Britain and security

Edited by Dr Paul Cornish

Britain and security

2007

The Smith Institute
The Smith Institute is an independent think tank that has been set up to look at issues which flow from the changing relationship between social values and economic imperatives.

If you would like to know more about the Smith Institute please write to:

The Director
The Smith Institute
3rd Floor
52 Grosvenor Gardens
London
SW1W 0AW

Telephone +44 (0)20 7823 4240
Fax +44 (0)20 7823 4823
Email info@smith-institute.org.uk
Website www.smith-institute.org.uk

Designed and produced by Owen & Owen

THE SMITH INSTITUTE

Britain and security

Edited by Dr Paul Cornish

Published by the Smith Institute
ISBN 1 905370 19 9

Contents

Preface

Wilf Stevenson, Director, Smith Institute

The Smith Institute is an independent think tank, which has been set up to undertake research and education in issues that flow from the changing relationship between social values and economic imperatives. In recent years the institute has centred its work on the policy implications arising from the interactions of equality, enterprise and equity.

While the classic menace of invasion no longer represents a key threat to the UK, an ever-widening range of dangers – international and domestic terrorism; energy insecurity; organised crime; infectious disease; and the consequences of conflicts and instability elsewhere in the world – represent new and complex threats to the country. Britain, therefore, will need to develop a diverse range of instruments to respond to these threats. In our increasingly diverse society it is clear that foreign, security, and national policy responses must be rooted in shared values. But they must also offer practical means by which the integrity of our crucial infrastructure and our civil society structures can be maintained in the face of new threats.

This collection of essays by key experts in the field offers a wide-ranging and thought-provoking account of security policy in today's world. They address both the core values that must guide policy makers in the coming years, alongside hard-edged analysis of the complexity and nuance that must be taken into account if measures to safeguard the British public are truly to offer robust safeguards against the range of threats that we may face over the coming decades. In the context of an increasingly "contracted out" public sector, how can we best ensure that the vital mechanisms hold fast under the extreme pressure represented by any of these threats? How can partnership working be strengthened to provide this security? And how can we expand these structures to take in the international and multilateral understandings so essential for our daily lives and positively crucial in times of crisis? What can be done to ensure that promoting our security is not confined solely to the Foreign Office, the Home Office and the security services but instead becomes the focus of each and every government department?

The Smith Institute thanks Dr Paul Cornish (head of the international security programme at Chatham House) for editing this collection and gratefully acknowledges the support of Smiths Group plc towards this publication and the associated seminar series.

Foreword

Keith Butler-Wheelhouse, Chief Executive of Smiths Group plc

The breadth and diversity of the contributions within this pamphlet are testimony to the scale of the challenge, and the sensitivity of the issues, faced by everyone engaged in the area of public security and safety.

The contributions also underscore how rapidly changing the security threats are that modern societies face, ranging, as Bruce Mann highlights in his chapter, from terrorism through accidents to natural disasters. Supporting this, Nick Mabey points out that, while the threats of terrorism and the proliferation of weapons of mass destruction currently dominate the agenda, a range of other dangers, fuelled by trends such as organised crime and corruption, and infectious diseases, will heighten our exposure to security risks in coming years.

While the authors set out a wide range of views, I believe that the scope of the debate encompasses three main dimensions:

- first, there is government, its institutions, structures and operational capability;
- second, there is society at large, its attitudes, what informs these and the way in which it reacts to the changing world; and
- third is the private sector, which is dedicated to helping solve problems and assisting in the delivery of agreed solutions both specifically for government and, as a consequence, for society too.

As chief executive of Smiths Group, I feel most qualified to comment on the third of these dimensions. As a global leader in the provision of threat detection and screening technologies for military, transportation, border control, homeland security and resilience applications, Smiths acts as an important bridge, enabling public policies to be actioned.

By closely working with the government and its agencies, we seek to understand and anticipate the security issues society is facing. And, on the basis of this knowledge, we develop the technological tools needed to meet these challenges.

And, in recognition of the scale of the challenges we face, Smiths and our colleagues in the security and resilience industries, together with leading academics (some of whom are among the contributors to this pamphlet) are working in partnership to make it easier for

the government to engage with us. One concrete manifestation of this is the formation of the new industry/government Security & Resilience Suppliers Council (RISC), which is chaired by my colleague Stephen Phipson, group managing director of Smiths Detection.

Security equipment facilitates the identification of explosives and of the potentially catastrophic chemical, biological, radiological and nuclear hazards that Dr Paul Cornish highlights in his chapter. It also helps to pinpoint narcotics and contraband, which are linked to smuggling and to illegal and subversive organisations. These technologies have been identified by the recent Defence Industrial Strategy as important to the UK and are deployed in a wide range of fields by civilian and military operatives.

However, deployment is just one aspect of all of this: understanding the interaction between technology and society is also vital. And this depends on how technology is used operationally and how society is engaged when it is deployed in the field.

Increasingly, people want to know that everything possible is being done to protect public safety. Yet, as Smiths knows better than many, there are also countervailing pressures to achieve this with minimum disruption to everyday, legitimate activity. Achieving the goal of "safety without social disruption" is the goal we all must strive for.

In conclusion, I welcome the opportunity to introduce this pamphlet and the chance to support the subsequent seminars. I hope that whatever your opinions regarding the personal views expressed here, you agree with me that the pamphlet furthers the debate around these important topics. For that, I heartily thank the authors and the Smith Institute.

Introduction
Dr Paul Cornish

Britain and Security is the product of a collaborative venture between the Smith Institute and the International Security Programme at Chatham House. As the title indicates, the purpose of this venture has been to examine aspects of British security policy in the early 21st century, at a time when the international political agenda seems particularly volatile and when a number of Western governments (including Britain's) are on the verge of change in one way or another.

For policy makers and independent analysts alike, "security" has always been an imprecise and even slightly problematic term. While the related fields of *foreign policy* and *defence policy* appear coherent, substantive and purposive, can the same be said of *security policy*? Security *from* what, or whom? Security to *do* what? Some analysts and scholars complain that "security" has become a catch-all term, with little or no precision in its meaning or its application. Professor Colin Gray, for example, the British-American scholar of strategic theory and practice, has argued that security studies "is a notably unhelpful concept" and takes issue with the "academic fashion which privileges the study of security over strategy".[1] By this view, the preoccupation with, and need for "security" is a feature of human life that is both intrinsic and general, and not susceptible to the narrow confinement of policy studies; a "ministry for human security" would be about as useful as a "ministry for human metabolism".

There is much that this collection of essays does not touch upon, such as humanitarian intervention and post-conflict reconstruction, traditional defence policy and military deployments, non-proliferation and arms control, energy and environmental security, and trade and economic security. Each of these subjects, as well as several others, might reasonably be included in any assessment of British security policy, broadly defined. Instead, and in an effort to bring some precision to the debate, *Britain and Security* focuses on more internal, domestic matters.

Al-Qaeda's attacks on the USA in September 2001, together with other terrorist outrages in Bali, Madrid, London and elsewhere, all indicate that a new and urgent, if not entirely discrete area of policy has indeed evolved in recent years. For those in government concerned to ensure public safety against violence and aggression, and the protection of

1 Gray, CS *Another Bloody Century: Future Warfare* (London: Phoenix, 2005), pp60-61

property and territory, these terrorist attacks call for a response which has elements of both foreign policy and defence policy, but which fits easily into neither category of policy and decision making.

In a December 2006 lecture, Sir David Omand – former Security and Intelligence Co-ordinator and Permanent Secretary in the UK Cabinet Office – spoke of "the 'global' nature" of hazards, threats and challenges faced by government, arguing that "the division into 'domestic' and 'defence and overseas' affairs should no longer be such a central organising principle of government". He went on to argue that the traditional paradigm of government organisation is "already shifting: for example in the UK counter-terrorism strategy that spans domestic and overseas action and relies upon the joint work of external intelligence and domestic police and security communities".[2]

In the UK, many analysts, academics and government officials are becoming increasingly interested in – and sympathetic to – arguments for the articulation of a national security strategy. In one of the leading contributions to this debate, a report by the London-based research institute Demos makes the following trenchant argument:

Increasingly the government will have to take a "networked approach" to national security, shaped and directed by an overarching strategy. This will lead to greater inter-dependence among departments and agencies, demanding a more holistic approach to security policy. The ramifications will become increasingly apparent as the responsibilities of departments blur, along with traditional lines of accountability; creating further opportunities for collaboration between public servants, and enhancing the prospects for innovation across government.[3]

"Security" might be a flawed term, but since *in*security has plainly arrived in Britain, it is difficult to imagine what other term might be more useful or accurate. There is a new security debate under way in the UK, one in which there are some obvious continuities with past practice; not least the public expectation to be protected from attack and aggression. But there is much less clarity when it comes to considering who Britain's adversaries might be, what they want and what they are prepared to do to achieve their aim. What is also open to debate are the costs (in cash and freedoms) that British society is willing to meet in order to achieve security from new and evolving threats and hazards.

2 Sir David Omand "In the National Interest: Organising Government for National Security", Demos annual security lecture, December 2006
3 Edwards, C *The Case for a National Security Strategy* (London: Demos, February 2006), p6

What is clear, and what complicates the debate still further, is that much of the response to these threats and hazards will have to be developed and delivered within a broad framework of domestic policy, rather than confined narrowly to considerations of defence in the Cold War style or pursued at arm's length under the rubric of foreign policy.

The first section of *Britain and Security* examines "Threats". My own chapter offers a deliberately stark, worst-case analysis of the danger of terrorist acquisition of CBRN – chemical, biological, radiological and even nuclear weapons and materials. I argue that the quality of the response to a CBRN attack will be governed by the level of public understanding of the threat. For Dr David Martin Jones and Dr MLR Smith, however, the security debate in Britain has become side-tracked, confused and diluted by the conviction held in some quarters that talk of threats and insecurity is disingenuous and manipulative – the "politics of fear". Jones and Smith see this discussion as largely delusory, obscuring the stark reality of the threat posed in Britain by violent extremists.

Finally, in the third chapter of this section, Nick Mabey seeks to take a broader view, arguing that the security and prosperity of the UK are being challenged by far larger movements than we are willing (or able) to contemplate. Short-term, so-called "hard" security challenges must, of course, be addressed. But in the era of globalisation there must also be a serious effort to come to terms with more complex, long-term and often "softer" means by which to deliver stability and security.

The delivery of security is the subject of the second section – "Policy responses". The first two essays offer the perspective of government insiders, while the third considers the problem of resilience and recovery in the private sector. Bruce Mann charts the changes made since 2001 in the organisation for civil protection in the UK. He writes of the development of a social contract between the citizen and what is increasingly – and usefully – becoming known as the "protective state". Under this contract, the public will make demands on government – for effectiveness and transparency – and, for its part, government will need to facilitate non-governmental and private involvement in the pursuit of resilience.

Rear Admiral Chris Parry calls for the rapid implementation of an idea that has been emerging in defence circles. The "comprehensive approach" offers a policy and organisational framework into which the diplomatic, military and economic functions of government can be integrated and can collaborate with foreign governments, inter-

governmental organisations and non-governmental bodies. Dr Bridgette Sullivan-Taylor and Professor David Wilson examine organisational resilience in the private sector. The terrorist threat to the private sector is real, but is often downplayed or ignored altogether, while more conventional business imperatives dominate the agenda. Sullivan-Taylor and Wilson argue that threat awareness and responsiveness should become part of business planning for any prudent and effective manager.

In the third section we address "Technology and the private sector". Writing on UK policy for research and technology, Professor Phil Sutton acknowledges that the threat to the UK and its interests is more complex and diverse than in the past. For sophisticated industrialised economies, research and technology has always been an essential component of security and defence policy. Sutton argues that this is no less the case now, but sees the need for government to collaborate more openly and efficiently with the private industrial and research communities, and with other governments.

Professor David Kirkpatrick offers an independent perspective on the UK's Defence Industrial Strategy and Defence Technology Strategy, making a plea for adequate funding for defence research in the UK, together with other measures to sustain the national defence industrial base. Looking to the future, Steven Bowns argues that defence research and development can be shown to have real, tangible value. Bowns is concerned, therefore, that the UK's competitive edge might be lost over the coming years. Unless investment is maintained in research and innovation, problems will be stored up "for decades to come".

Finally, Tony Baptiste shows how the private sector can contribute ideas, imagination and indeed technology to security and resilience in the UK. The maintenance of the UK's critical national infrastructure could be severely challenged by a multi-point, multilevel crisis, for example in the event of a major flood in one UK city coinciding with a terrorist attack in another. Communications, command and control will be essential, and the notion of a "virtual" national response system is that effective communications can be achieved and configured as required and as a crisis develops.

"Values in security" is the fourth and final section of this publication, and goes to the heart of the current debate about security in the UK. Shami Chakrabarti and Gareth Crossman warn against "overzealous law making" in the pursuit of security and protection. Security and civil liberties must be held in balance, and if that balance is lost – ostensibly for urgent and persuasive reasons of national security – then those rights and freedoms

that are characteristic of British society might be lost too, and perhaps irretrievably. A sense of proportionality is needed, otherwise security might be achieved, but at too great – and too fundamental – a cost.

For Bill Durodié much of the problem is that British society has lost sight of (or interest in) the values that ought to define and motivate life in contemporary Britain. For Durodié it is too easy to argue either that insecurity in the UK is the consequence of the actions of deranged foreigners, or that attacks on Britain represent just punishment for our country's past and present failings. Rather, insecurity in the UK stems from a deep malaise – "alienation and confusion" – which has gripped our country and the rest of the modern world. If terrorism is to be defeated, he argues, it will first be necessary to address the "dominant dystopian culture".

Finally, Elizabeth Wilmshurst calls for parliament to take – or be given – a more central role in the security debate. Wilmshurst's particular concern is with the process by which British armed forces can be deployed and committed to battle. At present such decisions are the responsibility of the Prime Minister, acting under royal prerogative, and the prior approval of parliament is not required.

With this collection of essays, written by experts in their field, *Britain and Security* offers a contribution to the debate surrounding security in contemporary Britain. The authors do not presume to provide all the answers; nor, indeed, have they asked all the questions pertaining to Britain's security needs and aspirations in the early years of the 21st century. Instead, the modest ambition of this volume is simply to provoke thoughtful, intelligent and fruitful discussion of some of the more urgent and complex policy challenges faced in Britain today.

Section I: Threats

Chapter 1

Chemical, biological, radiological and nuclear terrorism in the UK – how bad could it get?

Dr Paul Cornish, Carrington Chair in International Security and Head of the International Security Programme at Chatham House

Chemical, biological, radiological and nuclear terrorism in the UK – how bad could it get?[4]

In early November 2006 Dame Eliza Manningham-Buller, head of Britain's security service (known as MI5), warned that the danger to the United Kingdom of terrorist attack was "serious" and "growing", with as many as 30 terrorist plots under way. She argued: "Tomorrow's threat may – I suggest will – include the use of chemicals, bacteriological agents, radioactive materials and even nuclear technology." For the UK's security policy makers and practitioners, it would seem that traditional terrorism of the sort practised by the IRA has given way to the possibility (if not the expectation) that terrorist groups such as al-Qaeda might make use of chemical, biological, radiological and nuclear weapons and materials (CBRN) in an attack in the UK.

Dame Eliza's unusually public statement might be explained by the UK government's wish to improve national resilience by disseminating information about the CBRN threat. If so, this publicity campaign must be carefully managed. With too little information, the public might be insensitive to the risks and might not be in a position to react in a proportionate way in the event of an attack. Conversely, if the public were to be deluged with information about CBRN attack scenarios, then an exaggerated and even paralysing perception of insecurity might set in.

What is more, in the current climate, if any information (particularly about security and defence) is perceived to have been "managed" by government, then that information might be regarded as untrustworthy. Yet if there really is a threat to the public from some level of CBRN use by terrorists, no interest could be served by allowing that discussion to be lost to the cynical assumption that everything coming out of government is mere spin. With this in mind, this chapter draws upon material available in the public domain to address three questions:

- What are chemical, biological, radiological and nuclear weapons, and how available are they?
- What could terrorists do with CBRN, and why?
- How serious is the danger overall?

4 This chapter summarises the author's longer study entitled *The CBRN System: Assessing the Threat of Terrorist Use of Chemical, Biological, Radiological & Nuclear Weapons in the United Kingdom* (Chatham House, February 2007)

Chemical weapons

Chemical weapons are usually described as *agents*, which can attack the body in various ways: "nerve agents" such as sarin are highly toxic and attack the body's central nervous system; "blood agents" such as cyanide prevent the absorption of oxygen by the blood; "blister agents" such as mustard gas attack the skin and airways; and finally "choking agents" such as phosgene attack lung membranes.

In many cases, chemical weapon ingredients are "dual use", in that they have legitimate civilian industrial applications. The manufacture of mustard gas, for example, requires widely available chemicals such as ethyl alcohol, sodium sulphide and bleach, as well as the solvent thiodiglycol, which is used in the ink of ball-point pens. Many other industrial chemicals are also highly toxic, relatively easy to acquire and would need minimal processing and preparation before use. The US chemical industry, for example, produces about a billion kilograms of cyanide annually for industrial uses such as electroplating. Chemical weapons and toxic chemicals can be manufactured in solid, liquid or gas form, deliverable as powder, droplet or vapour by a variety of means including crop sprayers, smoke generators, artillery shells and aircraft munitions.

The availability of precursors has led to chemical weapons being described as "the poor man's atomic bomb", an expression that also captures some of the moral and legal taboo that has historically (albeit not universally) been associated with chemical weapons. Although the production, weaponisation and delivery of chemical weapons would be challenging, scientifically and logistically, as well as extremely expensive, a small number of low-yield chemical weapons would be relatively easy to hide and transport and might thus appeal to a well-organised and well-funded terrorist group. Produced and used in this way, while chemical weapons would not qualify as weapons of mass *destruction*, they could certainly have mass *effect*.

The public's vulnerability to lethal chemical weapons – particularly nerve agents such as sarin – has been apparent since the terrorist attacks in Japan in the mid 1990s. The fact that sudden death could come from colourless and (in some cases) odourless liquids and gases released covertly would add to uncertainty and could prompt panic. The possibility that a small-scale chemical weapon attack might trigger an immediate and disproportionately terrified response on the part of the target population could be seen by some terrorist groups as outweighing the difficulties, dangers and costs of developing chemical weapons.

Biological weapons

Biological warfare agents comprise micro-organisms and toxins. Micro-organisms depend for their effect on survival and multiplication within a target body and can be both contagious (for example, smallpox and Ebola) and non-contagious (for example, anthrax). Biological toxins such as botulin are poisonous products of organisms, are inanimate and cannot reproduce themselves, and are intended to have effects broadly comparable to some chemical weapons. As with chemical weapons, a covert biological weapons programme could make use of easily available dual-use material and equipment, and could exploit the "recipe books" that are reportedly available on the internet and elsewhere.

Unlike chemical weapon manufacture, however, a bio-weapon programme might require only a small research, development and production process, which would leave little or no signature and would therefore be easy to conceal. Although the weaponisation of a biological agent would be complex, requiring high-level competence in microbiology, pathology, aerosol physics, aerobiology and meteorology, for a terrorist group seeking a "single-shot" biological attack, safety, reliability and predictability in both production and weaponisation might not be of great concern. Delivery of a biological weapon could be a relatively straightforward matter, with a variety of dispersal means available and with more than enough suitable targets on offer.

Unless very large quantities of the most aggressive toxins were used, it would be difficult to be sure where and when a bio-weapon attack had taken place, since living biological agents need time to develop in the body before they can act. This becomes a problem not only for those responsible for managing the consequences of a bio-terror attack, but also for the terrorists themselves, since it would take time for evidence of their achievement to come to the fore. Nevertheless, biological weapons would be much easier to acquire or manufacture than nuclear weapons, and could have a bigger impact on public and political consciousness than chemical weapons. For these reasons, many argue that bio-weapons are becoming the terrorist's weapon of choice.

Western societies' visceral sense of vulnerability to bio-weapons, and to disease in general, means that bio-weapons have almost become something that the victim inflicts upon himself. Psychological vulnerability of this sort could easily be exploited by terrorists. Although casualty estimates vary widely, the political, psychological and economic impact of a bio-terror attack would be profound, even in the event of a low-level or bungled attack. If the difficulties of bio-weapon production and delivery could be overcome, the effect of an attack could very possibly dwarf any previous terrorist attack

in history; a possibility that might well appeal to the most committed terrorist group, taking a long view of the conflict in which it is engaged.

Radiological weapons

The purpose of radiological weapons would be to spread radioactive material over a wide area using either an explosive device, sometimes described as a "dirty bomb", or some other means of dispersal. Depending upon the material used, individuals might receive high doses of radiation, and the affected area (perhaps the financial district of a city) would be considered unusable until properly decontaminated. Radioactive material of various types can be acquired from a wide range of sources, including industry, hospitals and university research laboratories. The alleged murder of Alexander Litvinenko in London in November 2006 was apparently carried out with polonium-210, possibly from an industrial source.

The toxicity of radioactive material, and therefore the ease with which it could be handled, varies widely. But the combination of ready availability and (possibly) high toxicity has led to a widespread sense of vulnerability to a radiological weapons attack and even, in some quarters, to the belief that these would be the terrorist's preferred choice of weapon. Yet even though the use of these weapons could have serious political and economic consequences, in some circumstances the effects of such an attack would be limited.

The smallest type of explosive radiological weapons attack would involve a mass of high explosive (perhaps less than 100kg) jacketing a relatively small radioactive source of 1-10 curies.[5] A radiological attack on this scale would not cause mass casualties, but could cause disruption and economic damage. At the other end of the scale would be a device (explosive or other) designed to distribute tens or even hundreds of thousands of curies of radioactive material.

