown business class, so he did not see why business class passengers could not be fast-tracked through security as they would not be likely suspects for suicide attacks. It is slightly frightening that this is the level of understanding amongst what are supposed to be expert advisers to government policy makers!

As is always the case, the secret of effective security is to make sure that the basics are in place, rather than depending on a 'magic pill' solution that can miraculously solve all of our problems. The two basics that I would bring to the front of this discussion on the use of profiling is firstly, that all security is about the study of human behaviour, and secondly, the most effective way of using the understanding of humans behaviour is trained, motivated security professionals.

If we look at the classic example of Heathrow Airport over the last year, and especially since the alleged 'Liquid Bomb' plan that I wrote about in a previous column, we can see all of the classic mistakes that an ineffective use of profiling can achieve.

The Liquid Bomb Plot is alleged to have involved a number of people who were planning to smuggle liquids aboard a number of planes, which they would then combine in order to create an explosive device capable of bringing the plane down from out of the skies.

Leaving aside all question of whether this plot actually existed, and if so how credible the threat was, let us look at the reaction of the relevant authorities to these alleged threats, and specifically let us look at whether the security responses that they brought in to play (and which are still disrupting the lives of air travellers all over the world), have in fact made us any safer.

As anyone who has been through Heathrow airport recently knows, it is an experience that consists of hours of standing mindlessly in queues, going through interminable security checks, having to remove belts and shoes, not being allowed to take shampoo, drinking water or deodorants (if they are over 100ml) on board the plane, plus a myriad of other small and petty disturbances that seem, from the travellers perspective at least, to have no other purpose than to ensure that when you finally do get on board the plane everyone is angry, frustrated and vowing to cut back on future flying experiences whenever possible. So, what is the purpose of these security measures, and do they at least achieve their objectives?

The authorities would tell us that they have identified a potential threat – the use of liquids to blow up planes, and that they are introducing security measures that would prevent that from happening.

But what is the purpose of the terrorists? It is surely to create terror by making high-profile public attacks, and in so doing to disrupt to the greatest degree the international transport system. So what we then have is the situation of tens of thousands of people hanging around for hours in a public, open-access, non-secured area, where surely it would be easy for the terrorists to simply turn up with their backpacks and blow up the main holding area together with hundreds of travellers from all over the world. You can only imagine the impact that would have made as images of screaming people, mutilated bodies and mass panic are put on repeat loops on every media channel on the planet.

Besides that, it is still true that of the 67 million passengers that pass through Heathrow airport each year, if only 0.0001% were potential terrorist, that would still mean that 67,000 people were worthy of greater inspection. What the present programme does is to treat each passenger, irrespective of age, gender, or background as equally suspicious. The fact that international transport has been disrupted to such a degree is proof of the concept not only of asymmetrical warfare (ie using a relatively small amount of force in order to influence the actions of a much larger force), but of the 'Risk That Never Happened'. It is no longer terrorism that has an effect on our security, but the fear of terrorism – whether justified or not. So, how would profiling help in this instance? Firstly, as stated above, profiling is just one tool that must be used in conjunction with a much wider range of security measures, and which must be used by people who are highly trained in its use.

Given that it is almost impossible to 'bluff' normal behaviour when you are in a non-normative state of fear, anxiety, etc (remember how successful you were when you tried to lie to your Mum!), the purpose of the security operation is to create situations where that non-normative behaviour becomes easily identifiable, eg. if someone is acting in a nervous, agitated, stressed manner, walking around nervously, sweating, etc. The problem with the above system as used at Heathrow is that it creates exactly that behaviour in every single person who comes through. How many times have you seen a businessmen or young mother getting angry and frustrated and shouting at the security team because they have got to take their

shoes off or have to take a sleeping baby out of the buggy. The security team then ignore that behaviour – and similar behaviour that might be an indication that someone else may have terrorist activities on their mind.

One further point. What is the purpose of the body search? Is it to try and find something connected to terrorism? No, because we don't know what it is we are looking for. The purpose of that search is to put that person under extra pressure, so that by studying their behaviour we will get an effective idea of whether they have something to hide. It may well not be connected to terrorism (in fact, it is almost certainly not), but it does allow the security team to identify someone who is worth spending a bit more time over. Yet how many times have you seen a security person look up from the chat they have been having with their colleague, and then in a bored way run the metal detector over the suspect person and let them through, without once actually looking at them. Their idea is that if the metal detector doesn't beep, then there is no danger.

