

## SCIENCE AND THE TERRORIST CHALLENGE – OPTIONS FOR POLICY AND THEIR IMPLICATIONS.

SIR RICHARD MOTTRAM

### Introduction

Certain events have iconic status and shape perceptions of history- the impact is magnified if the event is accompanied by strong visual images. Examples include: the detonation of atomic bombs over Hiroshima and Nagasaki, the fall of the Berlin Wall, and the collapse of the Twin Towers on September 11 2001, events of worldwide significance. 9/11 put al-Queda even more clearly on the map in the way they wanted. But possibly to an extent they could not have dreamed of.

In the USA itself, the 9/11 attacks were followed one week later by five letters entering the US postal system contaminated with anthrax, followed three weeks later by two more letters addressed to Democratic Senators. In a short time, the US and its system of government had suffered two attacks- one “conventional” but using passenger aircraft as a weapon, one involving “bio terrorism”. This threat, and the wider context of concerns over states with weapons of mass destruction (WMD) and their possible links to non-state actors, has dominated security debate ever since. Almost un-imaginable sums have been expended in counter-terrorism activities, in the related war in Afghanistan, and in the much-more contentious invasion of Iraq.

Unsurprisingly, these attacks had profound impact in the US, on government and on politics. Other countries in Europe have suffered major terrorist attacks- including Spain and the United Kingdom - of devastating impact for those caught up in them and their families and friends, if not, taken as a whole, on the 9/11 scale.

Clearly, effective counter-terrorist policies and programmes are an essential part of modern government and need to engage every level from the individual to global cooperation. At the same time, like any other public policy issue, terrorism needs to be seen in context:

- As one amongst a number of national security risks and broader risks of harm.
- As a tactic with a long history which takes different forms in different places. Terrorism is not simply or mainly an anti-western phenomenon;
- While for the West the main focus currently is on “international” or “Islamist” terrorism, terrorism generically has a long history prior to 9/11, will outlast al-Queda, and, as a tactic, is not susceptible to defeat in military or other terms.

And the risk from terrorism needs to be seen in perspective and handled with proportionality in itself and in relation to other risks. For reasons I will touch on, this is, I think, a very difficult thing to do.

I want today to consider the terrorist risk in terms of its component elements; some of the implications for public policy; and how terrorism ranks alongside other risks we face as individuals, societies and states. This is a huge subject and I can only touch on some aspects of it. As will become clear, I am more comfortable with the questions that arise than the answers.

I should add that these are personal reflections and those of a non-scientist. To add a little colour, from November 2005 to November 2007 I was responsible at official level within the United Kingdom Government for the handling of civil emergencies. The problems I dealt with included a number of (alleged) terrorist incidents, and unusually large-scale flooding, both things Government would be expected to have plans for. They included a foot and mouth outbreak for which there were extensive contingency plans; but, interestingly, this outbreak was linked to a failure in bio security at either a Government laboratory or a related commercial facility. And they included the murder of Alexander Litvinenko by poisoning with polonium-210 in an attack by an individual with probable links to another state.

Inevitably experiences like these shape views about risk.

### **Why does science matter?**

Why do science and scientists matter on these issues? You may be expecting an exposition on how science and technology can be used to help counter terrorism. This is indeed very important and of significant potential value. But the contribution of science and technology is more interesting and broader than this. Science contributes potentially to the problem of terrorism as well as to helping to counter it. For example:

- There is the awkward fact that scientists, engineers, and doctors play a considerable role as terrorists. These are professions with ways of thinking which, for a very small minority of their members, seem to help point them towards terrorism.
- There is the risk that inadequately regulated scientific activity and the unconstrained dissemination of scientific knowledge may significantly enhance the terrorist threat in its most severe forms.
- And there is the risk that scientific and technological solutions, for example, exploiting developments in sensors and in biometrics, information handling and communications, could have significant impact on the character of the free society we are seeking to sustain against the efforts of terrorists to undermine it.