Analysts are, however, divided as to the effect of even a large-scale explosive radiological weapons attack, with some arguing that a victim close enough to the centre of the explosion to receive a serious radiation dose would be more likely to be killed promptly by the bomb blast than through radiation sickness. Yet while the physical harm from such an attack might be limited, the immediate blast could provoke panic and the prospect of

5 A curie (Ci) is a unit of measurement of radioactive strength. A 1 Ci source is regarded as large, and a 100 Ci source as extremely dangerous.

radiological contamination could cause widespread anxiety. The fear of radiation sickness would also feature in the public reaction to an attack; alpha or beta particles might be inhaled or ingested in the dusty environment just after the blast, while the longer-term possibility of cancers and other illnesses would cause concern.

The assembly and handling of a radiological weapon would pose significant technical challenges to a terrorist group, and very severe health hazards. The technical challenges would not, however, be insurmountable. And since in some cases the political and economic damage caused by a radiological weapons attack could be far-reaching, those terrorist groups and individuals for whom personal safety when handling radioactive material would not be a priority might well be tempted to acquire and use a radiological weapon.

Nuclear weapons

A nuclear attack could be achieved in one of four ways, the first of which would be to acquire and use a complete nuclear weapon. This is perhaps the least likely option, since stocks of nuclear warheads are generally closely supervised and the initiation of such a device would in itself be a complicated process. There are, however, persistent rumours that a large number of more useable, portable nuclear weapons (so-called "suitcase nukes") went missing in Russia in the mid 1990s and have yet to be found.

The second option would be to build a nuclear weapon. This would require access to significant quantities of fissile material (about 25kg of highly enriched uranium or 8kg of plutonium) as well as other sensitive materials and components. High standards of engineering design and manufacture are necessary for successful construction of a nuclear weapon. But according to some analysts, these standards are becoming steadily more attainable, particularly among developed and industrialised economies, and particularly where the simpler uranium-based gun-type nuclear device (such as the 12-kilotonne bomb dropped on Hiroshima in 1945) is sought.

If fissile material cannot be bought or stolen, it could be produced indigenously. But a clandestine uranium enrichment programme would require vast financial resources, together with secure and covert research and development facilities, as well as a very high-capacity electrical power supply. A programme on this scale would be difficult, if not impossible to conceal, and would therefore not be attractive to terrorist or radical groups, however well-funded. Plutonium separation is generally understood to be orders of magnitude more difficult than uranium enrichment, requiring a nuclear power infrastructure.

The third option would be to construct an improvised nuclear device (IND) with much larger quantities of lower-grade, power reactor-quality uranium. The device might then "fizzle" rather than detonate its entire mass instantly and efficiently. But even if the resulting explosion were to be equivalent to just a few, rather than tens of kilotonnes, the result could be devastation and contamination on a huge scale.

The final option would be to attack a nuclear power station, using conventional means (such as a large proximate explosion or the direct impact of a missile) to cause catastrophic breakdown of the reactor and its subsequent destruction.

The likely effects of a nuclear detonation are well-known; blast, thermal flash and nuclear radiation causing vast numbers of deaths and very intense destruction over a wide area, together with an electromagnetic pulse capable of destroying communications systems. It has long been supposed that use of a nuclear weapon would go so far beyond any notion of political violence as a form of negotiation that terrorists would not seek a nuclear capability. But thinking has shifted, and it is now feared that for terrorist individuals and groups driven by some religious, millennial or apocalyptic vision, the massive and hugely symbolic impact of a unilateral, spectacular nuclear strike could be precisely their goal.

It is widely believed, for example, that al-Qaeda has long been interested in acquiring a nuclear weapon, and that Osama bin Laden has declared it a "religious duty" to do so. Given the increasing availability of nuclear weapon-related technology, the destructive effect of a nuclear attack, and the reported intention of al-Qaeda, terrorist acquisition of a nuclear capability can be considered as nothing less than a threat to the security of the UK.

Conclusion

Quite apart from the obvious scientific and technological differences, each of the CBRN categories also differs in terms of availability, delivery systems and effects. A well-funded terrorist group, particularly one with a long-term vision of conflict and with the intention to inflict as much damage upon unprotected populations as possible, might be attracted to the most sophisticated chemical, biological and nuclear weapons, in spite of the associated technical challenges. Even if only a distant possibility, the effects of such an attack would be devastating and cannot be dismissed as too remote to contemplate.

But for some terrorist groups, the threshold of success might be much lower; after all, Aum Shinrikyo's campaign in Japan in the mid 1990s killed few people but achieved

notoriety for the group for over a decade. At this level, the most basic chemical, biological and radiological weapons, and possibly even improvised nuclear devices, could all prove tempting and, crucially, could all be perceived as more or less interchangeable means to the desired end.

It is appropriate to think of CBRN as a system offering all that might be required for a range of terrorist groups from the largest to the smallest, from the almost casual to the most organised, and from the poorest to the best funded. But it should also be borne in mind that another element of the CBRN system is the terrorist's expectation that a targeted population will prove to be brittle, reacting in a panicked and disproportionate manner, thus magnifying the effect of the attack.

Thus, while any terrorist attack in the UK using CBRN would be terrible for all those affected, in most cases the broader impact of such an attack would be shaped by the nature of the public response. There is a strong case, therefore, for retaining the initiative in that part of the CBRN system that is largely beyond the reach of terrorists, by ensuring a reasoned understanding of the threat and wherever possible a proportionate response to an attack.

Chapter 2

The politics of complacency and the current threats to UK security

Dr David Martin Jones, Senior Lecturer at the University of Queensland, and Dr MLR Smith, Reader in War Studies at King's College London

The politics of complacency and the current threats to UK security

In a rare public speech in November 2006, Dame Eliza Manningham-Buller – the Director General of the British security service, MI5 – observed the "realities of the terrorist threat facing the UK". Her observations reinforced those of politicians and of intelligence and police experts. Deputy Assistant Commissioner Peter Clarke, the head of the anti-terrorist branch of the Metropolitan Police, described the threat to the UK from al-Qaeda-related terrorism as "real, here, deadly and enduring", and reinforced the words of the Home Secretary that "the threat will be enduring – the struggle will be long and wide and deep".[6] Given that, by 2007, MI5 and the police had exposed numerous plots and Londoners had experienced the bomb attacks on their transport system in which 52 people lost their lives in July 2005, one might imagine that such pronouncements, although disturbing, contained little that was either provocative or deniable.

Somewhat surprisingly, this is far from the case. Influential media and academic commentators regularly cast doubt on the scale of the Islamist threat, maintaining that the government invokes the spectre of Islamic extremism primarily to curtail political freedom under the aegis of counter-terror policy. Proposals to introduce identity cards and extend detention of terrorist suspects without trial give outward and visible form to this creeping authoritarianism. Criticism of official policy endeavours to shift attention away from the proponents of violence to the government's role in both causing and exaggerating the threat and overreacting to its discovery. What sustains this perception and, moreover, is it accurate?

Fear and complacency

Central to this perception is the belief that the government since 2001 has cultivated a politics of fear in order to persuade the gullible masses to accept an extension of state power. The politics of fear has an interesting genealogy. It first appeared after 1990 in the form of a critical academic theory that postulated that the end of the Cold War would now require the West to define itself against a non-Western "other". Islam, from this perspective, already constituted an all-purpose bogeyman prior to 9/11. Moreover, the fact that there existed a real, rather than an imagined or constructed, Islamist threat, demonstrated by the 2001 attacks on New York and Washington, only helped popularise the politics of fear.

6 "The International Terrorist Threat to the UK", speech at Queen Mary's College, London, 9 November 2006

Broadly, the politics of fear holds that government has both invented and manipulated an Islamist threat. Somewhat differently, it also maintains that if there is a threat it is negligible and confined to a small minority of ideologues. Further, that if this negligible threat exists it is in any case our fault, either for the UK's history of colonial exploitation, its intransigence towards non-Western cultural understandings or for its "anti-Muslim" foreign policy.

By early 2005, the BBC was transmitting a version of this hypothesis to a global audience. Advertising the series *The Power of Nightmares*, the BBC News website in April 2005 announced that it "explores how the idea that we are threatened by a hidden and organised network is an illusion. It is a myth that has spread unquestioned through politics, the security services and the international media." Pre-publicity presented the threat as a "fantasy", which "politicians then found restored their power and authority in a disillusioned age".[7]

A slightly different version of the politics of fear permeated the judiciary when called to adjudicate on deportation or extradition orders for suspects wanted in third countries for terror-related offences. Thus, in December 2004, the highest appellate court found the detention of Abu Qatada, the suspected head of al-Qaeda's European franchise, illegal. Law Lord Hoffman pronounced that: "The real threat to the life of the nation, in the sense of a people living in accordance with its traditional laws and political values, comes not from terrorism but from laws such as these."[8]

The politics of fear, moreover, has proved extraordinarily resilient. Even when confronted with the London bombings or the scale of more recent conspiracies and their home-grown provenance, some terror analysts could aver that "the politics of fear can often overshadow a more informed discussion" of the causes of and policy responses to terrorism. "It is easy to slip into prejudices and assumptions about the 'enemy' rather than focusing on any erosion of citizen's rights resulting from the 'war on terror'."[9] Other analysts contended that the best way to build community resilience against the threat was to assume that there was not much of a threat to begin with, claiming: "We should remind ourselves that

7 "The Power of Nightmares: Baby It's Cold Outside" on BBC News, 14 January 2005. At: http://news.bbc.news.co.uk/go/pr/fr/-/hi/programmes/3755686/stm, accessed 17 July 2006
8 Quoted in Clare Dyer, Michael White, and Alan Travis "Judge's Verdict on Terror Laws Provokes Constitutional Crisis" in *The Guardian*, 17 December 2004
9 Oates, S "Selling Fear? The Framing of the Terrorist Threat in Elections" in *Security: Terrorism in the UK*, briefing paper 05/01 (London: ESRC/Chatham House, July 2005), p9

there have been few significant terrorist attacks in the developed world." To suggest otherwise was both "alarmist and disingenuous".[10]

Confronted by the fact of home-grown terror, therefore, academic and media commentary negated the extent of the internal threat and proposed a domestic policy of complacency, while exporting both the cause and responsibility for the 7/7 attacks and subsequent conspiracies. Britain's involvement in the Iraq War as the chief coalition partner of the Americans and its continued participation in the occupation of that country served, from this perspective, as the sufficient external cause of UK terror.

Jihadi groups, of course, widely exploited the American and British occupation of Iraq to maintain the Islamist rage locally and globally. As the policy response crystallised, however, more moderate commentators explored the Iraq connection. Journalistic commentators like Salim Lone argued that anti-terrorist measures would "only succeed if accompanied by steps to address intense Muslim grievances, including curbing wars of aggression and occupation, which are among the central causes of the exponential growth in terror".[11] For Gary Younge, "invading Iraq clearly made us a target". He added: "The invasion of Iraq – illegal, immoral and inept – provided the Arab world with one more legitimate grievance."[12]

One academic assessment, published less than a fortnight after the London bombings, gave expert approval to the external cause thesis. The authors considered that the "UK government has been conducting counter-terrorism policy 'shoulder to shoulder' with the USA, not as an equal partner, but rather as a 'pillion passenger'." They concluded that "the situation over Iraq has imposed particular difficulties for the UK, and for the coalition against terrorism" by giving "a boost to al-Qaeda's network, propaganda and fundraising".[13] *The Guardian* argued that it was "self-evident" that "riding pillion on George Bush's motorbike ... has exposed Britain more than before to al-Qaeda's fanatical enmity".[14]

Root cause or root of the problem?

The contention, however, that the Iraq war increased Britain's vulnerability assumes that there had not been a "rising terrorist threat" prior to the invasion of Iraq. Yet, somewhat

10 Durodié, B "Terrorism and Community Resilience – A UK Perspective" in *Security: Terrorism in the UK*, briefing paper 05/01 (London: ESRC/Chatham House, July 2005), p4
11 Salim Lone "Withdrawal Would Curb Terrorism" in *The Guardian*, 12 July 2005
12 "Blair's Blowback" in *The Guardian*, 11 July 2005
13 Gregory, F and Wilkinson, P "Riding Pillion for Tackling Terrorism is a High-risk Policy" in *Security: Terrorism in the UK*, briefing paper 05/01 (London: Chatham House, July 2005), p3
14 "The Iraq Connection" in *The Guardian*, 20 July 2005

inconveniently for Iraq War critics, Islamist terrorist incidents had actually increased in the years before the invasion. More particularly, after the overthrow of Saddam Hussein's regime Islamist groups attacked states, or their interests, that had refused to participate in the coalition of the willing. These included France, Holland, Russia and Turkey. The belief that foreign policy caused Islamist rage, therefore, overlooks the fact that Islamists display an undifferentiated contempt for the pluralism, secularism and moral degeneracy that they consider renders all Western democracies *jahiliyya* (a state of debased ignorance).

Through Islamist eyes, Western foreign policy was damned whatever it did. Hence, the Iraq War cause and the London bombings effect are not logical inferences. Indeed, the complexity of the evolution of the Islamist challenge to the West defies such simplistic correlation. It was always likely that Western intervention in Iraq would form yet another source of Islamist wrath. Rather, it would be surprising if British participation in the invasion of Iraq did not increase the notional threat level to participants in the US-led coalition. Observations to this effect are therefore entirely unremarkable.

More significantly, stating that the UK faces increased risk as a result of its foreign policy contains little in the way of practical or moral content. Foreign policy calculations that seek to advance the national interest are necessarily open to question, but both calculation and question must extend beyond short-term considerations that may, at any given point in time, engender a threat.

In other words, all government policies have to be considered within the wider purview of the balance of national interests. In this context, the broad agenda of British policy evidently seeks the eradication of violent Islamist extremism. The precise means may be disputed, but this goal remains regardless of whether the near-term security risk rises or falls.

Those who believe that Iraq makes Britain vulnerable to suicide bomb assaults argue that the withdrawal of forces from the country would curb terrorism. Plausible as it may appear on the surface, such a course of action to reduce short-term danger invokes the logic of appeasement. Proponents of this strategy often neglect to consider, however, that appeasing Islamist suicide bombers in an age of protean and global jihadism is far from a straightforward or plausible strategic choice.

The reason appeasing Islamism fails goes to the heart of a media-driven orthodoxy that fatally misdiagnoses the nature of the threat. Informed academic and media comment

consistently underestimates the danger of Islamic militancy, because it views the problem solely in tactical terms. This approach treats the recourse to terror as a matter of cause and effect. The insensitive prosecution of British and American foreign policy caused Muslim anger, and is thus regarded as having inspired one-off attacks on New York, Bali and Madrid. Even after the July 2005 attacks, this tactical misconception assumed that suicide bombing was the product of a specific and resoluble grievance, namely Iraq. Consequently, the tactical solution to the problem required a swift and "orderly withdrawal".[15]

However, while the commentariat treats the problem as tactical, the Islamist's conception is total. This misreading of Islamism's ends ultimately produces a condition of denial. Entrepreneurs of Muslim grievance and Western historical guilt such as Ziauddin Sardar, Tariq Ali and Tarak Barkawi reinforce the misdiagnosis for a wider media and academic audience. Thus for Tariq Ali, "the murderous chaos of Blair's war on Iraq came home to London in a lethal series of suicide bombings".[16] Meanwhile Barkawi maintains that "many in the West" consider al-Qaeda and its affiliates a "fanatical strain of religious fundamentalism", rather than a hybrid form of colonial resistance.

For Barkawi, it was essential to "find the requisite empathy to understand why men dedicated to the betterment of their peoples and willing to sacrifice their lives ... found it necessary to fly jet aircraft into buildings or to blow themselves up in the compounds of humanitarian organisations". If the West were able to make this "difficult leap of imagination", he suggested, "we might also learn an even more invaluable lesson: how to live in peace with people different from ourselves, people who choose not to live as we do or to organise their societies along Western lines, but who are nonetheless fully human and deserving of respect and dignity".[17]

The problem with this diagnosis is that the society that produced the bombers was not different from ours. They were the product of British society, a society that routinely extends tolerance and empathy to its many faiths and minority communities. The problem for those like Barkawi who wish to open a dialogue with Islamism is that the ideologues he maintains are "deserving of respect and dignity" do not believe that either he or we are deserving of respect or dignity in return, and until that time have no desire to "live in peace" with "us" or anyone else.

15 Rosemary Hollis "Isolating Extremists" in *World Today* 62:8 (August-September 2004), p21
16 *Rough Music: Blair, Bombs & Baghdad* (London: Verso, 2005), p53
17 "On the Pedagogy of Small Wars" in *International Affairs* 80: 1 (2005), p22

Empathy with the proponents of Islamist terror, therefore, requires a self-deluding strategy that screens out statements made by its UK adherents, such as Omar Brooks (also known as Abu Izzadeen) of the Saviour Sect. In 2005, Brooks asserted proudly that "I am a terrorist. As a Muslim, of course, I am a terrorist." To avoid any possibility of misinterpretation, Brooks further asserted that it was necessary for Muslims to "instil terror into the hearts of the kuffar".[18] Similarly, Abu Uzair declared: "The banner has been risen for jihad inside the UK which means ... it is allowed for them to attack."[19] Meanwhile, one of the leaders of al-Muhajiroun, Anjum Choudhury, speaking at a public gathering after the 9/11 attacks, observed: "Blair came out; George Bush came out at the same time. But what did he say? He said: 'You're either with us or you're with the terrorists.' And what did we Muslims say? We said: 'We're not with you – we're with the terrorists!' Allah Akbar!"[20]

The commentariat and its discontents

That such statements do not self-evidently demand empathy illustrates a curious disjuncture between what Islamists themselves say, and have been saying for many years, and what analysts think they really mean; and between what the commentariat think they really mean and what Islamists actually do. Why does this misunderstanding arise?

Interestingly, those who promote the politics of fear as an explanation and an alternative policy of complacency towards the home-grown phenomenon inhabit a worldview that finds the proponents of Islamism literally incomprehensible. The academic, judicial and media elite who favour either dialogue with Islamism or complacency towards its means and ends function within successful, market-oriented, post-religious, plural societies characterised by a modular and disenchanted pursuit of reason. Their worldview further assumes the movement of history globally in the direction of a convergent progressive, democratic, secular modernity. Violent disruptions on the path to this ineluctable end of history are treated as temporary aberrations, caused either by local psychopathology or structural inequality, to be solved by market access coupled with economic redistribution. It conceives political action in terms of cause and effect. It assumes, too, that if an actor's means appear limited so, too, must the ends.

By contrast, the contemporary Islamist challenge denies the inevitability of a pluralist and secular end of history. When Osama bin Laden proclaimed on 9 December 2001: "The time

18 Quoted in "Inside the Sect that Loves Terror" in *The Sunday Times*, 7 August 2005
19 Quoted in report by Richard Watson, *Newsnight*, BBC 2, 1 August 2005
20 Ibid

has come when all the Muslims of the world, especially the youth, should unite and soar against the kuffar and continue jihad till these forces are crushed to naught, all the anti-Islamic forces are wiped off the face of this earth and Islam takes over the whole world and all the other, false religions," he, and his followers, comprehensively rejected secular rationalism.[21] Much of the commentariat, however, refuses to accept this rejection, because their worldview denies Islamism's premise.

Thus, while the protean jihadist cells may appear inchoate, their plotting disjointed and the means limited mainly to unpredictable bomb attacks or hostage taking, the vision is nevertheless total, aiming to resolve the predicament of modernity not by accommodation, but by destroying it. Its prescription can be traced to the growth of an Islamic formalism from the 19th century onwards that sought to address the challenge posed by a progressive and increasingly secularised modernity held responsible for the relentless degeneration of Muslim civilisation.

Thinkers like Muhammad ibn Abdul Wahhab (1703-87) sought to remedy the failed Muslim response to the Judeo-Christian or "Western" civilisational challenge through a return to a stricter piety and the pure fount of the Koran's teachings. Although the return to authenticity was initially a call for spiritual rejuvenation, the purification of Islamic thought and practice inexorably acquired political overtones that would transform it into a *nizam* – total ideological system – demanding individual subservience to holy law.

For Islamism's most important ideologist, Sayyid Qutb, this imperative involved the division of humanity into the sphere of Islam and the world beyond it, which was *jahaliyya*, a debased state of ignorance. In Qutb's view, it was the complete "submission to God alone, in its beliefs, in its observance and its legal regulations" that constituted "the only civilised society".[22] The Islamist, therefore, seeks a condition where "sovereignty belongs to God alone, expressed in obedience to the Divine Law, only then is every person in that society free from servitude to others, and only then does he taste true freedom".[23]

This Manichean worldview incites an activist approach to politics that legitimates violence to bring about the desired utopia. The critical political difference between Islamist and

21 "Declaration of War Against Americans Occupying the Land of the Two Holy Places" in Alexander, Y and Swetnam, MS (eds) *Usama bin Laden's al-Qaida: Profile of a Terrorist Network* (Ardsley, New York: Transnational Publishers, 2001), Appendix 1, A, p19
22 Qutb, S *Milestones* (New York: Mother Mosque Foundation, 1979), pp81 and 94
23 Ibid, p94

fascist totalising visions is that Islamism currently lacks the resources afforded by a modern state to prosecute its version of a total ideological solution, thus compelling recourse to asymmetric means. And Qutb's vision inexorably invited violence, given that he considered it the duty of all Muslims to struggle against everything *jahaliyya* and replace infidel arrangements with Koranically acceptable alternatives.

Over time, the ideology fashioned a resistance beyond the established international order, which relied increasingly upon a de-terrorialised transnational *umma* (community of believers) to lead the assault against "domineering Western enslavement". Islamism's all-embracing *nizam* encourages a will to action that affirms the right to "slaughter" unbelievers "like lambs".[24]

As an Islamist training manual captured by Manchester police in 1998 declares: "Islamic governments have never and will never be established through peaceful solutions and co-operative councils. They are established as they always have been ... by pen and gun ... by word and bullet ... by tongue and teeth."[25] Such statements do not recognise limited goals that might afford a space for political dialogue.

Conclusion: an end to denial

The failure of sections of the media, academic and political commentariat to accept the actual character of Islamist ideology has thus engendered a tendency to mistake limited means for limited ends. The means, however, remain limited only for the time being. Islamists are entirely clear about the nature of the conflict in both its global and local form and the means to achieve its end. While there exists an asymmetry in comprehending the character of the threat, complacency will continue to afford the space for extremists to exploit.