One final thought to allow you to sleep easily before you take your next flight. If the security at Heathrow, and at all other airports, is so effective, how was it that a Russian hitman, at the absolute peak of security scares on international airlines, was able to walk through the international airport security systems carrying highly toxic radioactive material, and then wander around London leaving a radioactive trail behind him in restaurants, hotels and bars, before finally poisoning Russian dissident Alexander Litvinenko in a Japanese restaurant. Imagine what would have happened if that had been an Islamic terrorist with a vial of Ebiola, Black Death or just your common or garden radioactive nuclear waste, and whether the security systems that we have in place would have been any more effective at stopping them than it was our Russian friends.

Have a good month – and watch out for the sushi!

---

## Global War on Terror (Part 1): Al-Qaeda – Still A Threat?

September 2007

Given that recent weeks have seen the discovery of a major Al-Qaeda-connected terrorist threat in Germany, the release of a new video from Osama Bin Laden to mark the sixth anniversary of the 9/11 attack in 2001 and an Al Qaeda-connected attack in Algeria that killed thirty coast-guard personnel, it might perhaps be worthwhile to have a look at what is the current status and capability of Al Qaeda, and how well the security authorities are doing in the ongoing 'Global War on Terror'.

This month I will look at the situation from the Al Qaeda perspective, and next month from the western security perspective.

The first thing that is absolutely evident as far as Al Qaeda and its supporters are concerned is that the US- led battle to defeat radical Islamic terrorism has not only failed to achieve its targets, but is actually in disarray and even retreat. The sight of US presidential candidates falling over themselves to distance themselves from any activity that can be construed as having been supportive of the war in Iraq, as well as the dismantling of the original Bush team that led the US into the war in Iraq will be widely seen as yet one more indication of the inherent weakness of the western democratic model as opposed to the disciplined and motivated structure that Islamic radicalism offers its adherents and supporters.

The winding down of the UK presence in Iraq and the lack of agreement over the success of the latest US 'surge', as well as the chaos and confusion associated with the timetable of the handover to Iraqi political and security authorities is being widely advertised as a victory for the radical, anti-Western forces in Iraq.

This has been coupled with the re-emergence of local and regional Islamic groups who are prepared to align themselves with both the political aims and operational tactics of Al Qaeda. This has been particularly clear in the emergence of Al Qaeda in the Islamic Maghreb, the area covering Morocco, Algeria and Tunisia, as well as to a certain extent Turkey. Developing out of previous anti-government organisations, these groups realise that by using the Al Qaeda name they are able to create a much wider interest in their activities than would otherwise have been the case. As one terrorism authority stated, they have been quoted as being a major threat to the wider western European region, despite the fact that they haven't carried out a single successful attack in the eight years of their existence.

This enlarging of the Al Qaeda community through affiliation of local organisations is an indication that even more than before, Al Qaeda is increasingly an umbrella label for a wide variety of radical Islamic anti-western groups, who often share little in terms of political, social or tactical backgrounds. However, despite the increase in rhetoric from both the radicals themselves as well as the government forces that are ranged against them, the threat in Germany proves yet again that as soon as anything larger than a small localized attack (as

was seen in London in July 2005) is attempted, then local and national security agencies are very quickly able to identify and trace all potentially connected terrorist activity. This was clearly demonstrated by the fact that as early as July, six weeks before the Germany arrests, specialist police units were able to swap the original barrels of explosive material for a mixture of much more diluted quality. As in so many cases where the authorities have declared a 'last minute' discovery of a major terrorist threat, it has actually been the case that there was actually little, if any, likelihood of a successful attack being made.

From the Al Qaeda leadership perspective, one of the worrying aspects of this emergence of local and regional anti-government organisations using the Al Qaeda name is that in many cases their own political and military agenda is not aligned with those of Al Qaeda leadership. We see this in Algeria, where the Salafist Group for Preaching and Combat (GSPC), the forerunner to the Al Qaeda in Islamic Maghreb group, is much more interested in anti-government activity rather than anti-western attacks. It has been mainly involved in attacks on military, police and government targets, and has not shown itself, in the main interested in the large scale, anti-civilian attacks that we have seen in other Al Qaeda activities. In fact, if you didn't know that it was Al Qaeda related, there is little to suggest it as being part of the larger AQ grouping.

As with any other 'brand' that allows itself to be identified with a populist expansion rather than its original highly-focussed core activity, it can soon be seen to lose its elitist cachet and to become a general catch-all for whoever wishes to gain from association with the brand name. In this sense, AQ is little different from Chanel or Louis Vuitton.

The main lesson to be learned from both the Germany plot and both London attacks, is that rather than Al Qaeda threats being planned, managed and implemented by top-level international terrorists, Al Qaeda, in Europe at least, is limited to low-level, under-funded and under-resourced threats that are characterised by the local and amateurish nature of their participants. While it is impossible to guarantee that these sorts of small local groups will never succeed in delivering a successful attack, it is false to claim that they are able to offer some sort of existential threat to the continued existence and safe operation of western society.