Conversely the contribution of science is potentially a very rich one including:

- Helping more effective intelligence gathering, the disruption of terrorist activity, and forensic support for the criminal justice process;
- Helping to neutralise, or mitigate the effects of, terrorist attacks;
- Improving the protection of infrastructure;
- The contribution of social scientists to enhancing our understanding of what drives terrorism and how therefore it can most effectively be prevented;
- And the contribution of a range of scientific disciplines, including psychology, to our understanding of how individuals and societies perceive risk and how risk might be better handled in public policy.

### **Terrorism and National Security**

The UK and a number of other countries have sought to assess the terrorist threat in the wider context of a national security strategy focused not just on traditional inter-state risks but also on challenges at the level of the individual. Thought about this way, terrorism needs to be seen, evaluated and decisions on how to counter it taken

alongside the evaluation of other risks. These might be other “hard” security issues—such as the risk of inter-state conflict. Or they might be other risks to the individual, such as from a pandemic flu outbreak or from the impact of climate change, etc.

The UK has sought to develop a more effective approach to resilience planning designed to minimise the impact of major emergencies. There are a number of steps in this process including:

- Risk identification;
- Risk assessment, ensuring that risks are routinely assessed in terms of likelihood and impact, and that assessments are thorough, balanced, and proportionate;
- These assessments can then be drawn on to inform the development of a common set of planning assumptions on the nature and scale of the consequences which might need to be addressed; leading in turn on to discussion of
- Capabilities that need to be developed.

A process of this kind is an essential planning tool in which scientists and engineers have very important parts to play.

The methodology is sound. In a different context, with examples principally drawn from financial markets, bestsellers have been written on, amongst other things, the importance of weighing both probability and outcome - the lesson being that it is the low-probability/high-gain or high-loss events that are the basis for spectacular success or catastrophic failure. In the world of trading, as Nassim Taleb has argued, the big gains come from understanding properly both the risks and the opportunities. [1] The calculus in government and politics can be different - success in terms of the untoward not happening can go unrewarded as being the expected outcome, while failures of risk management can be severely criticised, often with large helpings of hindsight.

An illustration of some of the tensions involved in thinking about probability and consequence in government might be the so-called “One Percent Doctrine” attributed to US Vice-President Cheney by the author Ron Suskind. According to Suskind, Cheney said in relation to the threat of terrorist acquisition of a nuclear weapon: “If there’s a one percent chance that Pakistani scientists are helping al-Qaeda build or develop a nuclear weapon, we have to treat it as a certainty in terms of our response. It’s not about our analysis, or finding a preponderance of evidence, it’s about our response” [2]

The quote should not perhaps be taken too literally. There is an implicit piece of analysis underpinning such an instruction for urgent action in that a possible link between a Pakistani nuclear scientist and al Qaeda represents a plausible and potentially very-dangerous threat. And the action taken as a result of the Vice-President’s intervention was proportionate, involving a high-level demarche with the Pakistani Government.

But the underlying tension remains. Low probability means just that. It does not mean something will not happen. Or, put another way, long years of experience in working in government taught me the value of the maxim: “Never say never” in relation to a

variety of internal and external events. But not all potential low-probability/ high-consequence events can be planned for or actioned, even more so in the case of a country like the UK than for the US. So some potentially uncomfortable judgements need regularly to be made.

### **Thinking about the terrorist threat**

How, against this background, has thinking developed about the terrorist threat and its component elements? In the case of the United Kingdom, a variety of potential terrorist risks have been assessed in this way for likelihood and impact. These planning-based assessments operate alongside more immediate operational concerns that include a published system of threat levels.

Our thinking about terrorism has increasingly come to be seen through the prism of the 9/11 attack for obvious and understandable reasons. But in thinking about the panoply of terrorist risks and how they might evolve, we should perhaps not become too narrowly-focused, particularly when weighing the likelihood of and impact of different types of terrorist attack. Events could have taken different courses in the past (not just in terms of the nagging question of could the 9/11 attacks have been avoided) and there are plenty of plausible futures against which we have to prepare and plan.