Yet the evidence revealed by the regular discovery of plots demonstrates the existence of a threat, not just the fear of threat. Policy towards this threat should therefore be framed in conditions unencumbered by the politics of fear and the associated practice of complacency that have conspired to deny the nature of the current danger and impeded its effective interdiction.

24 *Al-Qaeda Training Manual*, document recovered by Manchester police in 1998, translated from Arabic to English and presented as evidence at the trial of Richard Reid in the USA in 2003, p5. The passage continues "and let the Nile, al-Asri, and Euphrates rivers flow with their blood".
25 Ibid, p3

Chapter 3

Security trends and threat misperceptions

Nick Mabey, Chief Executive of E3G: Third Generation Environmentalism

Security trends and threat misperceptions

Beyond intent: the security challenges of growing interdependence

The threat of terrorism and proliferation of weapons of mass destruction dominates the conventional security agenda, and in doing so often obscures trends that have far larger impacts on the security and prosperity of UK citizens and companies. These threats emerge from the rapidly growing interdependence that is the defining feature of our world: an interdependence that is deepening through multiple channels of communication, trade, investment, migration and the impact of economic pressures on the supply of natural resources and climate stability.

The spectacular rise of China illustrates how these changes will affect the global security landscape, in both positive and negative ways. China is radically changing the global economic power balance, leading to concerns about competitiveness and future military threats. China's interventions in Africa, Central Asia and South Asia to secure access to energy and minerals are affecting the whole range of security concerns: from limiting Security Council action against Iran and Darfur to weakening the international community's influence in moving regimes like Myanmar and Zimbabwe towards democratic reforms. China will become the world's largest emitter of greenhouse gases in the next five to 10 years.

But while traditional military strategists – particularly in Washington – focus on the threat from China's future economic and military strength, the reality is that it is China's weakness that is the biggest challenge to UK and global security over the next few decades.

China is still a relatively poor and developing country, undergoing profound and destabilising changes. Chinese leaders estimate that the economy must grow at around 7% a year to prevent internal social unrest, and they need to secure the energy supplies to achieve this. China's inability to compete against the USA in political, financial or military influence is a key reason for it striking energy deals with "pariah" states such as Sudan, Iran, Myanmar and Angola; with India (the world's largest democracy) following close behind. China's fears about destabilising shortages of food and water are also driving its relationships in Latin America and Africa, to secure access to fertile land. China's economic need to use its major domestic energy reserves of coal is behind the rapid rise in greenhouse gas emissions.

China is trying to manage the domestic tensions caused by its growth, but is hampered by the immaturity of its political, governance and social systems. Ambitious targets to increase energy efficiency and lower oil imports have been missed; policies to save water and reduce pollution are not implemented; outbreaks of infectious diseases such as severe acute respiratory syndrome (SARS) are covered up; people traffickers continue to send economic migrants to Europe; and regulation to prevent land expropriation for commercial development is ignored, leading to 70,000 public protests every year.

In the past we would perhaps have seen these as internal matters for the Chinese to deal with, and an internal crisis in China could have been welcomed as reducing their global influence. But interdependence now means that we cannot afford for China to fail. The majority of the economic growth driving these tensions is devoted to producing exports for the developed world, often from factories owned and built by foreign companies. A failed China would bring global economic depression and probably a more dangerous and hostile regime into power. A hostile China would be less interested and less able to control its greenhouse gas emissions, which constitute a direct threat to the UK.

China is just the most visible example of how our security and prosperity are becoming ever more intertwined with what was previously called the developing world. UK security and stability will be increasingly determined by the ability of India, Brazil, Mexico, Indonesia, South Africa and many others to manage the tensions of industrialisation and globalisation.

In this context, traditional security policies of deterrence and containment will increasingly fail to deliver. For these threats there is often no malign intent to identify and then deter, and we have in any case often chosen increasingly to intertwine ourselves with the sources of these challenges.

Four trends to watch

Interdependence heightens our exposure to governance failures and instability elsewhere in the world. These risks are being heightened by four key trends that will strengthen over the coming decades.

Organised crime and corruption

Before 9/11, international security discussions frequently focused on the rapid growth of organised crime as one of the largest security threats. Though terrorism has largely displaced organised crime as a priority in security and intelligence agencies, at least in the

USA and Europe, crime remains a core concern. Illegal drug use alone costs the UK £24 billion every year in crime, health and policing costs. Online fraud and extortion are increasingly a trans-boundary problem, with a growing incidence in the UK of infra-structure attacks.

The markets supplied by international organised crime are estimated to be worth around $1 trillion annually. Market growth is fastest in urban areas in newly industrialised countries, and in Africa, which is fast becoming a major transit and demand area for illegal drugs; in 2004, five of the seven fastest-growing markets for heroin were in Sub-Saharan Africa. International organised crime undermines and corrupts supply and transit countries, and leads to high levels of violence. Latin America shows these impacts very clearly. Crime-related violence is the major cause of death for young men in five Latin American countries, and costs the continent $138 billion every year as well as financing urban and rural narco-insurgencies in several countries.

Organised crime by its nature corrupts public institutions, particularly law enforcement and border systems; global money-laundering activity alone is estimated to involve annual flows of $800 billion. Around 85% of class A drugs are sourced in countries classified as unstable; for example, Afghanistan, Columbia and Burma. Transdniestria in Moldova is an example where organised criminal networks involved in the arms and drug trades are closely linked to the ruling elite and have become embedded in the institutions of the country. This is driving instability on Europe's borders and spreading corruption to other countries, as well as increasing the risk of terrorists gaining access to sophisticated weaponry.

Organised crime creates an illegal infrastructure that is readily exploited by terrorist groups that do not themselves have the financial power to bribe officials. Al-Qaeda's global budget has been estimated at between $10 million and $50 million a year, which is dwarfed by organised crime flows in its core operating areas in Asia, Middle East and East Africa. Drug-smuggling networks are thought to have provided the transit routes to take Afghan insurgents to Iraq for training in the manufacture and tactics of "improvised explosive devices". Worldwide, there are over 35 reported cases of close links between international organised crime and terrorist groups. Organised crime in the UK is also funding conflict; for example, through extortion and fraud the Tamil community in London is a source of funds for the Tamil Tigers, and the Turkish Kurdish community for the PKK.

The globalisation of transit routes and the demand for illegal commodities will make law enforcement action against organised crime groups increasingly complex, and will spread the destabilising impact of corruption widely.

Infectious diseases

As increased interconnectedness increases opportunities for organised crime, it also raises the potential speed, scope and severity of infectious disease epidemics. A serious global flu pandemic could cause global economic losses of $800 billion, owing to knock-on macroeconomic effects. Following the experience of the avian flu and SARS outbreaks in Asia, estimates of the direct economic losses in Asia from a future pandemic lie between $99 billion and $283 billion.

Containing the spread of pandemics depends on effective global monitoring and surveillance, and on prompt and efficient action by countries where the outbreak occurs. A threat that is harder to control is the evolution and spread of drug-resistant diseases – from TB in Russia to HIV in Africa – which is hastened by poor prescribing and medication practices. Drug-resistant strains of dangerous diseases already present a growing threat to the UK, and this will only increase as global travel intensifies and the number of drug-resistant strains increases.

Financial stability

Much of the economic impact of pandemics is caused by the precipitation of a financial crisis following a rapid decline in investor confidence. The fragility of the international financial system in the event of such shocks was exemplified by the impact of the relatively small Thai economy in triggering the Asian financial crisis, in which Indonesian GDP was reduced by a startling 20%. Over the last 30 years financial crises have reduced global GDP by around $8 trillion, with percentage impacts split evenly between developed and developing countries. However, the impacts on political stability are more severe in developing countries, where increased unemployment is not cushioned by social safety nets and savings are low.

The increasing integration of global financial markets both stabilises the overall system, by increasing overall global liquidity, and destabilises the system by making contagion effects from unstable to stable economies more likely. The ability to monitor and predict these crises is limited by their overall complexity – each financial crisis is unique – and by the continuing lack of financial transparency in major economies such as China and India. Though the UK, along with other developed economies, has been relatively insulated from

recent financial crises, our exposure can only grow in the coming decades. The UK's high economic dependence on financial markets makes it particularly vulnerable to serious crisis.

Energy and climate security

Of all the systemic threats, energy and climate security is likely to become the defining issue for international relations in the coming decades. Instability in oil-exporting countries was estimated to add a $10-$15 bbl premium to oil prices in 2006, costing the UK between $6 billion and $9 billion a year; far more than estimates of the cost of any terrorist attack. The recent rise in oil prices has cost low-income countries $270 billion, compared with net aid flows of $85 billion, reducing the pace of economic growth and poverty reduction.

Reserves of oil and gas will become increasingly concentrated in the OPEC countries and Russia, as overall supply reduces and long-term prices rise. This is already increasing the political influence of fossil fuel exporters at the regional level – for example, with Russia having an increasing influence in preventing democratic reforms and conflict resolution efforts in Europe's eastern neighbourhood. Scarcity is driving geopolitical competition among major energy-consuming nations, which often has the perverse effect of further destabilising supplier countries by preventing necessary political and economic reform.

Fears about energy security continue to drive military planning for intervention in oil-producing regions and protection of strategic assets and transit routes, and increasingly also investment in more secure energy alternatives such as coal, biofuels, renewables and nuclear energy. Countries such as China, India and the USA are turning to coal to satisfy their energy security, and the lifetime greenhouse gas emissions of all planned coal power stations would equal total global emission from the Industrial Revolution to 1970. If these investments go ahead without carbon sequestration, the world will be committed to over 6^{o}C of global temperature rise by the second half of the century, with devastating impacts on global prosperity and security.

The alternative of investing in more nuclear power raises serious issues over nuclear proliferation. Experts estimate that an aggressive programme of new nuclear build would see a tripling of global installed nuclear capacity over the next 40 years – half of which would be in developing countries, many of which are unstable, such as Nigeria and Indonesia. This would only have a modest impact on reducing climate change (about 10% of total carbon reduction needed by 2050), but a major impact in the spread of nuclear technology and fuels.

In the medium term, the costs of energy insecurity will be dwarfed by the impacts of climate change, which could produce impacts of 5-20% of GDP from 2050 – with negative effects highest for poor people in poor countries, who are least able to adapt. However, the security and stability impacts of a changing climate will arrive much earlier than major economic disruptions. Average global temperatures may only have risen by 0.7°C owing to climate change, but the impact on marginal areas has been large. Major droughts in Sahelian Africa have been linked to climate change and El Nino events.

These abnormal conditions have pushed traditional resource management regimes beyond breaking point, resulting in a wave of migration and low-intensity conflict across the region. The roots of the Darfur conflict in part lie with the communalisation of conflicts between pastoral and agricultural groups over access to scarce resources. Even without climate change, increased population and industrial demand means that by 2025 over 60% of the global population will be living in countries with significant water stress.

Among those areas where water supply is vulnerable to early climate change, where the natural resource base is weak, where governance is poor and where communal tensions already exist over resources, several areas stand out as highly at risk, including North and Sahelian Africa, the Middle East, Central Asia and several small island states. More severe climate changes, including rapid sea level rise from the melting of major ice sheets, would severely affect major coastal populations in South Asia and Africa, especially Bangladesh. The water supply of over 1 billion people is at risk from declining Himalayan glaciers, which feed the major rivers in India and China. Sea fisheries that provide primary protein for 800 million people are already being disrupted by climate change. These large events will produce mass migration, including across international borders, and severe conflict over remaining access to water basins and other resources.

Adaptation to help cope with these changes will require expenditure of between $10 billion and $40 billion per year, and increased humanitarian costs from natural disasters and environmental refugees estimated to be between $30 billion and $60 billion by 2015. This compares with current total aid expenditures of around $100 million, climbing to $150 million by 2015. The peacekeeping costs of responding to endemic instability from climate change would be far higher, as would be the consequent impacts on security.

Reducing the risks of instability and conflict

Though the negative trends above pose growing security threats to the UK, they are neither inevitable nor entirely without positive features. The growth of the global

economy, fuelled by global trade and investment, is also raising people out of poverty, strengthening managerial and governance systems and providing state resources to ensure stability and security.

However, for many countries the negative factors outweigh any positive trends, and are compounded by destabilising demographic trends increasing the proportion of young men, by economic transformation and by the HIV/AIDS epidemic. HIV/AIDS disproportionately affects working-age and professional people, reducing the capacity of the country to manage tension peacefully; in many African countries 80% of the armed forces are HIV-positive, compared with 5-10% of the general population. Many weak governments have few resources to manage these threats and reduce the risk of instability and conflict. State weakness is particularly correlated with the incidence of "grand corruption", much of which is related to industrialised country investment, and which imposes annual costs of between $1 trillion and $1.5 trillion on the world economy.

The impact of global instability on UK security, as opposed to humanitarian or poverty reduction goals, is never straightforward, but these threats should not be dismissed on the grounds that the countries concerned are far away and that future conflict and instability can never be exactly predicted. The major driver of asylum seekers moving to the UK has been internal conflict and state failure, and refugee camps have provided ideal recruitment camps for extremist movements globally. The UK's long-term strategy to engage and foster moderate Islam, especially in the European neighbourhood, would be fatally undermined by the emergence of endemic instability and economic decline in these countries; a scenario that is highly likely given current trends and an absence of serious economic and political reforms.

Rebalancing the strategic mix

A broad-based security strategy needs to take into account these trends as both drivers of direct security threats and inhibitors of successful security responses. It would take a long-term and systemic approach to managing these risks, through a combination of four generic strategic approaches, which span foreign and domestic policy:

- **Isolation** – closing/restricting borders, pursuing self-sufficiency in energy;
- **buffering** – reducing exposure to global shocks, for instance building national oil reserves, vaccine stocks, diversifying export markets;
- **reaction** – rapid response to emergent threats, for instance through military intervention and international police activity on drugs and international crime; and

- **prevention** – investing in global, regional and national governance networks to reduce instability and strengthen governance of key threats.

There is no simple strategic solution to these complex problems; all responses are costly and have different probabilities of success. Interventions must be targeted and sustained if they are to be effective, and no country can work everywhere. The effectiveness of each approach is heavily determined by the prevailing political context and willingness of others to co-operate.

There has been much analysis of the ineffectiveness of reactive responses in controlling the international illegal drugs trade, as prices continue to fall in all major markets. However, investment in strengthening national policing systems in supplier and transit states (such as Columbia, Afghanistan and Jamaica) has also met with mixed success. UK energy security policy has so far focused on EU market liberalisation. But with the decline in national oil and gas reserves, the UK now needs to reduce exposure to volatile markets through efficiency and renewable energy, and through much stronger engagement on energy and climate security with other countries through the EU.

The reality of UK security policy is that choices between these approaches are often made implicitly, and are heavily determined by existing institutional structures. The security architecture is designed essentially to deliver isolation and reaction strategies, and it tends to underinvest in resilience and preventive strategies. Except for high-profile missions such as Iraq and Afghanistan, the UK security machinery finds it difficult to maintain a long-term strategic focus on delivering reform and stability in any region.

The result is an unbalanced portfolio of action and funding, which does not reflect the relative size of different security threats. The UK spends only £40 million on tackling organised crime overseas, and £200 million on preventing crisis and conflict (including UN and EU contributions but excluding peacekeeping missions and general development aid), compared with an annual armed forces budget of £35 billion. The UK is one of the largest global investors in preventive responses globally, but still has a large imbalance between its capability to project force and its capability to project stability, enforcement and good governance.

This approach does not mean cutting the UK's ability to project hard power, but complementing it with new capabilities to deliver stability and security. It is vital that the security benefits of such investment are clearly prioritised, in order to strengthen the

political impetus behind such interventions. A good example is the Extractive Industry Transparency Initiative launched by the UK in 2002, which works with resource-rich countries and oil and mining companies to make payments to public authorities transparent and so less prone to corruption.

Given the very strong links between badly managed resource extraction, corruption and conflict, this probably represents one of the UK's most effective conflict prevention and security initiatives. However, it is still primarily seen as a development policy (and though created in the Cabinet Office is now led by the Department for International Development), which reduces the political priority given to engaging countries such as China, which are essential to its long-term success but have yet to co-operate.

Following the spate of civil wars in the 1990s, there was political pressure in the USA, the UK, Germany and others to invest in new forms of preventive security capability. However, this political push has disappeared since 9/11 and many of the reform processes have stalled. The failure to produce sustainable stability in Iraq and Afghanistan and potentially Congo is also leading to a louder call from "neo-realists" to retreat to a mainly reactive approach: avoiding "nation building" and merely intervening on a short-term basis to attack perceived threats. But events in Somalia show the danger in taking a short-term approach to building security, as this allows the creation of "ungoverned spaces" and weak governance, which undermines a range of security objectives – not least, the attempt to win hearts and minds in the Muslim world.

It is unsurprising that there have been failures, given our weak capacity and short experience of stabilising countries and building governance systems; but this has been a failure of implementation, not strategy. The emerging successes in the Balkans, Aceh, East Timor and Sierra Leone, among others, show that with concerted long-term effort by the international community, security and stability can be achieved in these areas. The task is to move forward with a more ambitious and balanced security agenda, which will require some fundamental reforms in the security architecture.

The danger is that current proposals to combine and centralise UK security architecture around anti-terrorism strategy will result in only strengthening capability to deliver hard security and intelligence co-operation. While important, this will further marginalise and weaken the UK's ability to anticipate, prevent and respond to more complex and long-term threats driven by the trends above, and will undermine our ability to deliver a long-term strategy towards global Muslim extremism. The UK should reinvigorate its

role in pioneering new approaches to facing these threats, as it did through leadership on the International Criminal Court, the "responsibility to protect" agenda and increasing global peacekeeping capability.

The coming years also give the opportunity to reshape the EU's security capability, as the revived constitutional debate brings back discussion of a strengthened security architecture, including a new EU external action service. As enlargement has shown, if deployed imaginatively the political and economic scale of the EU provides a unique ability to promote stability and good governance; particularly important in North Africa, the Caucasus and Central Asia, and through partnership with the African Union into Sub-Saharan Africa.

Terrorism and proliferation of weapons of mass destruction are core security threats, but they often obscure the importance of other threats to the UK's security and prosperity. In an interdependent world, a security strategy must of course address short-term hard security threats, but must also be able to motivate the long-term investment in co-operative institutions, relationships and governance needed to tackle underlying drivers of insecurity and conflict and the negative side of globalisation.

Section II: Policy responses

Chapter 4

The UK civil contingencies framework – building common endeavour

Bruce Mann, Director of Civil Contingencies at the Cabinet Office

The UK civil contingencies framework – building common endeavour

The UK has, since 2001, pursued a fundamental shift in the purpose and organisation of civil protection[26] in the UK. The Cold War model of civil defence – focused on a single, monolithic threat, managed top-down by central government in secret and restricted to a small community – has gone. In its place has come a model better suited to a modern "network society",[27] with its increased connections and interdependencies bringing with them greater vulnerability to external shock. The new model thus addresses a wide range of security risks, from terrorism through accidents to natural disasters. It involves a broad range of organisations, in the public sector and beyond. Work at local level is the building block of preparedness. And there is a premium on inclusiveness and transparency.

The scale of this shift has been characterised as a move from "the secret state" to "the protective state".[28] It has at its heart the twin goals of joining up practitioners at all levels in the UK *and* joining practitioners with businesses and citizens in a campaigning partnership to improve preparedness. Such a move, with its inherent shift to "multi-level governance"[29] or "networked governance"[30] is not, of course, unique to civil protection. There are other social policy case studies. The key characteristics are brought out in academic analysis.[31] Military practitioners, too, would recognise much that is common with their world, from campaign planning[32] to mission command.[33] But with similar

26 Defined as being "about protecting the public from the effects of emergencies (whatever their causes may be). In addition to risk assessment and planning, it includes taking action before an emergency to mitigate its possible effects and responding in such a way that minimises the impact of the emergency on the public and speeds recovery from that impact." (Cabinet Office *The Future of Emergency Planning in England & Wales – A Discussion Document* (2001)
27 Castells, M *The Rise of the Network Society* (Oxford: Blackwell, 1996)
28 Hennessy, P *The Secret State: Whitehall & the Cold War* (London: Penguin, 2003) and "The British Secret State Old and New" in RUSI Journal vol 150, no 3, pp16-22 (London: Royal United Services Institute, 2005); Omand, D *The Secret State Revisited* (London: Royal United Services Institute, 2003). Available at: www.rusijournal.com
29 Pierre, J and Stoker, G "Towards Multi-level Governance" in Dunleavy, P, Gamble, A, Holliday, I and Peele, G (eds) *Developments in British Politics* 6 (London: Macmillan, 2000)
30 Benington, J and Hartley, J "Pilots, Paradigms and Paradoxes: Changes in Public Sector Governance and Management in the UK", International Research Symposium on Public Sector Management in Barcelona, 2001
31 Mulgan, G "Joined-up Government: Past, Present and Future" in Bogdanor, Vernon (ed) *Joined-up Government* (Oxford: Oxford University Press, 2005); Goss, S *Making Local Governance Work* (Basingstoke: Palgrave, 2001), pp97-99
32 Ministry of Defence *Joint Operations – Joint Doctrine Publication 01* (2004). Available at: http://192.5.30.131/linked_file/jdcc/publications/jdpd.pdf
33 Defined as "a style of command that seeks to convey understanding to subordinates about the intentions of the higher commander and their place within his plan, enabling them to carry out missions with the maximum freedom of action and appropriate resources" (MoD, JWP 0-01.1)

networking concepts now increasingly apparent in the broader security field[34] this essay focuses on key governance issues.

Accepting leadership responsibility

Civil defence quickly withered after the collapse of the Soviet Union. The emphasis fell on to work by local authorities and others to build plans and capabilities to secure the safety of the public in a range of essentially local emergencies. This shift was reflected in the residual actions of central government, restricted to the provision of brief guidance and limited sums of public expenditure.