---

## Global War on Terror (Part 2): The New Game Plan

October 2007

Last month I offered a brief review of the present status and capability of Al Qaeda, and promised that this month I would look at the status of the response to those threats by various authorities across the world. By chance, the well-respected think-tank International Institute for Strategic Studies ([www.iiss.org](http://www.iiss.org)) has this month released its annual strategic review of global security, and a number of its findings concerning AQ and associated Islamic extremist terrorism made front page headlines. Its' main findings, in short, were that Al Qaeda has regrouped, and is now back to pre-2001 levels of capability that allows it to be able to plan and deliver large scale, high-profile international attacks on the same scale as 9.11. Some of the evidence that it used to support these claims were the German AQ cell that was planning large-scale attacks, as well as the UK groups that planned the 2005 7/7 and 21/7 attacks. As anyone who has been reading my columns over the last couple of years knows, I am not convinced of this argument, and in response have written a fairly detailed rebuttal of the IISS arguments which was circulated to our international corporate clients, in which I say that actually these attacks show how fragmented and low-level the level of AQ capability is at the moment, and the fact (as I have often made) that the Global War on Terror is a political response to an isolated (though terrible) act, rather than a security one. If anyone is interested in receiving a copy of the report, please contact me through the e-mail address at the foot of the column.

As far as the authorities' response has been changing to the threat of GWOT over the last six months, there are three points that seem to stand out. The first is the clear de-coupling of the Iraq War from the War on Terror. It is now clearly acknowledged that although the war on terrorism was used as an excuse for the invasion and control of Iraq, the main trigger for that was the desire to control Iraqi oil out-put, as even Alan Greenspan, former Chairman of the Federal Reserve Board, and therefore the most influential economist in America, has publicly stated. It has taken a long-time for what was clear to most people right from the start of anti-Iraq rhetoric, namely that the regime-change policy that was the clear US position did not have anything to do with Al Qaeda or defeating the forces of international terrorist conspiracies, to be admitted in public, but it is only now that the effect that this 'false flag' operation has had can be truly appreciated. As the Oxford Research Group ([www.oxfordresearchgroup.org.uk](http://www.oxfordresearchgroup.org.uk)) has recently stated, there is almost no aspect of the GWOT that can not be seen as aiding Al Qaeda in its ability to recruit personnel and develop grass-roots support.

The second point that has become clear is the understanding that an effective long-term response to terrorist threat can only be developed based on effective policing and intelligence gathering, rather than military-based 'war models'. I have written before about the dilemma's caused by handing responsibility for the war on terror to military commanders rather than police authorities, and it is now accepted that effective pro-active and pre-emptive anti-

terrorism programmes come about by the use of traditional law-and-order mechanisms utilised within the normal framework of domestic and international legal systems. This is a radical change from the original GWOT rhetoric which stated that the threat posed by fundamental Islamic terrorism was so great and so unprecedented that it was only by ignoring or even dismantling our own western legal and justice systems that we would regain the capability of opposing those forces in an effective and meaningful way.

And the third point that has emerged is the necessity of creating a balance between an effective, sustainable security system and the needs of the general population to live its life in as normal a way as possible. There has been a significant pendulum swing from the idea that the threat of terrorism is so severe that we must all accept the sacrifices that we must make on a personal and societal basis in order to counter-act those threats, to the realisation that in fact, the threats are of a limited and handle-able nature, and that in fact terrorism has become in many ways just another law-and-order issue to be dealt with in the same way as under-age drinking and dealing with drug dealers. It is interesting that in the recent UK national party conferences, terrorism and its effects had almost zero impact on the proceedings, whereas tax programmes and cash for the NHS was at the top of the agenda. The war on terrorism has become a nasty smell in the room that everyone is pretending to ignore in case everyone else thinks that they are responsible for it!

With the UK under a new Prime Minister and the US already into its 2008 election programme, it seems clear that for many people this is an opportunity to draw a line under the 'old' policies of GWOT, and to create a new, more realistic and sustainable set of policies that will allow old ties and alliances to be renewed, and in many ways the old world order to be restored. It may be that in a few years time the period of the last six years will come to be seen as a minor aberration, a panicked response to a unprecedented attack, and that 'normalcy' will have returned under new regimes. But, as everyone knows, at the end of all the best horror movies there is the last shot of the unhatched eggs that will set the scene for the re-emergence of the next generation of bugs, spiders, zombies and other monsters that will return to wreak vengeance. Whether the world can walk away so easily from the legacy it has left in the bombed out cities of Iraq and Afghanistan, and the refugee camps of Lebanon and Gaza, is something that only time will tell. But personally, I am not betting against the possibility of a sequel, and, as any horror-movie fan will tell you, in most cases at least the sequel is usually gorier and more bloodthirsty than the original.