To illustrate this I wanted to quote to you an extract from a 1999 report to the Congress, which begins as follows:

“In recent years, the United States has focused increasing attention and resources on countering the threat of terrorist use of chemical, biological, radiological and nuclear (CBRN) weapons. The main catalyst behind this was the 1995 sarin nerve gas attack.... Two years earlier the bombing of New York City’s World Trade Center by Islamic fundamentalists had demonstrated that the United States itself was not immune to acts of terrorism intent on causing large numbers of casualties.”[3]

Why go back in this way? Well it illustrates the point that potentially mass-casualty terrorism is not simply an al-Qaeda related issue. And these attacks were instructive in what did and fortunately did not happen:

- The 1993 World Trade Center attack killed 6 people and injured a 1000. Its perpetrator - who was trained by al-Qaeda but probably not tasked by them - had wanted to topple one of the towers into the other and was also interested in the use of a radiological weapon as part of the attack. Fortunately, he failed on both accounts;
- The 1995 attack on the Tokyo subway left 12 people killed and more than 5000 injured. A Japanese apocalyptic sect perpetrated the attacks. At the time the attacks were seen as the defining incident for all discussion about the use of CBRN weapons and a turning point in the history of terrorism. It emerged that the sect had been very well resourced - it had highly skilled members and had aggressively recruited graduate students in biology, chemistry, physics and engineering. It had deployed biological weapons (botulinum toxin and anthrax) unsuccessfully. Problems with biological weapons had led to the switch in focus to chemical weapons. They had a stockpile of sarin sufficient to kill 4.2 million people, if they could have successfully deployed it in attack planning. Fortunately, this turned out to be a very big ‘if’. They were also in the market for nuclear materials and nuclear weapons.

It is I think worth having the perspective of the 1990's threat as viewed at the time – the first World Trade Center attack, the Tokyo subway attacks, the Oklahoma bombing, fears about lost Russian nuclear weapons and materials - as a complement to the unsurprising dominance of focus on al-Qaeda since the 9/11 attack.

Of course, al-Qaeda was moving up the threat picture in the 1990's and is referred to in the report to Congress I quoted from. We now know much more about its interests and activities then and since 9/11. Then these included, alongside attacks with conventional explosives, an interest with the Sudanese government in developing chemical agents, and an attempted purchase of uranium, which turned out to be a scam.

While in Afghanistan, the number two in al-Qaeda, Dr. Ayman al-Zawahari, was said to be particularly keen on the use of biological and chemical weapons. His professional background is interesting. Zawahari trained as a doctor; his father was a Professor of Pharmacology; in the mid-1990's, of 46 prominent members of the Zawahari family, 31 were doctors, chemists or pharmacists. Zawahari was said to have pored over medical journals to research various poisons and to have commented: "Despite their extreme danger, we only became aware of them when the enemy drew our attention to them by repeatedly expressing concern that they can be produced"[4] His comment illuminates an awkward handling issue for governments and the scientific community in seeking simultaneously to constrain the dissemination of sensitive information while not drawing attention to its sensitivity.

Among other al-Qaeda activity, a Malaysian businessman - with a degree in chemistry and laboratory science from California State University - was said to be seeking to cultivate biological weapons, particularly anthrax.

There are many other examples in the open literature of possible interest and involvement in Chemical, Biological, Radiological, and Nuclear ( CBRN) capability. There was also said to be an active debate within al-Qaeda on the benefits and risks in using CBRN weapons in terms of public reaction and the risks of retaliation.

### **Assessing the CBRN threat**

These are, of course, just fragments and flavours of a complex threat picture, which governments have to try to seek to make sense of, drawing on intelligence. The difficulties that arose over the collection, validation, analysis, and assessment of intelligence on Iraqi WMD illuminated the limitations of intelligence. One clear lesson to be drawn from the Iraqi WMD episode is the importance of ensuring that intelligence analysis and assessment draws on expert scientific advice and more broadly on the scepticism at the heart of the scientific method. One policy conclusion is the importance of maintaining deep scientific expertise within the intelligence community.