Much of what had been used for civil defence was clearly life-expired. But, while it was clearly right to be rid of the superfluous *tangible* infrastructure of civil defence, the decision by governments during the 1990s to retreat from their *intangible* leadership role rather than update it to the needs of a modern networked society left four key gaps. There was no shared framework – by definition national in scope – within which to build a common endeavour. Its absence made more difficult the task of developing consistency so that pieces fitted smoothly together in an emergency. There were no structured processes for detecting and acting on emerging risks that could pose a severe challenge to society, many of which central government was best placed to see. And there was no ready mechanism for identifying and sharing knowledge of the way in which major emergencies could challenge societal interdependencies, generating the disruption of those essential services on which the smooth functioning of society is based.

The "millennium emergencies" (fuel protests and widespread flooding in 2000; the foot-and-mouth epidemic of 2001) exposed those gaps. Together, they provided the stimulus for a range of initiatives after the 2001 general election, which signalled recognition that it was no longer adequate to leave responsibility for building preparedness with individual government departments, where, even if it was done, work tended to be narrow in focus; synergies were not exploited; and, in the absence of challenge, issues risked being left under the carpet.

Thus the newly elected government made changes to the machinery of government, including the creation of a new unit in the Cabinet Office; new legislation was developed; new investment programmes were started; and substantial increases in funding were

34 Most powerfully as argued by Leon Fuerth, in "Strategic Myopia: The Case for Forward Engagement" in *The National Interest* no 83 (Spring 2006)

provided. A further, substantial stimulus towards reform was provided by the al-Qaeda attacks in the USA on 11 September 2001, and the resulting new "calculus of threat" that they ushered in, of "the desire of terrorists and extremists to cause casualties on a massive scale, undeterred by the fear of alienating the public or their own supporters"[35] – that is, a scale of jihadist terrorist challenge and, importantly, of consequence going well beyond that which the UK had experienced in 30 years of Irish terrorism.

Identifying scope

If the first key to success is providing leadership, the second is identifying who can contribute. Everyone has a role to play in building preparedness. State practitioners have responsibilities for ensuring public safety. Businesses can help to minimise impact through sustaining essential services. Individual citizens can contribute through involvement in voluntary groups. They can, too, help themselves and those around them. The potential scope of civil protection in 21st-century society is well recognised in some continental European states that have historically devolved governance structures coupled with relatively higher degrees of citizen participation. The need to "harness a genuinely national effort"[36] has, however, been less well recognised in the UK. As the Lessons to be Learned inquiry on the 2001 foot-and-mouth epidemic noted:

Whatever central government does and however well, it cannot defeat a major outbreak of animal disease on its own. It needs to co-ordinate the support and services of many others, including those most directly affected ... Wholehearted support for a common purpose depends on mutual trust and confidence ... [These] cannot be built by the independent actions of one side alone.[37]

Building involvement

A governance framework that mobilises this broad range of actors is clearly challenging to operate. It requires clarity of purpose, although this is, thankfully, easy to define – ensuring people's security, safety and well-being. It needs a readily understood framework that finds the right balance between central prescription, to ensure the necessary consistency of action, and permissiveness, to allow local solutions to be found to local challenges.

35 Butler, R et al *Review of Intelligence on Weapons of Mass Destruction – Report of a Committee of Privy Counsellors*, HC898 (London: Stationery Office, 2004), p125
36 Omand, D "Emergency Planning, Security and Business Continuity" in *RUSI Journal* vol 149, no 4 (London: Royal United Services Institute, 2003), pp27-31
37 Anderson, I et al "Foreword" in *Foot & Mouth Disease 2001: Lessons to be Learned Inquiry Report*, HC 888 (London: Stationery Office, 2002)

The government brought in new legislation – the Civil Contingencies Act 2004 – to provide part of that framework. The act seeks to establish a clear set of roles and responsibilities; greater structure and consistency; better communication; and a basis for performance management. It includes both functional and collaborative duties to achieve these goals, requiring those ("category 1") responders at the core of emergency response (such as the emergency services and local authorities) to undertake:

- **risk assessment** – to assess the risk of emergencies occurring and use this to inform contingency planning;
- **emergency planning** – to put in place emergency plans and exercise them to ensure they are effective;
- **business continuity management** – to ensure that responder organisations can continue to exercise critical functions in the event of an emergency;
- **public communications** – to make information available to the public in advance of an emergency, and to warn and inform the public in the event of an emergency;
- **information sharing** – with other local responders;
- **co-operation** – with other local responders to enhance co-ordination and efficiency; and
- **business continuity management promotion** – to provide advice and assistance to businesses and voluntary organisations about business continuity management.

The act also defines a group of co-operating bodies ("category 2" responders) who are less likely to be at the heart of planning work, but will be heavily involved in incidents that affect their sector (for example, utilities), who are required to co-operate and share information with other responders.

As far as the business sector was concerned, policy making around the act had carefully to consider the impact of market pressures – whether positive, in providing firms that engage in relevant planning with a competitive edge, or negative, in placing burdens on firms that do so. It thus had to find the right balance between, on the one hand, placing preparedness duties in law on the business sector that mirror those placed on public-sector bodies, and, on the other, the strong desire to reduce the burden of regulation on business.

In the end, the act did not place statutory business continuity duties on businesses, even those within the critical national infrastructure, but sought instead to encourage their voluntary engagement in preparedness work. Time and the trend data we are

gathering[38] will tell whether this was the right decision.

The challenge of gaining the involvement of the wider community is much greater. A first step was to reverse the legacy of Cold War secretiveness, and to establish a governance framework that gave observable permission to the involvement not only of public-sector practitioners but also of non-practitioners. Key components have been:

- the establishment of regional resilience forums in each region of England and Wales, and beneath them local resilience forums at broadly county level, bringing together not only governmental practitioners but also businesses, and voluntary and community groups;
- the creation, at both national and local levels, of mechanisms to engage the business community in either generic resilience activity or work focused on building preparedness for specific major risks (such as a flu pandemic); and
- the establishment of a concordat between local government, the emergency services and the voluntary sector covering their involvement in building resilience, underpinned by a duty in legislation on government practitioners to have due regard in their planning to the capabilities of voluntary agencies.

Building and sustaining relationships

Pivotal to the effective operation of the governance framework is clarity of understanding by all participants of their and others' respective roles, including the ability of some to set standards and boundaries. Much depends on "[t]ransparency, honesty and clarity about the purpose, the limits of what can and cannot be changed ... [and] what happens as a result".[39] That means that there are substantial issues of trust.

A basic level of trust between parties is clearly essential in any field of activity to sustain and deepen collaboration over time. In the context of civil protection, however, the need for trust goes deeper, inasmuch as the collaborative arrangements used and the personal relationships built in preparedness planning will be drawn on heavily in the response to a major emergency. Associated with trust are respect and credibility. Civil protection is a field populated by professions that continue to command both. Perhaps as a result, the chairmen of most of the local resilience forums described above tend to be senior police officers.

38 Most recently, Chartered Management Institute *Business Continuity Management Survey* (2007). Available at: http://www.managers.org.uk/client_files/user_files/Woodman_31/Research%20files/Business%20Continuity%20Management%20report%202007.pdf

39 Involve *People & Participation: How to Put Citizens at the Heart of Decision-making* (London: Involve, 2005)

Effective communications

Effective communications between those who choose to become engaged in preparedness planning are clearly a fundamental enabler. There is also a substantial need for communications with those who are not so engaged – the "general public" – so that they can receive and act on messages from practitioners that will enable them to secure their own safety in an emergency.

In an area that still carries the taint of past (civil defence) and present (counter-terrorism) secretiveness, the hurdle for public managers in carrying out communications activity is high. But it nevertheless needs to be done. "Cold calling" – starting citizen engagement in the face of a looming crisis – will result in less effective outcomes.

The resulting underpinning communications strategy has four key elements: to inform and desensitise, especially to strip away unnecessary "secrecy"; to demonstrate competence and coherence; to reassure and build confidence and trust; and to help build public resilience by instilling life-conditioning behaviour, before and after a crisis.

A key enabler is the provision of information that is as full, honest and candid as possible, allowing people, including via their social networks, to draw their own conclusions about the competence of response arrangements, hence allowing them to build confidence and trust. The (idealised) first end goal might be expressed as the public perceiving that: "We're prepared for emergencies, and I know my interests are being looked after." Atomised against the analysis above, this becomes: "There is a strategy; it is well thought through and coherent; it is being implemented by organisations working together; someone visible and accountable is in charge; and it is delivering real improvements." The second, again idealised, end goal would be the reciprocal of this – a public that is willing to say: "I am prepared. I know what I should do to take care of myself and others."

Our research suggests that the public can be split into several groups, for each of which a different approach is needed to achieve these ideal goals. It also suggests that the public is most appreciative of messages about *what* to expect and *how* to respond. As in other public policy fields, most interest is focused on issues that have a local resonance. In the civil protection field, that means local responses to local incidents, so that material from local councils that refers to local hazards and to familiar resources and channels of communications seems the most influential. Again, as in many other fields, research also offers a clear pointer on *who* should transmit the messages – respected and trusted practitioners, who have greater credibility than politicians or policy makers.

Conclusion

In all this work, there are two guiding concepts. The first is recognition of the implicit social contract between the protective state and its citizens. Citizens have an important part to play in securing their own and their neighbours' safety. They will, however, place their actions within a framework of two expectations of government – that it will manage effectively its part of the response; and that it will be honest in providing the information needed to allow people to take the steps necessary to maximise their own safety. As David Miliband put it in another context, the resulting shared governance framework should embody "shared expectations of what citizens will do for themselves and for each other, and shared understanding about what they can expect from government. Shared expectations that embody moral commitments and common values. Shared expectations that unite self interest and common interest."[40]

The second guiding concept covers the role of government, simultaneously enabling and constraining, adopting a facilitative, steering role that "rests less on its authority to make decisions and instead builds on its capacity to create the conditions for positive-sum partnerships and setting or changing the rules of the game to encourage what are perceived as beneficial outcomes".[41]

Or, in more operational terms:[42]

- *Clear long-term goals set by the elected government;*
- *A clear division of responsibility and accountability for achieving those goals with proper co-ordination at the centre;*
- *Maximum local flexibility and discretion to innovate, respond to local conditions and meet differing ... demands;*
- *And ... maximum transparency about both goals and progress in achieving them with proper scrutiny and accountability.*

40 "Building a Modern Social Contract", speech to the Together We Can conference (London, 2005). Available at: http://www.communities.gov.uk/index.asp?id=1122750
41 Stoker, G *Participation of Citizens in Local Public Life* (Strasbourg: Council of Europe Publications, 2000), p98
42 Ed Balls "The New Localism: Devolution and Localism in Public Policy – A View from the Treasury", speech to the Chartered Institute of Public Finance & Accountancy annual conference in Brighton, 2002. Available at: www.hm-treasury.gov.uk/newsroom_and_speeches/press/2002/press_55_02.cfm

Chapter 5

The comprehensive approach

Rear Admiral Chris Parry CBE, Director General of Development, Concepts and Doctrine at the Ministry of Defence

The comprehensive approach

Forecasters differ about the precise shape of the future, but almost all analysts, academics and commentators agree on one thing. The future – as well as being like the present, only more so – will, in broad terms, be highly volatile, extremely complex and characterised by challenge and change in every aspect of human activity and governance.

There are also clear indications that these levels of complexity will demand increasingly sophisticated mechanisms and processes in relation to crisis and conflict resolution. In order to manage these complexities, it is widely agreed that multidisciplinary approaches and the integration of all available instruments of power by states and institutions offer the best prospects for achieving favourable outcomes.

Historic experience and recent operational evidence suggest that the most promising way to address these complex issues is through a comprehensive approach – that is to say, "commonly understood principles and collaborative processes [between military and non-military agencies and organisations] that enhance the likelihood of favourable and enduring outcomes".[43] By implication, it involves a return to high-level decision making based on strategic principles.

This challenge is recognised by the UK government, but recognition is not resolution. Resolution of challenges to the international system relies on the judicious use by states, in support of their interests, of the three main instruments of national power[44] – diplomatic, economic and military – alone or together with other nations. In practice, any hope of achieving favourable, sustainable outcomes, especially in areas of doubtful security, will rely on both containing the symptoms of crisis and conflict and addressing the causes of instability, just as the physician attempts to cure the disease while, in the short term, providing analgesics to alleviate the accompanying pain.

However, used alone or out of harmony with other instruments and agencies of power and influence, the military instrument is a blunt instrument that can achieve specific objectives, but only contributes to lasting outcomes when integrated with other disciplines.

43 MoD UK definition – *The Comprehensive Approach*, joint discussion note 4/05 (MoD, January 2006)
44 In UK defence doctrine, three instruments of national power are acknowledged – diplomatic, economic and military; some states claim a fourth, information, but the UK view is that information enables activity in and between the diplomatic, economic and military instruments.

Challenges of application

All this appears self-evident. However, although the principles are simple, the implementation and application are immensely difficult.

In dynamic situations the military, like nature, abhors a vacuum and will rush to fill it if its own objectives are jeopardised by inertia. The momentum to develop the comprehensive approach has been increased because of experiences in Iraq and Afghanistan, where the military had to take the lead in several areas – governance, the economy and infrastructure and (in Iraq) public-sector reform – outside its proper traditional functions. This situation characteristically prevailed in those areas where the security situation did not allow more "comprehensive" approaches before the establishment of the provincial reconstruction teams (PRTs); the military had considerably more freedom of movement than personnel from other government departments and international organisations and were often the only human resources available for projects.

However, military personnel are generally, by education, training or temperament, ill-equipped to deal with these issues except by process of pragmatic adaptation. Furthermore, the development of networks and co-operative relationships with other agencies and international bodies was hampered by the frequent turnover of personnel and the six-monthly deployment of units. As a result, in the absence of a coherent institutional and structural framework and commonly accepted doctrinal practice, co-operation depended on the personalities in post at any one particular time.

At present, in Iraq and Afghanistan, there are indications that the comprehensive approach is beginning to demonstrate results, as commanders and their staffs absorb the very simple logic and encourage their partners to engage in collaborative planning and working. In particular, PRTs are beginning to encourage and reap the benefits of collaborative working between civilian agencies and military organisations in theatre, especially when collocated and with dynamic dialogue in relation to the achievement of "success" and de-confliction across all lines of development and activity.

Again, NATO experience (especially in the Balkans and with the International Security Assistance Force, ISAF, in Afghanistan) in harmonising multinational sensibilities, priorities and procedures has shown how different working cultures and regimes – both civilian and military – can be accommodated to produce a coherent basis for planning, decision and action. Indeed, ISAF headquarters is already implementing effects-based thinking, alongside structures and working cultures designed to stimulate and progress a comprehensive

approach with other government departments and an increasing number of international organisations.

In those areas of doubtful security, it may be that commanders and their staffs might still in future have to possess or acquire attributes that fit them for "comprehensive" direction and leadership in areas beyond those normally expected of the professional military, before handover in more settled conditions to appropriate authorities. In practice, often by default, this pro-consular trend has been evident already in Iraq and Afghanistan. Yet if UK armed forces are to undertake this role in certain phases of an operation, the full implications for education, training and the selection of commanders must be recognised and resourced.

What needs to be done

How can the situation be further improved and progress achieved? In the first place, the comprehensive approach desperately needs political championship and vocal support at the highest level. The comprehensive approach is the expeditionary equivalent of domestic joined-up government and should be promoted as such, both for its utility and obvious efficiencies. It is worth remembering in this context that "joint-ness" in the Ministry of Defence, although piously accepted and solemnly preached in principle, only really began to become a reality once a progressive chief of defence staff embraced the idea and let it be known that officers' careers depended on a cultural shift in their views and demonstrated practice.

In practical terms, a hub within government is required to implement the comprehensive approach at the strategic level and to set the standard for lower levels of engagement. Except in circumstances of grave national crisis, the present arrangements simply perpetuate the culture of stovepipe and fiefdom, which promotes an atmosphere of competition at the expense of co-operation. What is required is an organised, recognised and empowered authority capable of sustained decision and action along the lines of policy, together with control and direction of the resources available to contain or resolve a conflict or crisis. The formation and development of the Post-Conflict Reconstruction Unit (PCRU) has not yet fulfilled this requirement; mainly because it lacks authority, as the illegitimate child that its parents seem oddly reluctant to recognise and promote, but also because it is significantly underpowered and under-resourced.

The PCRU experience suggests that the level of authority for national strategic direction, executive authority and co-ordination of the comprehensive approach should reside

much higher, perhaps within the Cabinet Office (which at present does not have or desire the power or authority) and under the day-to-day direction of a senior minister: not necessarily from one of the main departments involved in the implementation of the comprehensive approach, but someone with experience of defence overseas policy. Only then will other government departments have an incentive to be more active in developing mechanisms for a fully integrated approach, whether or not they accept or like the MoD's position out in front – rather than in the lead – on this issue.

The comprehensive approach has gained momentum from being the civilian-friendly, acceptable face of the effects-based approach; structural and intellectual innovations have therefore benefited both approaches. There has also been steady progress in acknowledging the necessity for a comprehensive approach across government, and broad agreement on the principles underlying and underpinning the construction and implementation of collaborative mechanisms, communications and processes. Based on a bottom-up approach, the ministerial committee on defence and overseas policy's subcommittee on conflict prevention and reconstruction, or DOP (CPR), accepted the principles contained in the MoD's joint discussion note *The Comprehensive Approach*, and the Foreign & Commonwealth Office's Comprehensive Approach Working Group (CAWG) has started concrete work on how to take forward collaborative mechanisms.

"Comprehensive" theory – and participation - lies at the heart of the Permanent Joint Headquarters' joint venture series of exercises and is the basis for the extensive, well-resourced Joint Forces Command-led Multi-National Experiment 5, running for two years from March 2007. At the intellectual and conceptual levels, the Development, Concepts & Doctrine Centre has been pioneering and publishing innovative approaches to the planning and implementation of both the comprehensive and effects-based approaches, based on lessons and insights from operations, first principles and experimentation.

A problem of culture

If we are to build on and consolidate our experience so far, one of the most important areas for systemic improvement is the promotion of a strategic, comprehensive way of thinking across Whitehall at all levels. This is not simply a matter of planning and consultation, but a cultural understanding that decisions and actions in one area inevitably have influence to a greater or lesser extent in others.

At present, improvements are impeded by traditional loyalties, lack of understanding and a protective attitude to the preservation and influence, image and resources of individual

departments. Progress will depend on a range of collaborative projects and processes, including the production of a common vocabulary, agreed mechanisms for assessment, analysis and planning and an understanding of the very real differences in discrete working cultures and thinking communities.

The CAWG and the latest Development, Concepts & Doctrine Centre joint doctrine note have already initiated the process of harmonising a common lexicon and a basis for a common planning tool, but a great deal still needs to be done to encourage a way of thinking in each department that instinctively includes and considers all factors that affect a situation of national importance. This will be assisted and advanced by more networked solutions for promoting shared situational awareness and collaborative working, most of which are available and demonstrably effective in the commercial sector.

The comprehensive approach is also an opportunity to revive the lost art of strategy. The simple fact is that unless strategy – the harmonisation of political aspirations with the realities of military, diplomatic, economic and institutional capacity – is formulated and intelligently implemented for each complex situation, no amount of tactical excellence and operational sophistication is likely to prevail. Strategy needs to harness the successful orchestration of the instruments of national power, both alone and with other states, to manage not only the symptoms of challenges that will emerge in the international scene and within states, failed and otherwise, but also the causes and long-term consequences.

Diplomatic, economic (including development) and military activities need to be planned, co-ordinated and implemented together within a coherent strategic approach if sustainable solutions to crises are to be credible and favourable outcomes realised.

Does NATO have a role?

If one is searching for a truly "big idea", then NATO, as a proven political and military alliance, offers a suitable vehicle and opportunity for transforming itself into a strategic alliance based on the principles underlying the comprehensive approach. Indeed, the comprehensive approach could be a reasonable leitmotif for sustaining the momentum and focus of Alliance transformation, especially in the face of an array of potential transnational and regional crises arising from the consequences of climate change, globalisation and demographic imbalances and inequalities.

In the light of NATO's experience and continuing operation in Afghanistan and the

intention expressed at the Riga summit, it would, in combination with parallel work on incorporating and extending the effects-based approach, provide a firm basis for understanding and development for the evolution of Alliance instruments of power capable of engaging in the wider world. As such, it would also offer a coherent doctrine and junction box for the individual and collective integration of the military, diplomatic and economic instruments of Alliance power, a basis on which all member states could make a meaningful contribution (according to capacity and political will) and a formidable expression of its collective will.

The question might then be how this model would interface and interact with other major players, such as the World Bank, the UN, the EU or the G8, as the means for concerted diplomatic, economic and military activity. In all cases, however, each of these "global" strands would need to be planned, co-ordinated and implemented together, around a leadership that can determine the priorities, resolve resource issues and realise the outcome that is required. Perhaps the EU might find the comprehensive approach a suitable method of kick-starting or energising the European Security and Defence Policy.

The bottom line is that, without development of the comprehensive approach, the UK would be likely to eschew strategy and would be unlikely to meet political or public aspirations in expeditionary operations. Similarly, in the absence of a more coherent, streamlined way of integrating national strategy and resources, the military instrument of power is likely to be more heavily burdened and expensively used in dealing with the symptoms of an increasingly wide range of crises in the coming years whose causes and consequences will not be satisfactorily contained by incoherent government responses or by military means alone.

Finally, there is another compelling reason for implementing the comprehensive approach as quickly as possible, exemplified in two quotations:

Everywhere, they have established the rule of law, good government and provided welfare systems and schools. They have shown respect and protected the people from hunger and harm.

After this disaster, they are protecting us from the enemy, rebuilding our schools and hospitals, giving us enough money to feed our families and ensuring that everyone behaves themselves.

On the face of it, these look like two victories for the comprehensive approach. Indeed they are – but they describe, respectively and in the words of the locals, actions by the Supreme Council for Islamic Courts in Somalia and Hezbollah in Lebanon. Our potential opponents seem to be "doing" strategy and the comprehensive approach already.