---

## Effective Security – More Complex Than It Seems...

February 2008

There has been a significant change, certainly since the events of 9/11, in the way that we perceive the whole concept of 'security'. In previous, perhaps more innocent times, when the main role of security involved protection, whether of a factory, office, person or operation, the skills of the security manager were to identify potential threats, develop effective preventative security measures, and to implement and manage those measures on an on-going basis. In this way they would maximise the security of a named person or facility against an identified danger.

However, in the modern day the threats and dangers that we face are much more complex, and often almost undefinable in their exact nature and manifestation. It is clear that if we, as people responsible for ensuring the safety of our clients, principals and operations, are to be able to do so in an effective manner, our own security management capabilities must be on the same level of sophistication as the threats that we are facing. In this way, for example, we have seen a shift in strategic military thinking from the idea of 'defence' (defence strategies, defence policies, defence options, etc) to 'national security'. Whilst it is clear that defence capabilities are still a vital function of national security, and without a national defence capability no country would be able to claim that it could safeguard its own interests, on a wider scale national security also includes regional and global economic, political, social and over-all geo-political considerations. Paradoxically, the people who understand this the most are senior military strategic thinkers, who are the first to admit that in the face of today's multi-faceted, multi-level threats, military capability alone is not enough to guarantee the security of the homeland or their citizens. Unfortunately, the people who do not understand this are politicians, who have a tendency to see the world in terms of simplistically-described problems that are open to simplistically-described solutions. The problem starts when we offer simplistic solutions to complex situations such as Iraq and Afghanistan, or even the problems of using arable farmland to grow bio-fuel crops which is having major effects on the prices of other staple foods across the world – and especially in areas already suffering from deprivation.

So what can we as security managers and team leaders operating on a much more local level learn from this developments from 'defence' to 'national security'. Well, the first thing is that security is only a very small part of an operation, and 'security' alone may not be the best means of ensuring safety. A team that upsets the local population, that obviously has no considerations of local culture or acceptable behaviour, will clearly create more problems than they solve. A security force that relies purely on reactive options to attacks that are already incoming will clearly not be as effective as a security team that values the contribution of locals intelligence, and which goes out of its way to ensure that potential local intelligence sources are comfortable about approaching them. A security team that is seen as in some way contributing to the safety and stability of the local area, rather than ensuring the safety of

one person or institution by increasing the danger and threat to the surrounding population is in all likelihood going to find that it will soon be in a loop of needing increasingly high levels of security to counter higher levels of threat, which have been created in many ways purely by the direct actions of those security forces themselves.

Although there may be obvious examples of some of the situations I have mentioned above in your own work environments, they are sometimes more subtly hidden than you might think. A simple example would be an executive CP team wearing radios and earpieces in a public space, and immediately becoming highly-visible and attention-attracting. Another might be an embusing technique at an airport that is too high profile for the surrounding environment and potential threat levels. Aggressive driving is another example, as is wearing inappropriate clothing, either too smart for the principal's situation or too casual.

Even in PSD situations, the first priority must be to try and prevent situations occurring rather than reacting to events that are already underway, and the ability to fit in and be a natural part of the environment that you are operating in is as valid a rule in the corporate security world of Geneva, Bahrain or Moscow as it would be in a jungle or arctic survival exercise in Brunei or Norway.

The reason that basic principle are called basic principles is because, having been tried and tested over many years and countless operations, they usually work in whatever situation that you are operating in, and they are usually the best way of ensuring that you get through whatever needs to be done in the most effective manner, in ways that maximise your security at the same time that they minimise the likelihood of anything bad happening. The person who claims that he is going to 'beat the jungle' will not last long – and it is probably just as true in whatever security role you find yourself.

---

## Terrorism – Does it Work?

March 2008

Recent weeks have seen the re-emergence (if it ever went away) of political terrorism in both Israel and Pakistan, with high-profile attacks on politically sensitive targets in both countries.

It may well be seen, in a hundred year time, that the first period of this century will come to be known as 'The Age of Terror', and certainly 'The War on Terror' will be one of the phrases that will be remembered about this period when everything else will be forgotten.

But one of the questions that is often noticeable by its absence is the simple one of 'What is terror designed to achieve, and does it have an effect'?