Intelligence can be said to involve a combination of secrets and mysteries. In the days of the Cold War, each side managed to understand the other's secrets in terms of military capability; the mysteries lay around intent. With terrorism the picture is reversed - there is reasonable understanding of intent; the mysteries lie around capability.

As the un-classified version of the US National Intelligence Estimate put it in 2007 in relation to the threat to the US homeland:

“We assess that al-Qu’ida will continue to try to acquire and employ chemical, biological, radiological or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.” [5]

So there lies the rub: how likely is such an eventuality? This requires us to predict both the steps al-Qaeda and other terrorist groups may take and the effectiveness of the actions that governments, other organisations and individuals take to counter them, stretching many years ahead.

Clearly a threat of conventional terrorist attack using conventional explosives will remain, from a variety of organisations in a variety of places. What is the prognosis for non-conventional attack? As I discussed earlier, the Japanese experience illuminates the difficulty in producing and deploying a biological weapon based on an existing, traditional agent. It can be argued, however, that biological weapons are easier to produce than nuclear weapons because the materials are more accessible and less expensive, the footprint in manufacture may be smaller and less detectable and their use could unfold and become clear only over a period and be less traceable back to the perpetrator and possibly a state supporter than the nuclear alternative. [6]

The further question which arises is how the risk calculation may change as the ability to modify DNA becomes ever more widespread. Here I am in the hands of the experts. It is not difficult to conjure up very frightening possibilities. In his book “The Meaning of the 21st Century”, James Martin suggests a truly deadly combination would be: a virus that is highly infectious; carrying a variant of the disease that has been created by gene engineering so that no protection against it exists in nature; one which has a long incubation period so that it could spread everywhere before anyone becomes sick; and which is 100% lethal. The lethality of such a virus would seem to take it outside the range of interest of today’s international terrorists whose target is not after all the whole world but defined parts of it. But it might, I suppose, appeal to an extreme millenarian. More pertinent perhaps is the judgement that the capability to create artificial pathogens against which nature has no protection is becoming easy: “a skilled person with the right equipment and appropriate training could do it in his basement.”[7]

Drawing lessons from the past is a dangerous guide to the future but we might draw some tentative conclusions from how the threat has and has not developed over the last 20 years:

- Terrorist attacks using conventional explosives or hijacked planes as weapons, with fatalities in the tens, hundreds and exceptionally thousands have had considerable impact on the affected countries and on the international community more widely. If terrorism is ultimately about achieving “Revenge, Renown and Reaction”[8], a strategy built around conventional attacks has proved very efficacious in these terms from the perspective of al-Qaeda;
- The Japanese and other experiences touched on above show the challenge involved in acquiring sufficiently lethal strains of present biological weapons of choice;

- The Japanese experience again shows the extreme difficulty that even a well-equipped terrorist group faced in preparing chemical and biological agents for dissemination and dispersal;
- If using biological and chemical weapons to produce mass casualties has thus far proved elusive, it is not hard, however, to conceive of scenarios for multiple limited attacks which could cause fatalities and have considerable presentational impact;
- While Islamist terrorists have been interested in CBRN attacks, the reality is that the main risk in terms of delivered attack has been from non-Islamist sources. The educated, alienated loner individual or cult in developed societies must be a source of concern, whether in biological or cyber attack.
- The detonation of a radiological device on an iconic target would have considerable human, economic and presentational impact;
- Subject to future developments in relation to biological weapons, the low-probability/high-consequence risk of most concern in terms of mass casualty attack would seem to be terrorist acquisition or development of a nuclear weapon. Some of the risk factors here are clear: in terms of the security of nuclear materials and of nuclear weapons themselves, and of links between present or former personnel of nuclear-weapons states and terrorist groups.