Chapter 6

Resilience and complacency in the private sector

Dr Bridgette Sullivan-Taylor, Leverhulme Research Fellow at Warwick Business School, and Professor David C Wilson, Professor of Strategy at Warwick Business School, University of Warwick

Resilience and complacency in the private sector

A great deal of debate surrounds risks, hazards (man-made or natural) and national security. This chapter argues that an overlooked area of research and knowledge is the threat of terrorism to private-sector organisations. The preparedness of an organisation (via its managers) to assess and face such risks is crucial. Organisations in telecommunications, finance, pharmaceutical, transport and leisure industries (for example) form a significant part of the critical national infrastructure. They keep normal life going. A recent estimate concludes that 80% of the critical national infrastructure is owned by the private sector.[45] A critical question, therefore, surrounds the preparedness of such organisations for the threats of terrorism, however such a threat may present itself. To what extent are these private-sector organisations vulnerable, exposed and even complacent about the threats and hazards they face? We use the term "resilience" to cover these factors.

Key features of organisational resilience are listed in table 1.

Table 1: Key features of organisational resilience

- **Technical:** the ability of physical systems to perform to desired levels when subject to extreme stress.
- **Organisational:** the preparedness of managers to make decisions and take actions to reduce disaster vulnerability and impacts.
- **Resourcefulness:** the capacity of managers to identify problems, establish priorities and mobilise resources to avoid damage or disruption.
- **Rapidity:** the capacity of managers to meet priorities and achieve goals in a timely manner.

Senior managers and organisations vary widely in their preparedness for managing threats of terrorist activity. Furthermore, strategies formulated at an organisation's centre or headquarters might not be successfully transferred to and implemented in sub-organisations and branches throughout the UK, such as high-street branches of a retail chain. These considerations must influence the range and quality of strategic choices available.[46] Variations in levels of preparedness might arise from simple uncertainty as to the identity of a putative adversary, what their goals might be and, accordingly, what

45 Sir David Omand "In the National Interest: Organising Government for National Security", Demos annual security lecture, December 2006
46 Child, J *Organization* (Oxford: Blackwell, 2005)

decisions and actions might be necessary to ensure that the adversary's aims are not realised.

Preparedness might also be influenced by organisational culture, in the form of an inability to assess imminent dangers and pervasive vulnerabilities, and to prioritise risks. A terrorist attack might reasonably be perceived as a hazard – defined as the potential for harm – but without the competence to assess carefully the likelihood of such an attack, it cannot be said to constitute a risk. With that in mind, how much effort should managers make to ensure that their organisational culture has the capacity to identify hazards, prioritise threats and act accordingly?

Little research has, to date, been conducted into how managers deal with uncertainties created by the threat (and sometimes the actuality) of terrorist attacks, despite the fact that coping with uncertainty has been an enduring theme in organisation theory.[47] Coping with the terrorist uncertainty, however, has been under-explored and under-researched. One result is that practitioners typically respond either defensively ("We have done all that could reasonably be expected of us") or fatalistically.

Indications from a study of six private-sector organisations in the UK[48] are that some organisations are ill-prepared to face the hazards and risks of terrorism and that some managers have developed a relatively complacent attitude to the threat ("It won't happen to us").

Variations in preparedness arise from factors such as a lack of knowledge about who the enemies are, what they want and what actions might stop them. They also arise from more organisational factors, such as an inability among senior managers to assess imminent dangers, pervasive vulnerabilities and prioritise risks. A terrorist strike may be a risk, but how likely is it to happen? How much effort should private-sector managers make to ensure that their organisation has a strong capacity to anticipate, identify and act upon such threats?

Increasing resilience in private-sector organisations is an urgent need in a national

47 Thompson, JD *Organizations in Action* (New York: Sage, 1967); Aldrich, HE *Organizations & Environments* (New York: Prentice-Hall, 1979); Pfeffer, J and Salancik, G *The External Control of Organizations: A Resource Dependence Perspective* (New York: Harper & Row, 1978); Cummings, S and Wilson, D *Images of Strategy* (Oxford: Blackwell, 2003)
48 Sullivan-Taylor, B and Wilson, D "Rare Events, Uncertainty and Organization: Sensemaking and Theories of Action in the Perceived Threats from Terrorism", paper presented at the 22nd EGOS Colloquium, Bergen, Norway, 6–8 July 2006

context where a primary requirement is to anticipate and take action to enable risks to be managed (and new opportunities seized to anticipate them). Managers in private-sector organisations have the opportunity to build a more organisationally proactive, effective and informed stance toward terrorism. This must be seen as part of the wider context of anticipatory actions by governments to reduce risks and increase the overall levels of national security.

The sample comprises six organisations from the UK/EU international leisure and travel sector, which have high potential exposure to threats of terrorism. The study used in-depth interviews with senior managers in six different organisations at two different time periods (2004 and 2006) in order to record any changes to management perceptions and practices relating to risk after three key terrorist attacks: 9/11, 7/7 and 10/8.

The six organisations are located upstream and downstream in the UK tourism sector supply chain. The three upstream organisations are a catering supplier to the airline sector, a UK airport and a low-cost airline, and the three downstream organisations are a large travel organisation, and two high-profile arts and entertainment organisations based in London. The organisations studied are listed in table 2.

Table 2: Organisations included in the preparedness study

- **A supplier to the aviation sector:** one of the largest UK suppliers of retailing and catering services for airports and airlines.
- **A low-cost airline:** based at a regional UK airport, offering no-frills airline and related travel services.
- **An international tour operator:** a leader in the UK-inclusive holiday market, operating resorts and travel agencies, servicing over 40 holiday destinations.
- **An international airport:** one of the UK's fastest-growing regional airports, with over 6 million passengers travelling on domestic and international flights.
- **An international convention centre:** one of Europe's largest multi-arts and conference venues, providing art, music, film and theatre.
- **An international arts and entertainment centre:** an integrated entertainment complex providing concerts, dance, performances, films, literature, education and the visual arts.

Findings

Managers in the convention centre perceived other risks to be a greater threat to them than those presented by the uncertainty of terrorism. Perceived high-risk decisions

revolved around the content and type of work commissioned and presented (rather than the threat of terrorism). Managers also perceived other sources of uncertainty to be more important than the threat of terrorism, singling out the latest foot-and-mouth epidemic in the UK as an example. In this case, uncertainty was primarily perceived as variations in the flow of tourists into the country and region and the related fall in demand for conferences and events. The arts centre interviewees also did not perceive the highest levels of uncertainty to be associated with the threat of terrorism.

Managers in the aviation sector viewed the highest levels of uncertainty to be potential risks from terrorism, since these can have devastating effects on their business (as well as their passengers). For example, organisations supplying food to airlines recognise that introducing poison or a bomb on board a plane via the supplied cabin food is more probable than a terrorist getting on board as a passenger. It is simpler to infiltrate the food preparation areas than the plane itself.

Wider variations occur across the sample organisations when looking at practice. Organisations that supply the aviation sector consumables such as catering have traditionally adhered to strict quality standards and risk audit processes. There is always the danger of terrorists trying to poison airline food. Some airlines insist their suppliers comply with their standards of security. For example, British Airways not only secures the site, but also ensures final checks are conducted. Department for Transport representatives also visit unannounced to try and get access to the kitchens (to find any security loopholes).

No-frills airlines prioritise the threat of terrorism, but rely on other organisations a great deal for security procedures. Although they reduce exposure to risk by not providing a full catering service in-flight (thereby reducing the likelihood of any catering-related security breaches), they nevertheless rely entirely on local airports to manage rigorously other security procedures (passenger checking and profiling). They are highly dependent – and dependency increases risk.

International tour operators rely upon information from the British government regarding travel to particular overseas destinations to determine whether or not to continue to service particular destinations. The Foreign Office travel advisory service, therefore, has a significant influence on travel to particular destinations, directly affecting the viability and success of some key tour destinations. The problem is that this information is not always up-to-date or accurate. One manager observed how British Airways and Air France

were forced to cancel many planes travelling into the USA on the basis of faulty American intelligence, causing considerable disruption to the airlines and their passengers.

In the arts and entertainment sectors, economic uncertainty was viewed as key. Implementing practices to counter the threat of terrorism were problematic. Largely this was because a tight security policy was felt to have a deleterious effect on overall business performance. The economics of business took priority over managing security.

Principal findings

Organisations need to be more *resilient* to the threat of terrorism; managers of organisations need to avoid complacency and ensure they can identify problems, establish priorities and mobilise resources to reduce risk. Although the threat of terrorism gets almost daily high-profile exposure in the media, boardrooms and decision makers in organisations appear not to prioritise strategies to deal with possible threats. For example, no-frills airlines rely almost exclusively on airports to exercise security checks and regulations. Entertainment centres prioritise economic activities, adopting an almost fatalistic attitude to possible attack once obvious risks such as underground car parks have been averted.

Information on levels of threat (from governments and other sources) seems to be both partial and occasionally confusing, making the lives of decision makers in private-sector organisations even more difficult. This latter point emerges strongly in the context of the 7/7 and 10/8 threats. Both airports and airlines need increasingly precise information from government about the level and type of threat. Managers complain that they do not always receive sufficiently precise information, other than the level of security risk on a five-point scale.

The key question for private-sector managers is whether the right levels of security are being applied. As one interviewee from an international airport said: "Security measures are being decided by experts in London; but they don't have to implement them." More effective and efficient communication would seem an obvious need.

The no-frills airline had become increasingly pragmatic and focused following 7/7 and 10/8. Senior managers felt they were clearer about the type of threats facing airlines, which were not necessarily those faced by other transport organisations. In the words of one interviewee: "It is not attractive to a terrorist to bring down a plane and its passengers way out over the sea; the plane and its passengers disappear, but no one will

see the spectacle on the news and that is what the terrorists want. That's why a bus is perfect for the spectacle." A danger here is one of over-certainty on the part of managers. They assume they know more about the nature and type of risks faced on the basis of past experience (their own and that of other organisations). The fallacy of relying on the past as a source of certainty has been well documented by many organisation theorists.

Paradoxically, airline managers were aware that the airline was also useful to terrorists. One interviewee estimated that around 5,000 passengers a year travelling by that airline could be terrorists on the move. This utility value (to the terrorist) was assumed to protect the airline (to an extent) against attacks. At more operational levels, managers were making small changes, such as removing Union Jack flags from the fuselages of aircraft, since managers perceived threats to be targeted against the country (the UK), rather than specifically against the airline. The general attitude of interviewees, however, tended to be a little complacent. They felt greater knowledge and experience gained by each threat provided greater certainty for the future.

In contrast, airport managers had changed or intensified security procedures since 7/7 and 10/8. One reason for intensification was that layers of security and the ways in which they are applied in an airport are at a level defined by the government, and not by the airport managers. 10/8, in particular, emphasised x-raying and body searches, as well as restricting items that could be carried as hand baggage.

A result of the intensification of body searches was an increase in security staff illness due to backaches and related problems. As one interviewee explained, "Body searches are very labour intensive ... staff go sick with back problems ... we cannot replace them fast enough ... we cannot keep up such a level of security in the long term." The projection was that the airport might have to employ around 15-20% extra staff. The cost implications of this would be significant and would have to be weighed against the benefits of tighter security and fewer passenger delays.

The key difference between the airport managers and the no-frills airline is that airport managers were not trying to narrow down or specify the type or nature of any threat. As one interviewee said, "Just because it was liquids last time, there is no reason to suppose it will be the same next time ... it could be completely different."

The relationship between airport and government was considered to be unsatisfactory. In particular, interviewees highlighted the question of new technology and its purchase

and implementation (in this case new body scanners). Most interviewees argued that the government's view was that they don't pay for security in airports, "whereas our argument is that [they] should, because it's a national threat and therefore needs a national response". Waiting for government approval to use new equipment was also given as a barrier to implementation, especially if the equipment had been used successfully in other contexts (such as border controls in violent parts of the world).

Inevitably, costs were the drivers of decision making. Airports do not make the margins that airlines can achieve. Charging for extra security thus becomes a problem. Who pays? Airlines argue that an extra 10p per passenger on the ticket price could be a disincentive to travel. Airports say they shouldn't have to pay these costs. One suggestion from airport interviewees was to create one large security force (instead of the existing immigration, customs, police and airport security staff), "giving potential terrorists less chance to duck and weave as they go through the various checks". But it was felt that government and the agencies themselves would resist the creation of a broader security force, since it would be against their interests to lose their existing expert powers.

Preliminary interviews in other sampled organisations indicate that managers were prepared to meet the minimum standards for security investment to meet regulatory or consumer pressure and requirements. However, they wanted to achieve a balance between security management and consumer experiences, so were not prepared to impose extensive security-checking procedures and systems over a long period. Convention centres, for example, still prioritise the commercial aspects of their businesses over the security aspects.

Conclusion

Businesses need to take steps to protect themselves and their staff from the threat of terrorism. There is a need to dispel the myth in some organisations that security is a hindrance to business. There is also the need to beware of overconfidence in existing organisational capabilities, which appears to lead to an over-complacent orientation toward threats and risk assessment. Our future research agenda will address these issues in a wider sample of private-sector organisations.

Prioritisation is a key factor in the execution of strategic decisions. Managers who consistently prioritise other factors (such as profit or cost reduction) expose their organisations to greater risks. Future research needs to examine how managers *perceive* threats of terrorism as well as assess the *preparedness* of organisational systems and

processes to cope with the uncertainties posed. How much and what type of information is accessed, as well as organisational cultures (flexible versus bureaucratic), can have an impact on preparedness.

Finally, there is a pressing need to assess the *capacity* of managers to act in the face of threats, and to examine the extent to which existing relationships (such as those between government and business organisations) present barriers to innovation and development in dealing with the threats of terrorism.

References

Aldrich, HE *Organizations & Environments* (New York: Prentice-Hall, 1979)

Child, J *Organization* (Oxford: Blackwell, 2005)

Cummings, S and Wilson, D *Images of Strategy* (Oxford: Blackwell, 2003)

Miller, S, Wilson, D and Hickson, DJ Beyond Planning: Strategies for Successfully Implementing Strategic Decisions in *Long Range Planning* 37 (2004), pp201-218

Sir David Omand "In the National Interest: Organising Government for National Security", Demos annual security lecture, December 2006

Pfeffer, J and Salancik, G *The External Control of Organizations: A Resource Dependence Perspective* (New York: Harper & Row, 1978)

Sullivan-Taylor, B and Wilson, DC "Rare Events, Uncertainty and Organization: Sensemaking and Theories of Action in the Perceived Threats from Terrorism", paper presented at the 22nd European Group for Organisational Studies colloquium, Bergen, Norway, 6-8 July 2006

Thompson, JD *Organizations in Action* (New York: Sage, 1967)

Section III: Technology and the private sector

Chapter 7

UK policy for defence research and technology

Professor Phil Sutton, Director General of Research and Technology at the Ministry of Defence

UK policy for defence research and technology

Within defence research and development (R&D), the current emphasis on science and technology (S&T) has its roots in the early to mid 20th century and particularly the First and Second World Wars. By this time, the physical sciences had made great leaps forward, including an understanding of electromagnetism, wave mechanics, atomic and molecular structures, the forces that bind matter together, quantum mechanics and relativity.

These scientific advances enabled new technologies to be developed and applied, for example in materials, precision manufacture, process control, high-power electricity and electronics. These in turn enabled the inventors and innovators of the time to devise electric motors, the internal combustion engine, radio communications, radar, the jet engine, and stronger, lighter and more complex structures for aeroplanes, ship hulls and land vehicles.

Furthermore, these same scientific advances opened the doorway to space, in terms both of exploration and of the provision of satellites for communications, Earth observation and navigation. The same period also saw a dramatic growth in the understanding of biological systems, with a profound transformation in our knowledge of the microbiological world as well as of the human body and its functions.

The greater understanding of science, linked to the ability to translate scientific understanding into new devices, systems and procedures, occurred at a time when warfare had reached global proportions. The extent to which S&T affected the political aspirations of leaders seeking to extend their power is outside the scope of this paper, although there can be little doubt that the period saw an unparalleled growth in the technology of warfare driven by ambition and the struggle for national survival.

But the defence environment of the time was very much focused on interstate war. Here "victory" was expressed as the dominance of one state over another, resulting in either occupation or the imposition of a "puppet" government firmly in the pocket and under the control of the victor.

Today the talk is much less of war and more of security threats. Of course the traditional notion of interstate war, with armed forces fighting openly on land, in the air and at sea, has not disappeared, nor by some accounts is it likely to.[49] But the immediate concerns

49 See, for example: Gray, CS *Another Bloody Century: Future Warfare* (London: Weidenfeld & Nicolson, 2005)

relate to the clearly defined actions that threaten to undermine the values and habits of normal daily life in Western societies, without having to go to the trouble of invasion and occupation, as in the past. In this new environment, the notion of victory is harder to define, since in many respects it follows the pattern of a journey, not a destination. Many of those who threaten our security seem to be seeking to achieve particular effects. When objectives are given, they appear less clearly defined and specific, perhaps reflecting the many different agendas of those involved.

It was once possible for a state to be aware of a conflict on the other side of the world, yet to ignore it because it would have no direct impact on home interests. But today states and peoples are far more closely interconnected, via the global economy, greater individual mobility, communications and by a common natural environment. This greater interdependency has meant that both the threat and the response to it have extended their reach.

Whilst we have moved from the threat of global war (albeit perhaps temporarily) to the threat of local instability leading to wider impact and the threat of global terrorism, there is the looming impact of major changes in the Earth's climatic environment. How this latter factor will affect the security situation is unclear, but it is widely recognised that conflicts related to scarce resources and currently fertile land becoming barren or uninhabitable are likely.

Consequently, in many respects the scope and nature of the threat to the UK and its interests is more complex and diverse than in the past. This shift is likely to become more apparent, particularly as the availability of technology means that adversaries not constrained by the processes and moral values that characterise the major industrial nations will continue to adapt their use of technology within timescales that are short compared with those of the Cold War era. In such a situation it is critical that all UK government departments work ever more effectively with the wider private industrial and technical communities, and do so in a manner that is agile, responsive and where possible predictive to the changing security environment. Furthermore, to achieve its security needs, the UK (or any other nation) cannot work in isolation. Global problems demand global solutions.

In all this, the role of S&T will be profound. Science and technology is an important feature both of the likely threats and of the means to counter them. The UK's success in military operations, particularly since the Second World War, is without doubt due in large measure, albeit not exclusively, to the effective use of S&T. The skills and abilities of UK

military personnel have resulted in armed forces that are rightly respected throughout the world for their professionalism and ability. But there can be no doubt now, perhaps more than ever, that S&T not only can provide more effective means to achieve operational success but also, if used responsibly, can do so in a way that minimises the risk to human life and the wider environment. This should be contrasted with the actions of those responsible for many of the security threats we face, where modern and widely available technology is used with the apparent aim of large-scale and indiscriminate destruction and loss of life.

The role of science and technology in the threat environment

It is worth noting that current threats operate broadly at two levels: those based on advancing personal gain (for example, theft of some sort), and those linked to some form of political or more generally "group" objectives. S&T plays an increasing role in both areas. However, the former is very much a criminal issue, and whilst in many respects a serious threat to our individual and collective security, it is outside the scope of this paper. Turning to the latter, we find that the nature of security threats seems to be to achieve specific effects. But in treating this class of security threat, it is also important to address those activities that underpin the wider group objectives, such as fundraising via the narcotics industries and terrorist training.

A particularly important factor is the wide availability of the products of S&T. Twenty and more years ago, the pace and nature of S&T were largely dominated by defence R&D in a Cold War world. That is most certainly not the case now, since consumerism demands new products on a timescale often measured in months. The global consumer economy, stimulated in particular by what is generally referred to as information and computer technology (ICT), continues to have a profound impact on all aspects of society.

For the purpose of this discussion, ICT is taken to include global and local real-time communications including text, audio, imagery, video (all linked to a vast store of information of variable authenticity), remote sensing (from satellite to hand-held digital video cameras, low-light cameras and thermal imagers), data capture, storage and processing, displays and human-machine interfaces.

Amongst the resulting sophisticated products which are widely affordable are satellite communications systems, video games, audio-video entertainment and networked computers, as well as the underpinning technologies such as microelectronic chips, materials, software, long-life, small but energetic batteries and micro-mechanical sub-

systems. A particularly important technology that is widely available is the internet (interestingly, a by-product of defence) and the world wide web, enabling access to information in a largely unregulated and uncontrolled manner.

Overall, this situation means that highly capable and affordable technology is available to almost anybody, and as such is no longer exclusively the tool of financially and industrially strong nations. The easy access and affordability of technology enables a much larger array of threatening groups and individuals to achieve their desired effects. This is most clearly and dramatically evident in the case of the wide array of improvised explosive devices (IEDs) employed against the UK and its allies. Such devices are often associated with civil technology to detect their target or to be detonated. Delivery of the desired effect also often involves recording events on video, to be used in a manner and at a time to exert influence at a local or global level. Furthermore, taking the case of terrorists, to achieve whatever effect they seek it is not necessary for them actually to complete an attack; the significant risk of a security threat can result in major disruptions, as has been demonstrated on many occasions with the air transport industry.

Whilst civil sector S&T is, without doubt, a major contributor to insecurity and vulnerability (and, as is described later, the response to it), the defence-specific S&T is still highly important. Putting nuclear issues to one side, stealth, electronic warfare, sensors that operate effectively in the presence of high-power jamming, precision-guided weapons, and armour protection at the individual and platform level are examples of just some of the areas that have a strong defence-specific S&T component. Many nations are engaged in producing military equipment of significant potency, equipment which through a variety of means appears in the inventories of those that our armed forces may one day have to face.

It is true that even these defence-specific systems are underpinned at least in part by civil technology (such as microelectronics, computers, displays, solid-state devices and novel materials). However, the complete system concept is very much defence driven, and would not have happened had it not been for a wish to achieve some form of military superiority against a potential enemy.

The role of science and technology in UK defence

Faced with an ever more complex security environment, the UK Ministry of Defence is determined to use its resources to best effect. The Defence Industrial Strategy[50] (DIS) set

50 MoD *Defence Industrial Strategy* (December 2005)

out how the MoD intends to respond to the current and future environment and the implications for its relationship with industry in particular.