The first characteristic of 'terror' is that it is one of the basic tools of 'asymmetric warfare', ie when a weak force tries to take on a powerful one. If it is true that history is written by the winners, then the definition of terrorism is often written by the powerful. One argument has it that the suicide bomber is purely the poor man's weapon delivery system, and in fact there is very little military difference between a bomb attached to a pack on someone's back and a rocket fired from a helicopter gunship. Whilst one is seen as 'legitimate' military tactics, the other is seen not only as 'illegitimate', but also immoral and in fact putting the perpetrators outside the possibility of negotiations. As President Bush's press spokesman said in January 2006, 'We don't negotiate with terrorists, we defeat them'.

The root objective of terrorism has always been to effect another government's policies, and in doing so to gain benefit for the 'terrorist' side. Whether in Algeria in the 1950's, the Sandinistas in Nicaragua in the 1980's, the IRA for thirty years against the UK government or the ETA attacks in Spain, terrorism is the ultimate confrontation between the power-poor and the power-rich.

So, does it work? On one level, the answer has to be 'no', in that if the objective of terrorism is to create terror, and therefore to prevent a country from operating in a normal manner, even in the height of the IRA attacks in England (with over forty attacks taking place in London alone in the twelve months leading up to the Bishopsgate bombing of April 1993), or the PLO attacks in Israel, with high-profile suicide bombers causing scores of death, people still went to restaurants, disco's, wedding parties and rode on the buses and trains, and in no instance (outside of America in the immediate aftermath of 9/11) could it be said that a country or population significantly altered their behaviour as a direct result of terrorist activity.

On the other hand, on a more strategic level, terrorism could be stated to have had considerable success. And that is in the sense that **the purpose of terrorism is to create a response from the target government as though they are under serious attack**. Thus, by responding to a small explosion on a bus, or in a restaurant with dis-proportionately

repressive responses, by targeting specific sectors of the population in such a way as to raise the likelihood of radicalisation amongst a significant portion of that group, by creating in the mind of the population the feeling that there is a level of danger that is in fact much greater than the reality threatened by the 'terrorist' group, then the government itself will set in motion a feed-back loop that will start from a small attack, and then continue along a path of over-aggressive response, radicalisation, increased targeting and repression, more low-level disaffection with the government and increased identification with the anti-government groups by people who other wise would not have aligned themselves with either their aims or their tactics. This in turn leads to the identification by the authorities of non-radical groups from the same local population as being of the same danger....and so from one small attack or series of attacks an almost inevitable process of alienation, polarisation and radicalisation takes place.

This leads to a success for the terrorist group that they would never have been able to achieve on their own – as many leading commentators have phrased it, the US invasion of Iraq was AQ's greatest recruiting coup, and turned what was a relatively minor group on the international terrorist scene into a global player able to influence governments across the world.

There has recently been a move away from the rhetoric of terror to one of sustainable security through effective policing and monitoring of potential threats, and there is even talk in the UK of negotiations with the Taliban in Afghanistan. If there is one thing that history teaches us, it is that today's implacable enemy may well be tomorrow's strategic ally (as has already been seen with the Taliban since the days of the Russian invasion of Afghanistan), and if even Libya's Colonel Ghadaffi can be brought back into the fold, then the possibility remains open for every other terrorist group as well.

---

## It could be you...Countering Islamic Radicalisation

September 2008

There is a widely held belief that by the time that a government comes to accept something as true, it has usually become so widely acknowledged as to have become almost self-evident, or, in more colloquial language, 'the statement of the bleedin' obvious'! Whether it is the fact that children need more exercise, that poverty is linked to poor health or that large corporations are basically in existence to rip the rest of us off, governments seem to need fancy committees to tell them what to everybody seems perfectly clear and simple.

An article in the Guardian last month publicised that MI5 has concluded that there are no easy ways to identify radical Muslims, and that rather than being members of some SMERSH-like international organisation dedicated to the overthrow of western civilisation, Islamic radicals are 'home-grown' or 'grass root' terrorists who do not carry out acts of terrorism because of some rabid jihadist belief or because they truly believe that by dying a martyr they are guaranteed seventy-two virgins in Paradise, but rather because of the effects on their lives of their own governments, whether it is through oppressive laws targeting Muslims in this country or the actions of the UK and US governments in Iraq, Afghanistan and the Palestinian Territories. Now, this may seem reasonable to most of us, but it was only a few years ago that Tony Blair was denying any possible link between those UK government policies and the radicalisation of Islamic youth in the UK.