### **The link between terrorists and states**

How might the risk be affected by possible state sponsorship of terrorism? The state/terrorist link could potentially arise in relation to both actions effectively sanctioned by the agencies of a state and individual ‘private enterprise’. In assessing this range of risks, including through drawing on secret intelligence, governments can draw on the lessons from intelligence failures in relation to Iraqi WMD. The task of governments in persuading opinion formers and the public of these risks has, of course, been made much more difficult by the way intelligence on Iraqi WMD and on alleged links between the then Iraqi regime and al-Qaeda, for which there was no basis, were used as part of the justification for the invasion of Iraq. But the issue is real enough and, of course, a matter of serious current concern in relation to the transfer of conventional weapons to insurgent/terrorist groups in the Middle East and South Asia.

How far there is a meaningful risk in relation to the transfer of WMD, including nuclear materials or weapons, has to be a judgement. Some have downplayed this risk on the arguments that states would not put such potent capability in the hands of those over whom they do not have control and would also fear the consequences should such a link be successfully traced back to them [9]. The possibility of deterrence of this kind has important policy implication to which I will return. But there must be a real risk of miscalculation, both in relation to the likelihood of discovery and the consequences should this occur. US revelations about links between North Korea and Syria in the covert construction of a nuclear reactor in Syria are thought-provoking in this respect, admittedly in the context of a transaction between states.

### **Policy responses**

In tackling the risks I have briefly described, policy responses are required in the contexts both of terrorism generally and of countering the threat of proliferation of

nuclear weapons and other weapons of mass destruction. Science and technology need to be at the heart of such policies.

Some obvious illustrations can be drawn from the development of policy in these areas in the case of the UK Government, reflected, for example, in its recently published National Security Strategy. This identifies the four components of the UK's counter-terrorism strategy:

- Prevent: stopping people becoming terrorists or supporting violent extremism;
- Pursue: stopping terrorist attacks;
- Protect: strengthening protection against attack;
- Prepare: mitigating the impact of attacks.

The science and engineering community has an important part to play in relation to each of these:

- On Prevent, I have already mentioned the role of the social sciences in gaining a better understanding of drivers of extremism. There is also a more practical issue in the extent to which colleges and Universities are important places and institutions in which networks of violent extremists develop, and what can be done to counter this.
- The Pursue strand includes covert intelligence and police work to detect and disrupt the current terrorist threat in which there is increasing scope to exploit advances in, for example, sensor technology and increasingly powerful vision processing and data mining capabilities. Traditionally, intelligence agencies concerned with communications, such as GCHQ in the UK's case, have had world-leading capabilities in mathematics and information systems. But increasingly agencies concerned with human intelligence are huge data-exploitation businesses, drawing for example on private sector lessons in the development of social network analysis. With these changes come, of course, substantial issues about possible infringement of civil liberties to which I will return.
- The Protect strand includes work to protect infrastructure against all forms of attack; the development of enhanced physical protection against bomb attacks, including the development of blast-resistant materials; and work to protect borders against movement of suspect people and suspect materials. For the future an increasing focus will be on how security can be designed in to places and structures.
- On Prepare sophisticated capabilities are required to monitor, identify and respond to attacks, whether of a conventional or CBRN kind. At a more fundamental level, in modern economies stocks and spare capacity have been squeezed out in the interests of cost saving and complex networks have been created and operate on "Just-in-time" principles. The challenge is how more resilience can be built in at acceptable cost.

These considerations need to be addressed in the context of a threat that is international in two dimensions. For the UK at least these risks arise to our citizens both within the UK itself and overseas. Moreover, the threat itself involves links of various characters from ideological inspiration through to active advice and support from terrorists overseas to those engaged in terrorist-related activity in the UK

itself, often UK citizens. This intertwining of the domestic and the international adds greatly to complexity of handling.