Amongst other things, the DIS stressed the importance of taking a through-life capability management (TLCM) approach to delivery of military capability. Emphasis is to be given to the delivery of affordable military capability, recognising the dynamic nature of the threat, and to the opportunities offered by new technology, by designing equipment enabling an agile response to the changing threat environment, for example by better technology insertion. TLCM gives emphasis beyond initial capability when equipment first enters service, to take a whole-life cost view which means more cost-effective supportability.

A critical consideration in the delivery of military capability is the ability to work effectively with allies. This has impact at all levels of command, and requires UK C^4I (command, control, communication, computers and intelligence) processes and systems to be able to interoperate with those of its allies. This does not require the UK to have the same systems as its allies, but it does require commanders and operators to be able to pass and receive information across the various systems. Interoperability also extends beyond information systems and includes any aspect that might affect an allied force acting as a coherent whole.

As part of the DIS, the MoD has launched the Enabling Acquisition Change[51] programme. Through a number of work streams – including the establishment of a single defence equipment and support organisation, TLCM, people skills, behaviours and R&D – the programme seeks to achieve a major transformation in defence, focusing in particular on TLCM and the relationship between the MoD and industry.

Following the DIS (and as a specific target presented in the DIS), the MoD published its Defence Technology Strategy[52] (DTS), in which it identified its priorities for research and development. In so doing, it described those areas of S&T where the UK believes it must have a depth and breadth of capability in order to achieve operational sovereignty, as well as those areas where it believes international research collaboration represents the most effective way ahead. For example, research on topics of direct relevance to interoperability are high priorities for international research collaboration.

51 McKane, T *Enabling Acquisition Change* (MoD, May 2006)
52 MoD *Defence Technology Strategy* (October 2006)

Some of the key messages in the Defence Technology Strategy are as follows:

- The quality of military equipment is highly correlated with absolute R&D investment (no other factor correlates anything like as well).
- The benefit in terms of equipment quality depends equally on R&D investments made about 20 years before going into service (the research phase) and on those made five years before going into service (the development phase).
- Innovation is critical to achieving effective military capability.
- Whilst innovation is necessary at all levels within the equipment supply chain, there is a need to stimulate greater innovation and inventiveness at the earlier stages of R&D.
- The MoD needs access to highly capable scientists and engineers, within both government and the private sector.

As a consequence of the findings and conclusions of the DTS, the MoD has already launched a number of initiatives to stimulate greater innovation and inventiveness within the S&T community. For example, it launched its Competition of Ideas[53] and a Grand Challenge,[54] both aimed at stimulating interest in important defence S&T topics, particularly from organisations not traditionally part of the defence supply chain. The MoD is also in the process of launching fellowship schemes with the Royal Society and the Royal Academy of Engineering, as well as initiating a number of doctoral research opportunities.

Yet underpinning both the DIS and the DTS is a drive for wider engagement between the public and private sectors. A key objective in publishing the DTS is to give industry visibility of the MoD's priorities to help industry focus its own R&D spending so that the total UK defence R&D investment can deliver greater benefit. The benefit needs to be in terms of both improved military capability for the UK armed forces and commercial benefit for industry.

A key question, then, is how should government and industry work together to mutual benefit? As stated above, there is a critical need for innovation, agility and flexibility. Yet our current approach to applying S&T innovation to defence problems, in all but a few special cases, is still very much geared to the Cold War era, and is characterised by what appears to be surprisingly long acquisition timescales.

53 Competition of Ideas launched October 2006; www.ideas.mod.uk
54 Grand Challenge launched November 2006; www.challenge.mod.uk

The answer is not for government simply to throw money at the problem. Whilst more funding could speed things up, perhaps by creating more S&T options matured to an off-the-shelf state, in many respects this would simply be a distortion of the current way of researching, developing and acquiring elements of military capability. It could result in a more extensive equipment and service inventory, but would not necessarily be any more agile or flexible to fast-changing needs. The arrangements by which government can work with the suppliers of solutions to military capability need to be adapted if they are to be effective and efficient.

Work is under way involving the MoD and industry building on the DIS to identify such a model. Whilst there are no conclusions or firm proposals yet, characteristics of a more effective model might include:

- more emphasis on stimulating innovative and inventive solutions to current and anticipated capability needs by engagement of a wider R&D supplier base (including those areas traditionally outside defence);
- making defence S&T an exciting and worthwhile business opportunity for organisations with creative flare and the ability to make a positive difference to UK defence;
- greater openness by the MoD about its priorities (in a manner consistent with national security), constraints (including financial) and, critically, its capability shortfalls (including those areas where no solution is apparent);
- acquisition processes that recognise the benefits of an "80%" solution on time (or early) and within budget, but with design flexibility for frequent, easy and cost-effective upgrade/technology insertion (for instance as part of the routine service schedule but noting the implications for training and so forth);
- setting aggressive targets for delivery time of critical military capabilities;
- more effective means to transform new technology of clear potential benefit quickly into service – this requires more joint working and funding between the MoD and industry from research through to application;
- industry to open up its supply chains and to encourage innovation and inventiveness at all levels;
- avoiding early design freeze that forces out the opportunities to exploit new technologies available, for example from the civil sector;
- the MoD and industry to force out behaviours and processes that lead to cost escalation (which reduces the budget and hence leads to major knock-on effects with other programmes);

- system designs that are attractive for export but do not compromise UK military capability or effectiveness.

Conclusion

This paper has set the scene for the research and development of defence science and technology (S&T) by considering how S&T represents both an opportunity and a threat for the UK and its interests. It concludes that S&T will continue to be a major factor affecting national and global security, and that the way ahead must be to give greater emphasis to more innovative, inventive, agile and flexible exploitation of both civil and defence-specific S&T.

This change of emphasis will require a more effective and mutually beneficial relationship between government (particularly the MoD), industry, our international allies and the S&T supply base in general. This relationship will be enhanced significantly by a new business model for defence in the UK. Under the auspices of the Defence Industrial Strategy, work is already under way both in the form of the Enabling Acquisition Change programme and in the identification and development of a new model for relations between government and industry. But the process of change is at an early stage and there will be a need for an energetic commitment from all stakeholders if the necessary improvements are to be achieved, and in a timely manner.

Chapter 8

Research, technology and UK national security

Professor David Kirkpatrick, Emeritus Professor of Defence Analysis at University College London

Research, technology and UK national security

It is "a truth universally acknowledged" that in the summer of 1940 the UK was saved from defeat and occupation by its successful application of aircraft and radar technologies, as well as by the courage and skill of its airmen and the fortitude of its population. It is almost equally well known that other military technologies made significant contributions to the Royal Air Force's strategic air offensive against Germany and to the Royal Navy's protection of seaborne supply lines. During the Cold War, NATO planners recognised that a Soviet offensive through western Germany could only have been halted if NATO's out-numbered forces had superior equipment, derived from a leading position in some key military technologies. During and after the Falklands conflict of 1982 and the Gulf War of 1991, the Ministry of Defence's chiefs of staff appreciated that the results of British defence research, accumulated over preceding decades, were necessary for the urgent upgrading of their armed forces' equipment, and contributed to quicker victories at less cost in UK blood and treasure.

But in the 1990s, other parts of the MoD were seeking economies, to provide the expected "peace dividend" following the end of the Cold War. Service and civilian personnel numbers were cut (by about a third in both cases) and equipment procurement was reduced, thus decreasing employment in the UK defence industry. It was judged that the MoD's annual defence research budget should bear its share of the cuts, although in fact the scale of research needed to support the MoD's equipment programme is virtually independent of the size of the armed forces and depends on the diversity and sophistication of the equipment that they operate. Thus the reality was that research could be safely cut only if the UK government decided concurrently that its armed forces should forgo one or more of their major roles.

However, this reality was ignored and the MoD's annual cash budget for defence research fell by half through the 1990s;[55] its fall in terms of real resources (for example, scientific man hours) was even more severe. The MoD trusted that this reduction would be at least partially offset by greater expenditure on research within the UK defence industry, and by changes in the management of its own research programme (initiatives such as package management, competition for research contracts, and agency status for government laboratories). In the same period the MoD's annual budget for the development of national

55 House of Commons defence committee, *Defence Research*, HC 616, ninth report of 1998-99 session (London: TSO, 1999), fig 3

and collaborative defence projects fluctuated as various projects moved through their development cycles, but it remained roughly constant in cash terms (masking a reduction of about a third in purchasing power).

Research and development

Defence research and development are often inappropriately aggregated together as R&D, but they are in fact two distinct and complementary activities.

Defence research consists of original theoretical or experimental investigations to gain new knowledge of a particular technology, which may be exploited to enhance some military capability. All defence research is accordingly classified as applied research in OECD terminology, but it is convenient to divide it into work that can be exploited within the next decade and other (strategic) work that is unlikely to be used until later. The results of such research are generic and may be applied to various different defence projects.

By contrast, development is the exploitation of several synergistic technologies to create new defence equipment, or to enhance the cost-effectiveness of existing equipment, by applying the knowledge gained from defence research. The development of a defence project involves a suite of interrelated and interactive processes (project definition, detail design, and testing and evaluation), which are almost all relevant only to the new equipment being developed. Some of the resulting experimental data contribute to the generic database of defence technologies, but many aspects of development work are virtually routine and involve no appreciable novelty, so it is misleading to regard all development expenditure as enhancing knowledge of defence technologies.

Any nation investing substantial resources in the acquisition of defence equipment should do sufficient research in the relevant technologies to become an "intelligent customer" and thus become knowledgeable enough to ask critical questions of its suppliers, and to understand the answers. An ill-informed government may be overcharged by rapacious contractors (national or foreign) or their agents. The scale of research needed to support prudent acquisition is related to the range and complexity of the technologies embodied in the equipment within the nation's future acquisition programme, and particularly to the mission-critical and/or immature technologies involved.

Equally, any nation wishing to sustain a national defence industrial base must fund sufficient additional research in the technologies related to its national contractors'

products to enable those contractors to design and produce new defence equipment projects that will be effective on a future battlefield (and, ideally, will be competitive in the international market). Such expert design and production capabilities demand sufficient knowledge to generate solutions to any problem encountered through the projects.

Since defence contractors are notoriously reluctant to commit their shareholders' funds to long-term research or to development of equipment projects whose success depends on a few fickle customers, the nation must also fund contracts for the development, manufacture and support of such equipment with its national contractors. But the development of new projects will inevitably be unduly difficult and expensive unless the nation has previously done sufficient research in the relevant technologies to bring them to the appropriate readiness levels, and thus reduce the risks to the projects' target performance, cost and timescale.

It follows that timely and sufficient research is essential to the intelligent acquisition of defence equipment, and that a national defence industrial base must be supported both by additional research in the technologies that the national industry hopes to exploit and by an uninterrupted stream of development, production and support contracts for each class of defence equipment produced. Without such government support, the defence industrial base would be unable to sustain acceptable scale and profitability.

Acquisition reform

In recent decades successive UK studies, from ACOST[56] to AeIGT,[57] have expressed concern that the MoD's adoption of international competition in the 1980s was eroding the UK's defence industrial base whenever British defence contractors lost competitions to their foreign rivals, and that the decline in MoD expenditure on defence research was endangering the future competitiveness of the UK's remaining defence contractors.

The UK's principal military allies and commercial rivals had generally continued to discriminate against imported equipment and had (wisely) sustained or increased their defence research budgets after the end of the Cold War, thus giving their defence contractors a competitive advantage relative to those in the UK. The USA in particular had invested heavily in battlefield digitisation and network-centric warfare, evolving into the

56 Cabinet Office *Defence R&D: A National Resource* (London: HMSO, 1989)
57 *Aerospace Innovation & Growth Team Report*, unpublished (July 2003)

revolution in military affairs, to provide its armed forces with vastly enhanced capabilities in conventional warfare, and since 9/11 had dramatically increased its defence research budget to address the new threats of asymmetric warfare.

In response to increasingly strident pressure from the UK defence industry, and driven by its own concerns that in some future crisis a depleted UK industrial base would be unable to modify equipment in service with UK armed forces, the MoD has changed its acquisition policy. The 2005 Defence Industrial Strategy[58] (DIS) envisages the creation of long-term partnering agreements with designated British prime contractors for the supply and/or support of the classes of equipment within the contractors' areas of expertise, and the relegation of on-going competition to lower levels in the supply chain.

The DIS also included an MoD commitment to sustain onshore UK technological and industrial capabilities for the upgrading and support of key defence systems, in order to retain UK operational sovereignty. To create such capabilities on any imported equipment, and allow the MoD or its chosen contractor to act as local design authority, the foreign supplier must be persuaded that its intellectual property rights (IPR) will be protected, and its parent government must be assured that the MoD will prevent any unauthorised technology transfer to a third party.

Advocates of British defence self-sufficiency have interpreted operational sovereignty as the ability of the UK to undertake an independent military operation, even when some of its trading partners disapproved strongly enough to embargo their usual supplies of defence goods and services. A policy of onshore control of a greater proportion of the MoD's increasingly globalised supply chain would favour British defence contractors, but (even if it were affordable) it appears inconsistent not only with the MoD's declared policy of never again undertaking major military operations without the active participation of the USA, but also with the UK's present dependence on imported food and energy.

Technology strategy

The change in acquisition policy announced by the DIS is necessary but not sufficient to sustain the UK's defence industrial base. The UK also needs an appropriately large and well-targeted defence research programme to provide the foundation for judicious security policies and intelligent equipment acquisition, and for the design and development of new projects and upgrades of key classes of equipment now in service.

58 MoD *Defence Industrial Strategy* (December 2005)

As a contribution to formulating this programme, the recent Defence Technology Strategy[59] (DTS) catalogues several hundred defence technologies relevant to the MoD equipment programme, distinguishing between those in which it needs to retain (or to have assured access to) expert capability and those for which intelligent customer capability will be sufficient.

Although the distinction is sometimes ambiguous (because different sections of the DTS use different language and layout), it seems from the DTS lists that the MoD perceives no requirement for expert knowledge of many defence technologies, including, for example, fixed-wing aircraft technologies, maritime power generation and the weapons and drive systems for armoured fighting vehicles. Thus the implementation of the DTS would give the MoD operational sovereignty over some, but not all, of the defence systems and subsystems operated by its armed forces.

The DTS list of defence technologies requiring expert UK capability has been derived from the MoD's military requirements, in accordance with the (anachronistic?) UK tradition that funds voted by parliament for defence should not be allocated to other objectives. Other nations do skew the allocation of their defence research funding in favour of dual-use, civil/military technologies (such as those used in aero-engines), which have potentially profitable applications in commercial markets or which would stimulate depressed regions or industrial sectors.

Judicious investment in such technologies might stimulate faster national economic growth, although UK industry has often lacked the entrepreneurial skills and access to long-term capital to exploit successfully the spin-off from the MoD's research laboratories. Since the DIS requires the MoD to consider the impact on industry of its equipment acquisition decisions, the future allocation of MoD research funding to implement the DTS may be guided by similar considerations.

The DTS has 185 well-illustrated pages, but it is virtually a numbers-free zone, and does not address the issue of how much defence research would be required to implement its declared strategy (beyond hoping that industry will invest more). The minimum necessary level must be that which provides the UK with an intelligent customer capability in all of the technologies embodied in the MoD's future equipment acquisition programme. Additional investment must also be made to ensure expert capabilities in a smaller

59 MoD *Defence Technology Strategy* (October 2006)

number of key technologies embodied in equipment that will be produced or supported by the UK's defence industrial base.

Good, consistent data regarding current expenditure on defence research is relatively scarce, but the table below shows the 2005 levels in the USA,[60] in the UK and in some other nations,[61] and relates research expenditure to their current expenditure on equipment procurement.[62]

Table 1: Ratio of defence research spending to procurement

Nation	Research ($m)	Research/procurement (%)
USA	13,041	11.4
France	878	8.9
United Kingdom	826	7.8
Germany	513	10.2
Netherlands	139	9.1

The high expenditure in the USA reflects its need for expert capabilities in all of the defence technologies and its determination to maintain technological superiority over all potential rivals. Although the number of classes of equipment operated by the UK and France is not much less than that for the USA, European nations generally do not plan to procure or operate the full array of defence systems available, and may not need more than intelligent customer capability for some of their defence equipment.

European nations probably get more return on their research investment because they do more collaboration on defence research (yielding a return of three to five times the direct expenditure[63]), and the USA may get less because of overlap in its individual armed services' research programmes. Accordingly the difference in the ratio of research to procurement for the five nations is probably insignificant.

However, the number of technologies relevant to UK equipment projects is not an order of magnitude smaller than the number relevant to US projects, so it may be inferred that

60 American Association for the Advancement of Science, unpublished report (February 2006), table II-2
61 European Defence Agency *European Defence Expenditure in 2005*, unpublished (November 2006)
62 *Armaments, Disarmament & International Security*, Stockholm International Peace Research Institute yearbook 2006 (Oxford University Press, 2006), p353
63 National Audit Office *The Management of Defence Research & Technology*, HC360 session 2003-04 (London: TSO), p23

research per technology in the UK and other European nations is considerably smaller than in the USA. It has been estimated[64] that the USA spends 10 times more than the UK on the technologies of military gas turbine engines. If the scale of this difference were confirmed by more extensive and detailed analysis, it would indicate that European national defence projects are built on a smaller technology base and are accordingly liable to be outclassed and uncompetitive, and to be more prone during development to risks to their target performance, cost and timescale (though the risks can be slightly mitigated by intra-European collaboration which gives access to more than one technology base).

European nations may assume higher risks as an alternative to greater up-front investment in research, because they appreciate that each of their national military capabilities makes only a fractional contribution to the military strength of the EU (and an even smaller fractional contribution to NATO's), so a delay, performance shortfall or even cancellation of a national project is unlikely to be disastrous (albeit wasteful of taxpayers' funds). But for the USA such risks would be unacceptable, and it is prudent for the USA to spend more on research to reduce the risks of project failure.

Conclusions

If the parliament and people of the UK wish their armed forces to remain capable of operating alongside the USA in high-intensity expeditionary operations, those UK forces must have doctrine, training and equipment compatible with those of the USA (although for lower-level constabulary operations in different areas the nations may adopt different approaches to pacification).

For some classes of equipment the most cost-effective policy for the UK may be to develop equipment jointly with other nations (such as the USA) or to buy foreign equipment off the shelf, while retaining within the UK expert capabilities for support and upgrade of the key classes of equipment. To implement that policy the MoD's Defence Industrial Strategy has introduced long-term partnering agreements with British contractors covering one or more equipment projects, and its Defence Technology Strategy has identified those technologies in which the UK needs to retain expert, world-class capabilities.

However, there is no evidence that the MoD has rigorously assessed the costs and benefits of these complementary strategies, nor that it has budgeted for any increase in

64 Lloyd, PH *MoD Technology Strategy: The Case of Military Aero-engines*, RMCS dissertation (April 2002)

defence research (though one defence contractor[65] – from Qinetiq – has suggested that an extra £250 million a year would be required). Unless the MoD can allocate (from a defence budget under pressure from discontented armed services and from cost overruns on equipment projects) the appropriate funding for defence research and other measures to sustain the UK's defence industrial base, there is a real danger that the DIS and DTS will prove to be no more than empty rhetoric.

65 Ferrero, G, presentation at Royal Aeronautical Society conference, 20 February 2007

Chapter 9

Strategic directions for UK defence research and development

Steven Bowns, Director of Technology Futures Ltd

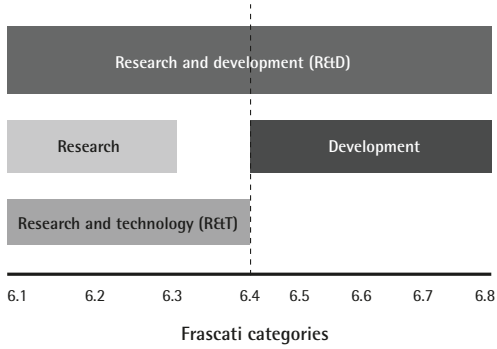
Strategic directions for UK defence research and development

This chapter will argue that measuring the value of research and development can greatly improve its strategic direction, by giving decision makers better evidence. It will explore the problems of directing R&D by first summarising the transformation in commercial technology management in the 1990s that was brought about by improvements in the way the value of R&D was measured. Exploring some of the reasons why these insights could not be straightforwardly applied to defence, the chapter will look at recent work that provides evidence of the value of defence R&D. It will then examine some of the implications for the direction of the UK defence R&D base, concluding with some suggestions for its future direction.

Definitions

The terms research and technology (R&T) and research and development (R&D) are sometimes confused or used interchangeably. Here, *R&T* will refer to early stage technology generation activity, sometimes also termed "blue skies" research or, in UK defence circles, "corporate and applied research". *R&D* encompasses R&T activity as well as "development", which is mainly focused on a known application. Development is often mainly concerned with the demonstration of technology, risk reduction, system integration, trials and tests, and evaluation activity. In terms of the Frascati definitions, we refer to R&T here as referring to those activities that Frascati termed 6.1 to 6.3, and R&D to all the activity from 6.1 to 6.8, as illustrated in figure 1.

Figure 1: Frascati definitions of research and development terms



Commercial technology management transformation

Large commercial companies take their R&D spend very seriously, especially in the electronics, communications, pharmaceutical and hydrocarbon sectors, where the technology base is pivotal to the ability to compete. Significant improvements could be made to the way R&D was directed once it proved possible to measure the value of it. During the early 1990s there was a fashion to "nail down corporate R&D spend". Led by certain management consultancies, various discounted cash-flow and net present value financial techniques were applied to R&D projects, with the result that the projects were often found wanting. This forced R&D managers to analyse and measure the value of what they were doing, or face having it cut.

The overall outcome was often a reorganisation to make corporate R&D more accountable to the operating divisions. This in turn led to project scrutiny using net present value techniques that resulted in a more short-term focus overall, although the positive effect was that R&D became more closely aligned with the business needs of the firm. But the same phenomena also delivered some disadvantages to firms, which lost their ability to compete using technology when their foreshortened new-product pipelines eventually ran dry.