The first credible organisation to make these claims was the Royal Institute of International Affairs (also known as Chatham House), who claimed in a 2005 report that UK participation in the war in Iraq had proven an ideal recruitment campaign for Al Qaeda, had put the UK public at risk and had increased the likelihood of Islamic terrorist attacks against UK citizens and interests. Given that this conclusion was completely unacceptable on political grounds, even if it was correct on every other ground, Tony Blair immediately responded with the claim that the attacks on London (the 7/7/2005 suicide bombings on three tubes and one bus, causing 51 deaths), was the work of fanatics who subscribed to an 'evil ideology', and that it would be a "misunderstanding of a catastrophic order" to think that if we changed our behaviour they would change theirs".

The recent MI5 report makes it clear that there is no single profile of a radicalised Muslim, and that the reasons that people who do choose a path of terrorism cannot be simplified down into an 'evil ideology'. Those who become terrorists are as likely to be university educated as to have left school with no qualifications, are as likely to be married with children as to be sexually frustrated youths seeking martyrship in order to sublimate sexual urges (which was one theory that for a time was quite popular!), and are as likely to be non-religious people who use alcohol, drugs and have a non-married sexual life as to be religious fanatics cocooned in an Islamic life-style. In fact, the MI5 report goes as far as to say that there is evidence that a well-established religious identity actually protects against violent radicalisation.

So what does this mean for us, both in the short term and long term? One of the clearest messages that this report sends out is that it is not only wrong but counter-productive to speak about a single unified form of Islamic radicalisation, and even more to consider UK Islamic community as one single unified group. There is a growing understanding that the answer to Islamic radicalisation lies within the community itself, allowing a wide-range of voices and counter-voices to be heard, and trusting that the lure of Islamic radicalisation will recede as the society in which those potential jihadi's live becomes more open, accepting and even welcoming. What certainly will not solve the problem of radicalisation is increased monitoring and disruption of the lives of the vast majority of Muslims who are not only not involved in radical Islamic ideology, but who are, according to some reports, likely to have a higher level and trust and belief in the British police force than the rest of the general population around them.

It may not be what politicians want to hear, but when even security chiefs are telling them that the answer to Islamic radicalisation is not increased police powers but rather an increase in the social freedoms and equality that our society is supposed to be based on, then perhaps it is time that they started listening.

---

## National Security – The Israeli Way

March 2009

Many people will have read with interest the announcement by the UK Home Secretary that 60,000 civilians are to be trained to be the front line in detecting and preventing terrorist activities. Whilst it has long been acknowledged that the secret to any sustained counter-terrorist programme has been grass-level support, this is the first time that such a programme has been officially recognised within the UK security environment.

It is interesting (and I think a positive step), that the people who are to be trained are working at hotels, shopping centres, leisure complexes and other similar community-based environments. Whilst the British government have made some disastrous decisions in the past about where and from whom they gain their counter-terrorist expertise (and I am thinking specifically about using Israeli-style programmes such as 'Operation Kratos' in order to police the streets of London, leading to the shooting of the innocent Brazilian student Charles de Menezes on 22<sup>nd</sup> July 2005), this is one area where the British authorities could learn a lot of positive things from the Israeli experience.

The first things that most people say on arriving in Israel, is how normal it is. Despite a constant threat of suicide bombings, rocket attacks and other forms of low-level warfare, for the vast majority of people life in Israel goes on as it does in any other western country, and there is little if any obvious security presence besides the large amount of young soldiers walking around with semi-automatic rifles slung across their backs – and it is always surprising how quickly that also becomes a normal part of the background street life. People go shopping, drop their kids at school, go to the cinema, hang around in coffee shops, and yet despite the fact that Israel is the target of most of the world's terrorist attacks, there is little if any feeling of panic or even unsafety.

As everyone will be aware, one of the fundamental laws of risk management is that there is a direct linkage between security and freedom, and that therefore the more freedom that you have the less secure you are, and if you wish to raise the level of your security then the price of that is that there will be less freedom. Although the Israeli situation seems to break this principle, in fact it adheres to it although in a slightly different way than is normally the case. Firstly, as is natural in such an environment, everyone is security aware. If you doubt this, sit in a coffee shop, walk away without taking your briefcase with you and see how long before someone draws attention to your lapse! So in fact, security is almost all pervasive, but very low-key. It is integrated into normal daily life in such a way that it is like the background hum of your fridge, completely unnoticed unless it stops. The second fundamental principle of Israeli security is that potential attacks need to be disrupted at the earliest stage, so that whether on a strategic planning level or an operational attack basis the likelihood is that someone will become aware of the potential danger before the final approach is actually

made. In this way, Israel has made itself almost bomb-proof, despite the fact that 20% of its population is made up of Arab citizens.