Similar complexity can be seen in the range of actions required to seek to counter the CBRN threat and the wider proliferation risk at state level, not only in terms of the levers that need to be developed but the range of institutions involved – from global and international institutions, through Government and private and third sector organisations, to the level of the individual. The UK's strategy seeks to:

- Dissuade states from acquiring, developing, and contributing to the spread of WMD and related materials and expertise.
- Detect attempts by states and terrorists, to develop or acquire this capability.
- Deny access to WMD and the necessary materials, equipment, technology and expertise to develop them, while promoting commerce and technological development for peaceful purposes.

In the time available I can touch only on some aspects of this agenda. An important element in the Detect dimension must be to support the work of relevant international agencies and to use our security and intelligence and law enforcement capabilities to target proliferation networks and financing. Secondly, the capability to determine the source of material employed in any nuclear device is an important element in the ability to deter State-sponsored terrorism, as it opens up the possibility of retaliation against the identified proliferator.

An effective Deny strategy must include strengthening control regimes and ensuring much more effective physical protection of nuclear materials wherever they are held throughout the world. As Graham Allison has pointed out:

“The good news about nuclear terrorism is that this ultimate catastrophe is, in fact, preventable. The bottleneck for terrorists is acquiring nuclear weapons or the fissile material from which they could make nuclear weapons. Advanced societies have technologies for preventing theft of items they are determined to secure... This spectre challenges our determination, not our technical capabilities.”[10]

The point can, however, be put the other way round, as he also points out. Given the existence of a relatively straightforward lever, why has it proved so difficult for it to be given consistent priority?

As I suggested earlier, an accelerating trend in many western Governments is to see national security in a broader context than the traditional focus on inter-state conflict. Risks and threats are thought of in terms of potential impact at the level of the individual citizen. This can be illustrated in the shift in thinking about the risks posed by developments in the biological sciences. This can be broadly characterised as a shift away from focusing on the role of biological weapons in inter-state conflict towards concentrating on the risks of bio terrorism. It has important implications for public policy because it also shifts the focus and scope of defensive efforts away from a concentration on the protection of military forces towards a wider effort to protect civilian populations.

Both changes in the perception of the threat and in the focus of defensive measures have opened up new ways of thinking about the nature of bio security as being about infectious disease outbreaks and problems, whatever their source of origin,

that could potentially disrupt the normal functioning of societies. In other words it brings together security and public health considerations in ways that are potentially valuable for the handling of disease outbreaks but involve a number of potential tensions in relation to public policy, including resource allocation. Not only are there potentially hard choices in relation to the balance of spending between tackling different causes of infectious diseases, but also in the balance within public health more broadly. It also brings together communities, whether at national or international level, with different outlooks and cultures.

I can touch only on some of the issues that arise and their implications for science. [11] These include the renewed emphasis on bio defence and how it relates to the Biological Weapons Convention; the implications of the regulation of science and the extent to which this should include self-regulation; and the implications for governance.

Briefly to take each in turn:

- The bio terrorist threat has renewed interest in bio defence, particularly in the US, that some have suggested might push at the boundaries of what is permitted under the BWC and certainly reinforces the importance of the effectiveness of bio security in laboratories undertaking sensitive research.
- A number of genetic engineering experiments have revealed the scope to enhance pathogen lethality, synthetically to replicate pathogenic agents and so on. How far should such research be disseminated openly?
- The bio terrorist risk has led to increasing regulation of biological science through identifying agents and toxins of concern, registration and regulation of research conducted on such agents, and strict standards for safety and security, potentially enforced by criminal sanctions. In the UK, for example, the activities of some 400 laboratories are subject to controls under the Anti-Terrorism, Crime and Security Act, 2001. The question must be how effective in practice is this regulatory framework? Again in the UK's case, a recent investigation by a Parliamentary Committee, following the failure of bio security in relation to Foot and Mouth disease, raised some awkward issues about process and accountability in Government [12]. There is no reason to believe the UK will be untypical in this respect.
- The philosophical question might be how far such approaches are compatible with notions of scientific freedom. In practice such freedom has always been heavily constrained in other fields such as nuclear-related research. The important issue must be how far such constraints will restrict research of value in relation to wider public health, either because of the opportunity cost arising from the regulatory process and/or because restrictions on information flows weaken scientific progress?
- There is the related issue of whether state regulation should be complemented by a Code of Ethics and self-regulation?
- Finally there is the broader question of governance. How best to manage and mitigate the risk from the spread of infectious diseases engages interest in the public health and security communities from the level of global institutions down to the individual. It is a fascinating issue conceptually and from a practical perspective. I am less clear of its effectiveness in

relation to the potential terrorist threat from groups and individuals outside such frameworks.