In the 1990s, however, the technology pendulum started to swing the other way. New financial techniques were developed based on real option value thinking, which better captured the true value of R&D. This was in line with a more general trend to express the value of R&D in terms of the options for future action that it could buy the firm. Options thinking improved commercial technology management, as R&D managers sought to balance a portfolio of options to deliver maximum future value to their firms.

Many firms consequently increased their R&D investment: some as a response to an earlier lack of new products, others as a deliberate policy to compete with better-managed technology. These improvements continue today, so that some pharmaceutical companies –GlaxoSmithKline, Roche and Merck Sharp & Dohme, for example – now have superbly managed R&D pipelines based on highly sophisticated option valuation techniques.

The value of defence R&D

Much of this thinking passed by the defence sector; it apparently made little sense to measure only the *financial* value of defence R&D projects because they were concerned with the delivery of *military* value. What would the net present value of a defence project matter, if the resulting equipment delivered inferior military utility? These difficulties in

estimating the value of defence R&D go very deep, possibly back to the fundamentals of modern economics. In *The Wealth of Nations* Adam Smith argued that the only thing more important than prosperity was defence, which occupied a unique place in national policy:

Further, commerce sinks courage and extinguishes martial spirit; the defence of the country is handed over to a special class, and the bulk of the people grow effeminate and dastardly, as was shown by the fact that in 1745 four or five thousand naked unarmed Highlanders would have overturned the government of Great Britain with little difficulty if they had not been opposed by a standing army.

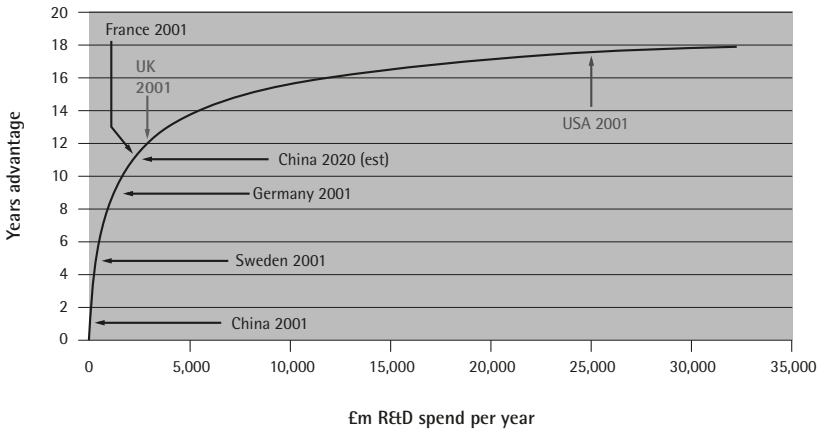
In the USA during the 1990s there was a frenzy of work based on the cost aspects of development and "value engineering", but these were never really harnessed to help direct the whole defence R&D activity. In the UK at the same time similar attempts were made, but despite the best efforts of defence output assessment studies and operational analysis, no methods emerged that were comparable to the usefulness of the commercial techniques. What chance, then, is there of measuring the value of defence R&D?

Recent work on the value of defence R&D

Some recent work commissioned by the UK Ministry of Defence offers some hope. In a paper in *Defence & Peace Economics*, Bowns, Middleton et al showed that it is possible to measure the value of defence R&D, at least comparatively, at a high level and over long periods. They used a comparative technique to compare 69 categories of like-with-like military equipment between 10 nations to give a relative measure of military equipment quality.

The underlying rationale was that, in the first place, military equipment quality is in reality very relative to other nations, since adversaries would probably be supplied with equipment designed by one of the 10 nations studied. Second, they argued that the value of defence R&D can mainly be expressed in terms of improved equipment quality, with a small exception in the area of human factors research. For most R&D, if it is not aimed at improving equipment quality, then what is it for? Their measurement shows that governments generally "get what they pay for". The paper explains a strong correlation between military equipment quality and the government defence R&D expenditure some 10-25 years earlier, illustrated in figure 2.

Figure 2: Capability advantage from R&D investment



Because all states occupy a point on this line, it was further possible to express the time advantage or disadvantage of one country over another; a high-level strategic expression of the value of defence R&D:

When describing the relative positions of nations, commentators have often described one nation as "so many years ahead" of another. It appears that this figure of speech accurately reflects the underlying situation in the case of military equipment quality.

So what now for UK defence R&D?

The UK has done well in delivering good military equipment quality against R&D expenditure since 1971. Only the high-spending USA and the Soviet Union/Russia have achieved greater equipment quality, and they show significant diminishing returns, suggesting that the UK has taken an almost optimum position, on the "knee of the curve". This seems plausible, even accepting the possibility of a pro-UK bias in this work since UK equipment was used as a baseline for comparisons. But the data also suggest that there may be a latent problem for the UK from cuts in defence R&D spending.

During the 1990s many NATO countries sought a peace dividend following the collapse of the Soviet Union. In the UK and USA some of this was manifest in cuts in R&D expenditure. But it is interesting to note that countries such as France, Germany, Italy and Spain either took smaller cuts in R&D or applied them for a shorter time, or both. The USA

reversed this trend during the late 1990s, and following 9/11 has significantly increased its R&D spend.

The UK, however, was somewhat out of step with other Western countries, in that it took a series of peace dividend-style cuts in R&D spending throughout the late 1990s and into the early 2000s. It has only very recently reversed this trend, with the 2006 and 2007 R&D expenditure set to take no further cuts. Given the 10- to 25-year time lag between spend and benefit, the UK may have stored up a particularly difficult problem for the period 2010-20, as the downturn in R&D spend in the mid to late 1990s pulls through into a reduced future military equipment quality.

This problem could prove especially challenging since the UK is most likely to favour a military posture that favours smaller and smarter capabilities. But there can be no simple, fast-spending solution, because even if the UK were radically to increase its defence R&D spending tomorrow, the benefits could not be expected to pull though into increased military equipment quality until the 10- to 25-year time lag had elapsed; which would be from 2017-32. The problem might also be exacerbated as possible future adversaries such as China have been steadily increasing their R&D spend recently.

Furthermore, using the same data set of 15,000 pieces of military equipment, it is possible to plot the average age of the equipment owned by the 10 countries studied over the last 30 years. For 1971, this method shows an overall average fleet age of all equipment of all nations to be some 9.2 years. But by 2005 this had almost doubled to 17.6 years, with a hint that this ageing is accelerating. This will come as no surprise to many analysts, who will have seen a reducing "replacement frequency" for all major platforms such as aircraft and warships as the 1990s progressed. It is, however, possible to extrapolate this trend forward to 2020, when the average age might be approaching 25 years. With such an average, many longer-lasting platforms might be approaching 50 years of age.

This raises a pressing question for UK defence R&D policy makers: will it be possible to accelerate the pull-through of R&D into equipment quality in the next decade in the face of time lags, worsening competition and an ageing fleet of equipment? The consequences of failing to address this question could be serious, as UK armed forces might face a significantly reduced equipment quality advantage over potential adversaries during the period 2010-20.

That said, UK force effectiveness is made up of many factors other than equipment quality. UK military personnel are well recruited, superbly trained and well led, and operate within highly effective doctrinal and operational frameworks. This might be enough to compensate for equipment deficiencies, but we should remember that UK forces have not faced enemies with superior equipment quality since the Tiger tanks and Messerschmitt 262 jet fighters of the Second World War.

Technology insertion

One solution to this impending dilemma would be to focus on the shorter-term development issues of equipment already in or about to go into procurement. By concentrating expenditure and management focus on this area, it might be possible to accelerate the technology pull-through and ensure that new equipment is as technologically advanced as risk-averse procurement processes will allow.

This might be achieved by looking for opportunities for technology insertion: incorporating a new piece of recent (often commercial, off-the-shelf) technology into a particular part of a piece of equipment. For example, the ASTOR surveillance aircraft has had up-to-date commercial digital recording equipment installed relatively late in the procurement process, to replace its aging magnetic tape storage. But there could be difficulties with this approach, especially with the risk-reduction aspects of insertion in the later stages of equipment procurement. It would be a very brave integrated project team leader that welcomed a technology insertion event late in the process, as the National Audit Office looked closely for cost overruns and delays.

The potential for insertion may also be heavily dependent on the degree of modularity in the target equipment. Some insertion is relatively straightforward and can deliver a huge return in equipment quality with relatively minor perturbations on the rest of the system or platform. One example of this is the retro-fitting of close-in weapons systems such as Phalanx and Goalkeeper on to warships during the late 1980s. Others are much more fraught, as they pose massive system integration challenges. Perhaps it will be possible to target opportunities for technology insertion using the degree of modularity as a key criterion?

Much of this may rest on the successful implementation of open systems architecture but is complicated by massive legacy software issues. Once again, however, there is as yet little firm evidence as to what works and what does not work in technology insertion. Decision making in this area is therefore likely to suffer from a lack of evidence-based support.

Development or research?

A further complication arises from a focus purely on the development side of the process. This could trigger a reduction in the longer-term R&T work, which could store up an even worse long-term problem into the 2020s and beyond. This will need to be guarded against, because longer-term R&T may account for about half of the correlation with equipment quality. As Bowns, Middleton et al showed, "the effect of short-term R&D expenditure ('development') and of long-term ('research') is roughly equal, based on analysis of the delay between R&D spend and equipment quality".

The UK MoD is already taking other action that should improve the situation. The recent Competition of Ideas and Grand Challenge initiative should bring more innovation into the R&T processes. This might both speed technology insertion and even possibly reduce the time lags, as already mature commercial technology is fed into the R&T mix. There are still barriers to be overcome, but the fact that these actions are taking place already is clearly a positive indication.

Conclusion

Surprisingly then, despite the many difficulties, it has proved possible to find real evidence of the value of defence R&D. This is already having an impact on the strategic direction of defence R&D in the UK, and has been cited in the recently published Defence Technology Strategy. Following a similar track to the commercial R&D management improvements of the 1990s, real evidence and meaningful measurement of value may be expected to make a significant contribution to the strategic direction of UK defence technology.

However, it will be essential to know what data to look for, to put in substantial effort and to analyse the results with the appropriate tools. By applying these methods, it is already disturbing to note that following the 1990s peace dividend cuts in R&D funding, the UK may be facing a significant risk of its relative military equipment advantage being eroded during the next decade.

Remedial action is possible but difficult, since time lags mean that simple "spend now" solutions will not pull through in time. Process improvements and technology insertion into equipment that is already in procurement are likely to yield results. However, this should be done together with a safeguarding of the level of R&T spend and by introducing more innovation; otherwise even greater problems will be stored up for decades to come.

References

Buckley, JV *Going for Growth: Realising the Value of Technology* (McGraw Hill, 1990)

Verloop, J *Insight in Innovation: Managing Innovation by Understanding the Laws of Innovation* (Elsevier, 2004)

Bowns, S, Middleton, A et al "The Effect of Defence R&D on Military Equipment Quality" in *Defence & Peace Economics* vol 17, no 2 (April 2006)

Chapter 10

Technology and the private sector – communication in a large-scale crisis

Tony Baptiste, Manager (Business Development and Strategy) at Fujitsu Defence and Security

Technology and the private sector – communication in a large-scale crisis

This chapter focuses on the principles for exercising command and control during a large-scale crisis, and the enabling technologies that support the overall requirement. The analysis highlights the need to establish more effective interoperability across a number of organisations and agencies. The chapter begins with a discussion of UK and overseas experience to date, setting the context for the remainder of the chapter. What lessons have been learned concerning the response to a large-scale, multi-agency threat to critical national infrastructure, whether prompted by terrorist attack or natural disaster, or some combination of both? The chapter describes the response of one company – Fujitsu Services – to the challenges discussed.

Context

Command and control is key to any response. Crisis response is often considered as a "vertical" or hierarchical challenge. But within a large-scale crisis, either multi-point or geographically widespread, there is an identifiable need for "horizontal" command and control – or at least intercommunications and interoperability supporting command structures.

A core concern is the relationship between technology enablers, organisation and process – and the dynamics operating between them. This is more pronounced the larger the scale of operation, since the number of organisations involved will increase commensurately, and a larger geographical area will be covered. This can be within a homeland security situation (where this paper is mainly focused), but is similarly relevant within a deployed or littoral (that is, evacuation) operation, where there is a similar need for communications and information management, and where the necessary infrastructure is either non-existent or heavily degraded. In many cases of deployed operations this might be because the infrastructure was never there or had been destroyed in conflict. In domestic security operations, on the other hand, the communications and information infrastructure might have been overwhelmed either by natural disaster (such as wide-scale flooding) or by terrorist action such as the release of a chemical, biological, radiological or nuclear weapon (CBRN) and the imposition of quarantine in large urban areas.

To date within the UK, major emergencies have mainly been "point" crises, focused on a single geographic area, such as London on 7 July 2005 (7/7), or, where a wider area has been affected, have been restricted in scope, as with the large-scale outbreak of foot-and-

mouth disease in 2001. The question then becomes how a large-scale threat to critical national infrastructure could be managed in which not only the emergency services were involved but also the military, all arms of government (central, regional and local), agencies, utilities, the health service and indeed the private-sector/industry, down to small citizen/kinship groups, whether formal or informal in constitution. The common factor would be the need for all these agencies to interoperate within a network-enabled command and control framework. But what would that requirement mean in practice?

Within a point crisis such as 7/7, help and assistance would be focused on a relatively small area. Tragic as the London bombings were, the crisis was relatively small-scale and London was probably the best-prepared target, with well-practised and professional emergency services rapidly deployed – as was demonstrated. However, the possibility exists that a number of attacks could be mounted across the country simultaneously and/or combined with a major natural disaster such as flooding, perhaps as a consequence of the destruction of the Thames barrier, for instance. It is now recognised that, while these scenarios are lower in probability, the severity of the impact should they occur makes them worth planning against. In this regard, the impact of Hurricane Katrina on New Orleans refocused attention and demonstrated a number of key lessons:

- Communications and information management are vital and were generally lacking. The lack of command and control communications interoperability was a significant issue, exacerbated by the federal, state and county constitutional structures. As it happened, in New Orleans the first emergency communications were erected by the Canadian armed forces.
- Local communities and kinship groups became self-sustaining, such as non-governmental organisations (NGOs), charities, faith groups and churches, all playing a key role in pulling together help for survivors. Interestingly, this effect was also apparent in the Boxing Day tsunami, where the emergency services and military were not initially in evidence; it was the local people and local/regional government that rescued and supported the many tourists and locals at threat. Similarly, in the January 2005 Carlisle floods, it was the local churches working together that initially provided first-line support to the community.
- Local planning was inadequate; no plans had been prepared for a major catastrophe.
- The first priority was search and rescue (SAR), followed by control of looting and finally relief supply and distribution. Law and order did not break down as such, although law enforcement was lacking. The military (National Guard) eventually took control of the situation, although the lack of effective communications made it more

difficult to get to grips with the widespread nature of the problem.

- Lack of co-operation with the public was a function of low trust. It became clear that when a family is at risk, its members will not follow instructions unless trust is already in place. What was required here was the involvement of the community in planning, in order to build confidence, and then good communications to maintain the contact in a crisis.
- Evacuation of the city went surprisingly well, since it had been practised earlier. However, there were no tracking systems in place so the authorities had (and have) no clear idea how many people left the city, where they now reside – or indeed whether they will return. In the UK, the experience in 7/7 was that while the emergency services responded well and support for individual citizens was adequate for the duration of the immediate crisis, there were no proper follow-up support systems in place for them or their families once they left the site of the emergency or aid centre.

Approach – engaging effectively with a multi-agency crisis

Whereas Cold War-style civil defence tended to marginalise local and individual judgment, homeland security in the early 21st century requires a more nuanced approach. With the prospect of complex crises and disseminated threats, the public must be more active partners in the enterprise, expected not only to know what to do in a crisis but also to contribute to the efforts of local communities and voluntary organisations in protection and prevention measures, and in consequence management and recovery.

In reality the difference in scale from the response at a point level will lead to two major shifts in consequence. Firstly, as noted above, there will be a multi-agency interoperability requirement, not just within the emergency services but also embracing all or some of the military, the Environment Agency, utilities, hospitals, local and regional as well as central government, NGOs, industry and so on. This will include not only communications but also information management and data-sharing capabilities.

Secondly, military involvement will almost certainly be required in support of the civil authorities, and will be deeper and wider than for a point crisis. A number of key capability areas should be considered here, including shared situational awareness, command and control, surveillance, intelligence and reconnaissance (C^4I STAR), and emergency communications. Another asset to consider is that the military are trained to manage within a chaotic and confused environment. This could include the breakdown of law and order or simply responding to unplanned and unforeseen events, such as might be witnessed within a large-scale scenario. It is important to recognise that this will require

a degree of harmonious working over a perhaps lengthy period of time, between the civilian and military emergency services, which could place a strain on communications technologies, process and doctrine.

In general, UK armed forces do not exercise with the blue light services to any extent, so it will be vital for communications to work seamlessly if more effective inter-working is to be facilitated within a crisis. Otherwise the risk is that the considerable capabilities at the disposal of the military will not be fully understood or effectively deployed in the right time frame. It is worth noting that, within the civil contingency framework, the military do not at present register in the list of first or secondary responders. For the military it is arguable that, within a terrorist context, the front line is as much on the home front as in deployed operations, and as such should be viewed as within their main remit rather than within the framework of Military Aid to Civil Authorities (MACA), where the role of the military is somewhat downgraded.

However, the essential features will remain the same, whether a large-scale or "point" crisis response:

- the emergency services will lead and retain civilian control overall – the military will stay in support;
- individuals will overcome failures in technology;
- local knowledge will be vital (see below);
- communications will continue to be limited/fractured, at least initially.

It is worth stressing the importance of local knowledge. This was demonstrated in the Boscastle floods in Cornwall in August 2004, where local knowledge played a key role in preventing loss of life. As well as the fact that daylight allowed the synchronous operation of up to seven helicopters, disaster was only narrowly avoided when a local resident noticed that the culvert under the main hotel at the estuary mouth was blocked, and managed to warn the large number of people sheltering in the bar to leave, minutes before the river broke through the bar ceiling and swept everything out to sea.

The Boscastle incident emphasised the value of good local communications, and the ability of the command organisation to identify and act on the information it received. While the constrained geography of Boscastle did not require the use of technology as such, the principles are relevant to a larger-scale crisis, where the communications structure would need to trap and disseminate local knowledge in the same, timely way.

One example where the lack of intercommunications had tragic results was the loss of over a hundred firefighters in 9/11, when they could not be warned of the imminent collapse of the Twin Towers.

Response – how technology can assist

The response on the ground to a multi-agency crisis will need to be different, smarter and sustained. The aim should be to generate a wide-area, fully functional, interoperability-based response to allow responders to "join up" across a multi-agency environment, and within an effective command and control framework. There are three generic IT technologies that can enable this.

Communications network integration

There will initially be a need to improve voice (and data) intercommunication to allow responders to co-ordinate their activities across a multi-agency environment. At the same time, the agencies and "independent" citizen groups (possibly cut off physically from the wider community) will need to be able to communicate their situation to rescue agencies and/or with their social and kinship communities, which by this time might be distributed across the crisis landscape. This horizontal communications capability enables society to help itself where there has been a major breakdown in infrastructure, and proved to be most important in recovering from Hurricane Katrina. In the Carlisle floods, when all other communications failed, including landline and mobile phones, this was achieved through broadcast local radio, but clearly this is limited to a single direction.

In a major incident in the UK, the Gold, Silver, Bronze command structure will be activated, where the following responsibilities are defined:

- Gold command (strategic level) – determining policy and resources;
- Silver command (tactical level) – in charge at the incident;
- Bronze command (operational level) – practical activity on the ground.

Typically the Silver commander will in the first 24 hours be mainly concerned with first responders, such as the emergency services. However, as the crisis widens over the first few days, he or she will increasingly need to be able to talk to a wide variety of other agencies to secure the information to pass on to Gold command in order that strategic decisions can be made, and in order that the agencies can receive any immediate guidance and decisions they need.

With this challenge in mind, Fujitsu Services has developed a crisis communications service, Cobalt, which integrates various communications networks and technologies to allow command units to talk to any relevant organisation directly. Importantly, command and operational units can continue to use their own communications, and do not have to be provided with different and additional handsets in order to communicate with other agencies, least of all join a separate communications network. The service not only provides the scope for full interoperability between various communications networks, including radio, mobile/GSM, Tetra (airwave), PSTN (landlines), VOIP (internet phones) and so on, but can also deliver alternative bearer capability (either direct or via subcontractor agencies) where existing infrastructure (such as mobile masts) is non-operational.

Joint Operational Picture

Alongside intercommunications, another key enabling technology is the provision of a comprehensive "Joint Operational Picture", accepting inputs from specialist situational awareness vehicles, communications sensors and information management feeds. Although the term "picture" is used in this context, this does not necessarily imply a single, viewable graphic on a computer screen. The "picture" is as much in the mind of the commander as it is a physical (or electronic) depiction of a situation. The Joint Operational Picture is essentially a mechanism for providing genuine shared situational awareness and agile information flows. Adapted from the defence world of networked enabled capability/network-centric warfare (NEC/NCW), it should also play an important part in defending the homeland "front". It works on the principle of layered infrastructure, with the technology covering the physical and information layers feeding into the cognitive and social levels. The fundamental objective is to provide the operational commanders with an unambiguous picture of the situation on the ground, such that any threat is perceived in exactly the same way and a unified response can be agreed. If there are overlapping outputs, the danger is that the varying perspectives in which the commanders are operating (including within the social layer) may lead to different, rather than shared responses.

Fujitsu Services delivers this capability through its openJOP product. The role of openJOP is to deliver information and applications in a consistent framework through a single, web-enabled interface. Information can be stored locally within the JOPWeb or accessed from repositories of other systems. If stored within JOPWeb, the information is replicated amongst all instances of openJOP. From an information perspective, the functions of openJOP are as follows:

- acquisition of information by the most appropriate means;
- aggregation of information content from multiple sources;
- customisation of information to reflect the role of the user; and
- presentation of information taking into account the available bandwidth and user access device.