There have in fact been a number of programmes in the UK to develop this sort of public awareness, particularly with Project Griffin, run by the City of London police, which has worked widely with security personnel involved in all aspects of private security, including retail guards, static guards, doormen and door supervisors, sporting event stewards, etc. Given that these people have already developed a strong security awareness, it is natural that they can be considered as the people who are most likely to become aware of a potential problem, even if it is the 'non-normal' behaviour of someone on the bus or train as they go to work.

It is well accepted that the time to disrupt terrorism is well before they terrorists move into their final approach. By that time it is almost always too late, and whatever security forces you have at your disposal it will not be enough to stop major damage and disruption – as has been seen in the recent Mumbai hotel attacks and the attacks on the cricketers in Pakistan. The drafting in of 60,00 local people into the battle against terrorism will mean that the likelihood of someone becoming aware of potentially suspicious behaviour will be radically increased, which is in itself enough to either prevent or deter potential terrorists from making their first preparatory moves. As always, we never know how successful we have been when nothing in fact happens, but there is no question that this programme, if managed correctly, could have a significant impact on developing a long-term sustainable security culture that is both embedded in and is a natural part of the wider British society.

---

## Umar Farouk Abdulmutallab: Why can't we learn.....?

January 2010

### **'If you keep doing what you've done, you'll keep getting what you got'**

The Christmas day terrorist attack by Umar Farouk Abdulmutallab on a Delta plane flying from Amsterdam to Detroit brought the question of airline security, and international counter-terrorism in general, back to the front pages. The immediate response of the US and UK governments was to announce that there would be an enquiry into the security failures that allowed the attack to happen, and that there would be an immediate upgrading of security technology at airports, including the use of full-body scanners that allows the observer to see an 'as naked' image of the passenger passing through. The immediate response of a wide range of security experts was that this would be ineffective, and in many ways even counter-productive, as it would reinforce the idea that the solution to the terrorism threat would always be more technology.

My own feeling is that these knee-jerk responses (which were entirely predictable), fall into the military mind-set of 'If you haven't managed to achieve your objective through the use of blind force – then you obviously weren't using enough'. Given the massive investment of literally billions of dollars of manpower and technology into developing an effective airport security system, together with the general high level of inconvenience that has already been imposed on all air travellers so that what might be called 'security by disruption' has now become an accepted part of international travel, I find it hard to believe that the simple addition of yet an extra layer of intrusive security will suddenly make the world a safer place. What has not been asked, at least in public, is why an international security system that has been specifically designed to confront what we have been told is the greatest threat that we have ever faced, can be by-passed by a man carrying an explosive device in his underpants, who has already been identified to the US authorities as a high-possibility suspect by his own father, who has bought an intercontinental ticket with cash, and has then turned up at the airport without any luggage, and at no stage has a single person made the decision that somebody should have had a chat with him.

The initial response from the US administrator who has ultimate responsibility for security and terrorism in the US, Janet Napolitano, Director of Homeland Security, was that 'Our systems worked', though that was soon shot down by President Obama, who made it clear that not only had there been systemic breakdowns across the counter-terrorism system, but that he was holding individual department heads responsible for the fact that a terrorist plot had, to all intents and purposes, been successfully delivered.

The basic flaws that allowed this 'plot' to succeed had already been highlighted in the Congressional Report that was released after the 9/11 attacks in 2001. They were quite simply a lack of information-sharing between agencies, and an over-emphasis on data-

collecting, without the resources to assess that information in order to identify the extremely few people who actually posed a serious and credible threat. The fact that they had data on 500,000 people didn't make us safer, and in itself was a factor in allowing someone who clearly should have been identified as a 'person of interest' to walk openly through the system without being picked up.

The other factor that wasn't mentioned was that 'total body' scanning wouldn't have succeeded in identifying the explosive materials that Abdulmutallab was carrying, and that in fact there were body scanners in place in Schipol airport (where Abdulmutallab boarded the plane), but they weren't in use because of US pressure that found the idea of security people seeing 'naked bodies' intrusive and unallowable. It did however lead to what is already a leading candidate for 'Terrorism Quote of the Year', from US Congressman Jason Chaffetz, who claimed that 'Nobody needs to see my wife and kids naked to secure an airplane'.

Once again, we have been given a warning: not only does the system not work, but playing around with a bit of extra technology here, or a meaningless review there, will not make any significant difference. Unless there is a genuine understanding of what is the nature of the threat that we are facing, and what are the strategic and management tools that we need to introduce in order to develop an effective counter-terrorism capability, we will remain in the situation where the authorities are taking action that makes them look effective, without doing anything that will actually do anything to stop the next terrorist attack.