### **Terrorism, Science and Society**

In a presentation of this kind I can touch only on some issues of relevance to the Conference's theme of Open Society, Open Science. I wanted to bring out one final example of the potential impact of scientific developments for the nature of the society we are seeking to protect. In his fascinating book "The Meaning of the 21<sup>st</sup> Century", James Martin suggests that the future is going to be a world of ubiquitous sensors linked to highly- intelligent computer systems. These will have a role in relation to business, crime-prevention, medical research, traffic management, and counter-terrorism. This world will be accompanied by a concept he terms 21<sup>st</sup>-Century privacy. The public may, he suggests, be divided into security categories, perhaps four. Those in category A will be security-cleared and have automatic identification wherever they go. The other three categories would consist of those who refused to engage with the system and those who did not meet the security requirements. 95% of the population might fall into Category A. Or put the other way round, 5%- in the UK 3 million people –could be at the mercy of the authorities. To be fair he concludes: "It is up to society to design computerized-enforced rules that protect our personal privacy, prevent undesirable interference with our freedom and punish officials who cause unnecessary harassment." [13] But perhaps that further compounds the problem. Despite or perhaps because of a lifetime working for government, I, for one, am not keen on the concept of either so-called necessary or un-necessary harassment by officials.

A number of excellent fictional dystopias have been written over the years around ubiquitous sensors and highly intelligent computer systems. They suggest extreme caution in contemplating such approaches to problems.

### **Science, Terrorism and Government**

My presentation today has covered just some of the dimensions of science and terrorism. This is I think a very difficult area for Governments to tackle for a number of reasons:

- Uncertainty over the likelihood and consequences of the component risks. Intelligence is uncertain. Assessments based on theoretical capabilities that might be deployed risk being excessively worst case.
- The terrorist threat is both domestic and international, linked together in complex ways. The policy response involves nearly all government departments, local government, security agencies and police, the private sector and individuals. Co-ordinating and orchestrating this effort is a massive problem generally.
- Individual organisations within this mix have their own science and technology strategies, some of long standing. But developing a Government-wide S&T strategy for counter-terrorism has proved difficult in the UK and I suspect elsewhere. The strategies rest at the centre of government or in Ministries of Homeland Security or of the Interior that, in contrast to Ministries of Defence, are not science and technology dominated organisations. One part of the way forward is to draw more clearly on defence expertise.

- There are related problems over the fragmentation of both the formulation of customer requirements and the responses of industry.
- In resource allocation terms, more immediate operational priorities can seem more compelling than S& T programmes, particularly when they are of a longer-term, more-speculative kind.

### **Thinking about Risk**

There is a further broader issue of how government weighs risks and considers the appropriate responses. In public discourse and the debate over priorities, terrorism has been a dominant theme since 9/11 for understandable reasons. But going forward do we need a more structured debate about different risks and their relative importance and do scientists have a role to play in such a debate?

A starting point might be the recognition that both Governments and citizens misperceive risks, in ways that are intertwined. This could be for a number of reasons. Studies suggest that the easier it is to recall examples of something, the more common we think that something must be. Or put another way, we overestimate the likelihood of being killed by the things that make the evening news and underestimate those that don't [14]. Now, of course, the things that appear on the news are shaped by journalists' views of what is newsworthy and in part by the agendas of politicians- who in turn are seeking to respond to issues of the day. As individuals, we are more relaxed about risks where we believe we are in control than those where we are in others' hands- say travelling by road in our own car in comparison with by rail or air. Deaths concentrated in place and time appear more horrific. And Government may have a sense of being more responsible for some issues than others particularly those with a security dimension. At the same time it is striking how individuals look to government to tackle issues that are largely the individual's own responsibility (for instance, obesity.)

Why does this matter? Ideally public policy should be shaped in relation to underlying reality –what is actually happening, alongside what we think is happening. If this is measured in terms of risk of premature death, it is not hard to find thought-provoking statistics that illuminate the need to see terrorist risks in a wider perspective. One example-in North America between 1968 and 2007, all international terrorist incidents killed 3765 people. This was slightly more than the number of Americans killed while riding a motorcycle in the single year of 2003.

Let me emphasise I am not equating terrorist murder- a completely unjustifiable act with an indefensible consequence- and the consequences of an accident. But they are comparable in two dimensions: each involves a life of equal value and each act and its consequences involve issues of public policy.

Another example of less potential controversy would be the comparison between the risks to individuals from bio terrorism and those from a possible flu pandemic. The latter is after all a high-probability event, of high-consequence. In the UK alone on plausible assumptions it might lead to 400,000 excess deaths or more. Has world effort been galvanised commensurate with the consequences of a flu pandemic?

To conclude as a basis for discussion with some headline points:

- Terrorism needs to be addressed in the wider context of other security risks and all these risks need to be evaluated from the perspective of the individual.
- Terrorism is a major concern whether in terms of the al-Qaeda threat or other possibilities that might unfold in the future. Low-probability/ high-consequence risks, whether in relation to nuclear or biological risks, need to be addressed alongside the inevitability of continuing conventional attacks.
- Science contributes potentially to the problem of terrorism as well as to helping to counter it.
- Intelligence has a crucial role to play and needs to draw on deep scientific expertise.
- As well as addressing scientific and technological contributions to new ways of more effectively countering terrorism, consistent attention needs to be given to crucial but relatively unglamorous actions- such as nuclear and biological security measures
- Social science has a key role to play.
- Inadequately regulated scientific activity and the unconstrained dissemination of scientific knowledge may significantly enhance the terrorist threat. Notions of scientific freedom and openness need to be tempered accordingly. But it will be very difficult to devise regulatory regimes that are effective on a global basis.
- Uncertainty over the threat and the breadth of the response required make countering terrorism a difficult subject to handle within Government, including in the development of Government-wide S&T strategies.
- And, finally, part of the contribution of science could be to help develop a better debate on risk.

July 2008

#### REFERENCES

1. N. Taleb, *Foiled by Randomness* (London: Penguin, 2007)
2. R. Suskind, *The One Percent Doctrine* (London: Simon and Shuster, 2006). p 62.
3. *First Annual Report To The President and Congress of The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons Of Mass Destruction*. 15 December 1999. (The Gilmore Commission). ([www.rand.org/nsrd/terrpanel/terror.pdf](http://www.rand.org/nsrd/terrpanel/terror.pdf))
4. L. Wright, *The Looming Tower* (London: Penguin, 2007) p 303.
5. See: [dni.gov/press\\_releases/20070717\\_release.pdf](http://dni.gov/press_releases/20070717_release.pdf)
6. See, for example, D. Fidler and L. Gostin, *Biosecurity in the Global Age* (Stanford University Press, 2008), p 25-6.

7. J Martin, *The Meaning of The 21<sup>st</sup> Century* (London, edenproject books, 2007) p.459.
8. L. Richardson, *What Terrorists Want* (London, John Murray, 2006), Ch. 4.
9. See, for example, the interesting discussion in the Gilmore Commission's First Report.
10. G Allison, *Nuclear Terrorism* (London: Constable, 2006) p 204.
11. For a fascinating discussion of these and other issues see Fidler and Gostin.
12. Bio security in UK Research Laboratories: Select Committee on Innovation, Universities, Science and Skills, Sixth report, Session 2007-8.
13. Martin, p 356
14. D. Gardner, *Risk* (London: Virgin Books, 2008) p.59.