---

## **'Lions and Donkeys...' – Still Getting It Wrong**

July 2010

It was the First World War that gave us the phrase 'Lions led by donkeys' to describe the bravery of the British fighting soldier and the foolishness and incompetence of the senior staff officers who led them, though it was probably a feeling that was recognised and echoed by fighting men back into the dawn of time. A recent report in The Times suggests that the strategic planners responsible for the battle plans for British troops in Helmand Province have learned nothing from history, except perhaps the undoubted truth that politicians (and politically-influenced military leaders) should not be trusted with the lives and destinies of those that they command.

It is easy to make such criticisms retroactively, and it is an equally famous saying that hindsight is always 20-20 (ie perfect), but, in another sector, the reports that have been coming out concerning BP and its failures both to plan for a major pipe-line malfunction as well as the clear lack of capability to respond to a major situation when one did arise, indicate that even the people at the very top of two of the largest (and supposedly most professionally competent in their own fields) organisations in the UK either did not have a basic understanding of major project management, or ignored those facts for their own ends.

According to classical risk management analysis, at the most basic level there are only three reasons why things can possibly go wrong in an operation: You have either misunderstood the nature of the problem; if you have understood the nature of the problem, then you have misunderstood the nature of the required response, and if you have got those two basically correct, then you have mismanaged the response over time. A further level of analysis says that the two ways that you can misunderstand the problem are in its nature - what it is, and its scale - how big it is going to be; there are three ways that you can misunderstand the response: the required nature of the response, the scale of the response and the timing of the response (ie the correct response at the wrong time is still wrong); and lastly you can mismanage the response over time on three levels: strategic, tactical and operational. (For an example of what happens when mistakes are made in every single one of these points, one has only to look at the FEMA response to Hurricane Katrina).

## The Only Three Things That Can Go Wrong in Operation Management

### 1. You have misunderstood the nature of the problem

- i. The Nature of the problem
- ii. The Scale of the problem

### 2. You have misunderstood the nature of the response

- i. The Nature of the response
- ii. The Scale of the response
- iii. The Timing of the response

### 3. You have mis-managed the operation over time

- i. Gold Command Level
- ii. Silver Command Level
- iii. Bronze Command Level

It has become clear that the misunderstanding of both the nature of the problems in Afghanistan and the required response to those problems were so fundamental that it is being questioned even by senior military officials whether the battle plan that was finally put into operation was ever fit for purpose in the basic meaning of the phrase. It is hard now to remember that the original purpose of the Afghanistan mission was one of stabilisation and development, and that the military role was primarily to offer security cover to the civilian missions on the ground. Shortly after he announced the deployment of 3,300 troops to southern Afghanistan, then-Defence Secretary John Reid famously announced that he hoped that they would return within three years 'without firing a shot'.

A basic law of operation management states that you must always have a reserve capability that will allow you to respond to unexpected circumstances, and that 'just enough' is never enough. However, the force that had planned to be deployed (re-deployed) to Afghanistan would have been drawn from troops that were freed up by the scaling-down of the operation in Iraq, and once it became clear that the withdrawal from Iraq would be longer and more complicated than planned for, then the Afghanistan operation was always going to be significantly under-resourced.

And the third and final principle of operation management that comes into play, and one that I have repeatedly referred to in my various columns, is that complexity is a major cause of failure, and increasing complexity leads to an almost inevitability of failure. That has clearly been the case in the BP oil disaster, where even now BP is claiming that the responsibility for the maintenance of the defective oil well was not down to them, and the BP CEO, in his

evidence before a Congressional Committee, repeatedly stated 'I don't know' or 'It was not my responsibility'.

In military terms, the chain of command should mean that responsibility for any action should be clearly delineated, and yet even the command and control structure for British troops in Helmand was unclear, with the larger British force being subsumed into a smaller international force led by a Canadian brigadier, at the same time that it was expected to report directly to its London HQ.

There is a natural tendency for all operations to suffer from 'Mission Creep', when what starts out as a clear and simple operation gradually grows bigger and more unmanageable as extra bits are added on to the original programme, but when Lieutenant-General Sir Robert Fry, at the time Director of Operations, can state that the campaigns in both Iraq and Afghanistan vastly exceeded the scale for which they were planned, resourced and organised, then it becomes clear that an understanding of classical risk management is still lacking even in organisations which have been planning operations for hundreds of years.

---



DAVID RUBENS  
ASSOCIATES

**David Rubens Associates**

The Arches,  
Maygrove Road  
London NW6 2EE

[post@davidrubens-associates.com](mailto:post@davidrubens-associates.com)

[www.davidrubens-associates.com](http://www.davidrubens-associates.com)