Standard features include a message tickertape and a "what's new" frame to keep users up to date with developments as they happen.

Command visualisation and integration of source (legacy) systems

Finally, there is the need to identify which of the existing information systems across government would need to be accessed and joined up in respect of command level visualisation. This is essential if the appropriate levels of authority are to have the required information to take whatever decisions are needed in respect of deploying resources across the crisis. Only in this way can the crisis be managed on a comprehensive end-to-end basis. This would include dynamic re-planning of resource deployment where the situation was rapidly changing.

Fusion technologies as delivered by Fujitsu Services within its logistics end-to-end supply chain system (FILM) for the Ministry of Defence now provide a cost-effective means for rapidly developing such decision-support systems, including updating the source legacy/silo information systems so that they can be embraced in any overall information management solution. This approach can ensure the protection of the existing investment and can facilitate component replacement at lower levels, whilst maintaining a consistent user experience at the front end and thereby negating the need for continual retraining.

Outcomes

At an organisational level, the benefits of improved interoperability are a command and control structure that will be better-informed and aware – thus allowing commanders at various levels both to take better decisions and to make best use of all the assets under their control or influence. At a societal level, a more joined-up response would also build trust between commanders and those they are seeking to lead, so that communities would be more inclined to accept help and direction – perhaps, in some cases, counter-culturally. Perhaps more importantly, those communities would begin to generate a level of self-help and resilience that would underpin the work of the direct responders.

Clearly, the interplay of vertical and horizontal communications within a common

command and control framework is a complex challenge managerially. The development of supporting doctrine, process and technological management control mechanisms should diminish the likelihood of communications anarchy. The overall aim should be to create a national response system that is "virtual" in some degree. Rather than static and institutional, premised largely on a single expected threat, it should be dynamic and adaptable. It should have the capacity to respond to the unknown and unpredicted, with the ability dynamically to reconfigure the combination of agencies and authorities most suited to the challenge at hand. The coherence of the virtual national response system depends crucially on the transmission of information: the basis of timely decision, effective action and public resilience.

Summary and conclusions

Modern technology, particularly in IT and communications, offers the opportunity to create information networks of the required scale, complexity and responsiveness, and to select from the mass of information available what is needed for good strategic decision making at the centre. Plans, processes and operational concepts can all be prepared, to ensure that the required capabilities in information management and sharing can be configured, and rapidly reconfigured, to meet as wide a range of contingencies as might reasonably be expected.

Technology is not, however, the sole or even the main driver in the development of a virtual national response system. Political and governance frameworks at the most senior levels will need to be adapted to enable new technologies to play and interplay to best effect.

The challenge of making an effective response to embrace these factors, and others, lies in our ability to harness that technology and to make the necessary changes to organisation, doctrine and process. With this in mind, a number of central principles can be identified:

1. Interoperability is essential and is more than intercommunications – although intercommunications are an essential prerequisite.
2. Information and communications technology is fundamental to enabling the different sectors to join up.
3. An essential asset in this regard is the existing base of information systems inside (and outside) government and the sectors that need joining up.
4. The core capabilities in delivering an effective and sustained response framework are

systems integration (the capability to integrate many different IT products from different suppliers into a coherent set of information systems) and technology watch (the expert knowledge and advice on how information and communications technologies are developing to support required processes).

5. The focus on solutions should emphasise service provision over product delivery, into all levels of a multi-agency constituency.
6. An effective doctrinal, organisational and process framework will be required to support the technologies deployed. This needs to be identified and exercised ahead of any large-scale crisis, with the involvement of all key responders.
7. Training needs must be factored in ahead of any event. Military capabilities in particular must be identified and exercised within a multi-agency environment ahead of any crisis.

This chapter has offered the response of one company – Fujitsu Services – to the need for an effective response to a large-scale as opposed to single-point crisis, where the critical national infrastructure is threatened in a quantitatively and qualitatively different way. The challenges, which were only just coped with at an institutional and organisational level on 7/7, need to be explored and tested in respect to a wide-scale and/or multi-point crisis. By and large, the technologies that need to be joined up are already there and are being further developed. But the exercise of command and control in a multi-agency environment, in the midst of a complex and urgent crisis, must be considered afresh after recent lessons from both the UK and abroad.

Section IV: Values in security

Chapter 11

The first victim of war – compromising civil liberties

Shami Chakrabarti, Director of Liberty, and Gareth Crossman, Policy Director of Liberty

The first victim of war – compromising civil liberties

London is not a battlefield. Those innocents who were murdered on July 7, 2005 were not victims of war. And the men who killed them were not, as in their vanity they claimed on their ludicrous videos, "soldiers"…We need to be very clear about this. On the streets of London, there is no such thing as a "war on terror".

The importance of these comments stems not from the originality of content. Liberty has warned against the dangers of the "war on terror" metaphor and its consequences for over five years. It is the fact that our concern is now shared by the country's chief prosecutor, Sir Ken Macdonald QC, the Director of Public Prosecutions. His words, made to members of the Criminal Bar Association on 23 January 2007, demonstrate how widespread concerns over government rhetoric and action on terrorism have become.

The government's tendency to speak of the terrorist threat in terms of a war arguably gives a false legitimacy to the motives of 7 July bomber Mohammad Sidique Khan and his associates. They agreed with the analysis, seeing themselves as soldiers and their actions as heroic. Such language also provides the background against which a multiplicity of anti-terrorism laws have been passed in the UK since 2000.

Opinion polls frequently suggest that people are willing to "give up" their liberty in order to achieve security. Immediately after the London bombings in July 2005, *The Guardian* ran an ICM opinion poll that showed that about three-quarters of people would be willing to give up liberties for improved national security. Eighteen months on, the national mood seems still set against human rights and civil liberties. The National Centre for Social Research asked a range of questions about liberty and security in its January 2007 annual report. It concluded that "an overwhelming majority of people are willing to give up various freedoms to help tackle the threat of terrorism".

Such surveys might make gloomy reading for those concerned with rights and freedoms. However, the telling feature of these surveys is that they use the language of "giving up" and "sacrificing" freedoms. Given an either/or choice it is hardly surprising that so many people favour national security. None of us wants to be blown up by a fanatic on the Underground. Yet to adopt a simplistic position of choosing one alternative or another is to ignore the nature of the post-war human rights consensus embodied in the Human Rights Act 1998. At its heart is the implicit acknowledgment that the state is entitled to take appropriate steps to maintain the safety and integrity of those living within its borders.

Proportionality is already accepted

In many ways we acknowledge this without thinking. Who does not feel outrage on viewing Sidique Khan's video diatribe in which he adopts the "war on terror" rhetoric and claims: "We are at war and I am a soldier"? Who (apart from commercial interests) really rails at the thought of facing any increased security at airports? There is understandable and rational acceptance that at times of heightened risk to public safety, the authorities can and must take appropriate steps to protect us.

This concept of proportionality is at the heart of human rights thinking. Part and parcel of an evaluation of whether the state can legitimately act is the acknowledgement that the security environment changes, that levels of threat change.

None the less, the framework makes vital and carefully calibrated distinctions between different types of rights and freedoms. So torture and inhuman and degrading treatment must be outlawed by civilised societies, even in "time of war or other public emergency threatening the life of the nation" – one limb of the test for lawful derogation from the European Convention on Human Rights (ECHR).

Due process rights against arbitrary detention to fair trial may be temporarily "derogated" from in national emergency situations. However, even such departure from democratic norms must by definition be temporary in nature and only that which is "strictly necessary" in the circumstances.

Thirdly, a group of "qualified" or "balanced rights" to, for instance, privacy and family life, and freedom of thought, speech and association provide the essence of life in a democracy. They are constantly and inevitably interfered with for a number of societal benefits, but only to the extent that is necessary, proportionate and in accordance with law.

Finally, there is the vital and overarching principle of both universal human rights and logical reasoning: that policies and principles applied to one person or group be applied in a non-discriminatory fashion to others in a like situation.

There have been useful additions to the statute book. However, these have tended to coincide with a great deal of cross-party and cross-interest consensus as to a specific gap in the law. For example, it was appropriate to create offences such as attending a place used for terrorist training overseas; preparation of terrorist acts; and making radioactive devices (all introduced in the Terrorism Act 2006). These new offences ensure that the

criminal law is developed to cater for situations relevant to modern terrorist practices and techniques.

Too much has been done

The problem is that we have done more than is proportionate, and so much that is positively counterproductive. After the Terrorism Act of 2000 there followed further anti-terrorism legislation in 2001, 2005 and 2006. A new bill is expected in parliament in the coming months. The government has frequently been accused of passing too many laws. Even in this environment of legislative overkill, anti-terrorism law making stands out.

So which laws are problematic? Of particular concern is the manner in which the use of criminal law to bring alleged terrorists to trial has been undermined by a reliance on quasi-judicial processes. Departures from the normal standards of criminal law create a culture of exceptionalism that heightens both real and perceived injustice in the eyes of millions and the "wartime" heroics of the dangerous minority.

The Special Immigration Appeal Commission was introduced in 1997 to provide judicial oversight for asylum and immigration appeals. SIAC procedures differ from normal criminal court processes in their use of special advocates: security-cleared lawyers who do not act for terrorism suspects but instead are used to represent their interests. The special advocate will often do this in closed hearings where the "client" is not present. After the September 2001 bombings, the government rushed through legislation allowing for the potentially indefinite internment of foreign nationals. The SIAC was delegated as the court overseeing detention.

The fundamental problem with the use of the SIAC in this way is that people who are accused of involvement in terrorist activity are not allowed to know what it is they have done, their lawyers are not told what they were supposed to have done, and the special advocates who do know are not allowed to tell then. This Kafkaesque system meant that it was impossible for a detainee to rebut evidence against him as he did not know what it was. This cornerstone of the government's anti-terrorism policy was thrown into disarray in December 2004, when the House of Lords appellate committee determined by a majority of eight to one that these detentions were discriminatory, disproportionate and breached the right to liberty.

The government response to the House of Lords decision was to introduce the "control order" regime in the Prevention of Terrorism Act 2005. This made detention of British

citizens as well as of non-nationals possible, and replaced detention in high-security prisons such as Belmarsh with other restrictions such as house detention, curfew and reporting to the police. However, it retained a virtually identical oversight process through use of the SIAC. As a consequence, challenges to this process have already resulted in the High Court determining that control orders are not compatible with human rights protections.

Free speech under threat

Attacks on free speech and expression have also been characteristic of government policy. Speech offences such as the encouragement or glorification of terrorism have become crimes, whether or not the person speaking intends for anyone else to commit a crime or act of terrorism as a consequence of what they say. This makes a crime of careless talk. Unfortunately, debate on speech crime can become confusing, especially when it is unclear what is being criminalised.

In one of his rare appearances on Radio 4's *Today* programme, on 16 September 2005, the Prime Minister justified the planned offence, saying "... the fact that someone who comes into our country and maybe seeks refuge here, the fact that we say: 'If, when you are here, play by the rules, play fair; don't start inciting people to go and kill other innocent people in Britain.'" These are difficult sentiments to argue against, if you are unaware that inciting people to go and kill other, innocent people was already an offence carrying life imprisonment.

Difficulties with these broad speech offences became apparent when government ministers struggled to argue with criticisms that refugees from Zimbabwe saying the Robert Mugabe regime should be overthrown (or even Iraqi dissidents calling for Saddam Hussein to be forcibly ousted before the invasion) would be caught by the breadth of their terms. Ministers who, possibly as young firebrand radicals, had vehemently called for the overthrow of the apartheid regime in South Africa struggled to deal with the classic conundrum of what distinguishes a terrorist from a freedom fighter.

The 2006 Terrorism Act made further inroads into free expression. In particular it broadened the definition of proscription contained in the 2000 act. As well as allowing for violent terrorist organisations to be outlawed, the definition now also covers non-violent political groups that glorify terrorism. The provisions in the 2006 act added to the ever-growing list of restrictions on rights and freedoms taken in the name of fighting terrorism. These include: restrictions on protection outside parliament; the creation of

city-wide stop-and-search powers without suspicion of wrongdoing; compulsory identity cards, and a variety of other privacy intrusions. In the words of the information commissioner, Richard Thomas, the effect of all these measures amounted to the creation of a "surveillance society".

Sometimes these measures have proved excessive for parliamentarians. Most notably, the government's plans to extend powers to detain suspects for up to 90 days without charge (the equivalent of a six-month custodial sentence) were defeated by an alliance of Conservative, Liberal Democrat and backbench Labour MPs. Despite such setbacks, ministers seem determined to press new measures through in the coming parliamentary session.

Why it is a problem

So, why is this problematic? If national security is threatened, does it matter if we overstep the mark on occasion? We believe there are good reasons why overzealous law making should be avoided.

First, once rights have been removed they are difficult to claw back. People living within the UK – a common law country – are generally free to do as they wish unless there is a law preventing it. Governments are more in the habit of making laws than repealing them and it is possible, if not likely, that restrictions on speech, protest and fair trial would remain on the statute book after the rationale justifying their introduction had been forgotten.

Second, excessive law making can prove to be positively counterproductive. Experiences of terrorism in Northern Ireland demonstrate that the goodwill of sections of the population is essential for the intelligence that effective policing depends upon. Government ministers will often talk about the vast majority of "honest, law-abiding Muslims" who despise terrorism. This is of course accurate. However, when internment, speech restrictions and stop-and-search powers are used excessively and disproportionately against particular groups, feelings of national solidarity are replaced with minority resentment and mistrust.

The Metropolitan Police Authority recognised this when giving evidence to the parliamentary home affairs committee in July 2004. Commenting on allegations that anti-terrorism stop-and-search policing powers contained in section 44 of the Terrorism Act 2000 were being used for general policing purposes, the authority said: "It [section 44]

has increased the level of distrust of our police. It has created deeper racial and ethnic tensions against the police. It has trampled on the basic human rights of too many Londoners. It has cut off valuable sources of community information and intelligence. It has exacerbated community divisions and weakened social cohesion."

Finally, we need to ask: where do we stop? At which point does a nation begin to lose its claim to the ethical superiority that separates us from those who would do us harm? The UK's credibility has arguably already been undermined through involvement in the Iraq War. How much more can we risk? Do we go as far as the USA, which now has held people for years without charge at Guantanamo Bay and which has admitted to the use of torture? In its "war on terror", the US authorities have determined that it is legitimate to abduct people and fly them around the world to secret "black sites". They argue that practices at black sites such as "waterboarding" (the simulated drowning of people by holding them underwater) does not amount to torture, which is categorised as activity harmful enough to cause organ failure.

Would the UK be complicit in such activity? According to the Council of Europe we may well be. Its investigation into "rendition" flights, involving illegal seizure and transportation to Guantanamo Bay and to black sites, concluded that it was likely that UK airspace and airports had been used by aeroplanes involved in a "spider's web" of rendition flights. The UK government has insisted that it does not condone torture. However, it remains keen to challenge laws that prevent the removal of other nationalities to countries where they are likely to be tortured or killed.

As a nation we cannot give any credence to the allegations of murderers like Sidique Khan. Our laws should reflect the need that we face to protect our security, but equally protect our fundamental rights and freedoms. Ensuring that our police and security services have sufficient resources to work effectively is paramount to security. The billions wasted on a national identity card scheme would be far better spent ensuring those resources are available.

Instead of 90-day pre-charge detention and secret SIAC courts, more can be done to bring to trial those alleged to have been involved in terrorism. Removal of the unjustifiable bar on the admissibility of intercepted communications in criminal trials would be an essential first step in achieving this. The moral authority actively to seek the partnership and participation of millions of British Muslims is the prize that follows an end to the exceptionalist and draconian legislative approach adopted thus far.

At the 2006 Labour Party conference, Home Secretary Dr John Reid was forthright about the proper approach to national security. He said: "Faced with the terrorist threat, as John F Kennedy said, we must be prepared to bear any burden, pay any price, face any foe, and support any friend." Unfortunately these stirring sentiments did not quite convey the message intended by the late President. At his inauguration his words were slightly lengthier, but perhaps of greater significance to the UK in 2007:

We shall pay any price, bear any burden, meet any hardship, support any friend or oppose any foe ... to assure the survival and the success of liberty.

Chapter 12

Home-grown nihilism – the clash within civilisations

Bill Durodié, Senior Lecturer in Risk and Security at Cranfield University

Home-grown nihilism – the clash within civilisations

Terrorism reflects a wide spectrum of causes and beliefs. Individuals who trained in camps in Afghanistan have different motivations from those who act out of a sense of vengeance in the Gaza strip. Some groups may hold global pretensions, but most have a more limited, regional focus.

What concerns us here, however, is what it is that propels young men from Birmingham, Burnley, Leeds or Luton – individuals with no tangible connection to Afghanistan, Palestine, Iraq, Bosnia, Chechnya or anywhere else much beyond these shores – to choose to be, or to support, terrorists.

Our ability to understand this objectively is crucial; otherwise we may impute meanings and motivations to those involved solely on the basis of their own statements, or of our prejudices. We would then fail to grasp any broader dynamic involved and may end up making matters worse.

The search for meaning

On 11 May 2006 the British government published the *Report of the Official Account of the Bombings in London on 7th July 2005*.[66] This document examined what was known of the terrible events that had occurred the previous summer and that led to the loss of 52 innocent lives, in addition to those of the four perpetrators.

The preface to the report describes it as a "narrative", and that is an apt and telling description for what follows. The document presents a step-by-step account of *what* happened, *where* and *when* it happened, by *whom* it was carried out and even *how*, but – despite investigations lasting almost a year and a section devoted to the issue – little explanation as to *why*.

Yet it is precisely the *why* that should be of most interest. Without understanding why, there is little hope of precluding such incidents from happening again in the future. In addition, not being clear as to *why* allows all manner of self-appointed experts, pundits and commentators – according to their pre-existing political persuasions – to project their own pet theory on to the situation with a view to shaping ensuing policy.

66 HC 1087 (Norwich: HMSO, 2006)

Most common among these purported explanations has been the presumption that the attacks formed some kind of retribution for the British government having supported the US-led invasion of Iraq in 2003.[67] But oddly, the assumed ring-leader, Mohammad Sidique Khan, made no specific mention of Iraq in his so-called martyrdom video released soon after the bombings.

Others suggest the bombers to have been part of a resurgent and radical global Islamist movement or extremist conspiracy. Accordingly, the presumed influences of madrasas, mosques and mullahs have come under extensive scrutiny. Alternative explanations and justifications have been sought in the supposed social and economic backgrounds of the conspirators,[68] as well as their psychological profiles and educational performances.

Much has been made of the fact that two of the four had travelled to Pakistan, but the report indicates that who they may have met there "has not yet been established". There may be some evidence that these two learned their techniques there from an individual who also taught one of the failed bombers of 21 July 2005. But it is also clear that they only sought this support and endorsement after deciding to act and that neither group knew of the other.

In fact, the *Official Account* describes the backgrounds of the perpetrators of the London bombings as "unexceptional", their purported links to al-Qaeda as lacking "firm evidence", and their methods and materials as, respectively, requiring "no great expertise" and being "readily available".

Bombers did not represent a wider community

We should not take the assertions of the bombers to have acted on behalf of other Muslims at face value. They had not sought the views of other Muslims and did not represent these in any way. A parallel Report into the *London Terrorist Attacks on 7 July 2005*, issued by the Intelligence & Security Committee, also notes that the claimed responsibility for the attacks by Ayman al Zawaheri was "not supported by any firm evidence".[69]

67 Such a view has become mainstream across the political spectrum, migrating from George Galloway's tirade against Tony Blair upon being elected MP for the Respect Party in the London Borough of Tower Hamlets in 2005 to the authors of "Riding Pillion for Tackling Terrorism is a High-risk Policy", a paper in the Chatham House publication *Security, Terrorism & the UK*, ISP/NSC briefing paper 05/01(London: RIIA, 2005)
68 Briggs, R, Fieschi, C and Lownsbrough, H *Bringing it Home: Community-based Approaches to Counter-terrorism* (London: Demos, 2006)
69 Cm 6785 (Norwich: HMSO, 2006)

By interpreting the available information according to their own preferred and uncritical models, many analysts have, in effect, been doing the terrorists' thinking and talking for them. They have helped to fill the vacuum of information and confusion otherwise left behind. These purported explanations may, in their turn, encourage and even serve as justifications to others intent on action. But are they right?

We will never know exactly what motivated the London bombers. Those truly responsible are no longer around to inform us. Yet many of the purported explanations seem to seek to excuse them of this responsibility. The publication of a rather limited "narrative", rather than of an in-depth political analysis, shows how difficult it has been for the authorities to establish the motives and drivers of those concerned. It suggests that much of the superficial speculation is not supported by any hard evidence.

There is little to indicate that Khan or his collaborators Shehzad Tanweer, Jermaine Lindsay and Hasib Hussain were particularly pious or held any deep appreciation of the Koran; still less that they had direct relations to anyone in Palestine, Bosnia or Iraq. They did not bother to ask their families, friends or neighbours what they thought about such matters. That is why these were so deeply shocked by their actions.

The bombers met in the local gymnasium rather than the local mosque, they went on outdoor activities together and, the day before the attacks, one of them played that quintessentially English game – cricket – in his local park. In the end, they acted alone – in isolation – a form of private gesture against a world they appeared to feel little connection with, let alone ability to influence. They took part in the ultimate "not in my name" protest – a trend and slogan manifested by many other interest groups nowadays.[70]

In other words, contrary to the popular image of an organised, global network of religiously inspired fanatics, determined to create mass destruction, the actual evidence points to a small group, operating in isolation, using rudimentary tools and looking to rationalise their rage through religion.

Pointless and meaningless acts

The real truth, then, about the London bombings may be that they were largely pointless and meaningless. This would suggest a problem entirely opposed to that presented by

70 "Not in my name" was the slogan used by many of those opposed to the Iraq war of 2003. Faisal Devji points to a growing usage of such non-political statements by a wide variety of groups encompassing environmental protestors and others in *Landscapes of the Jihad: Militancy, Morality, Modernity* (New Delhi: Foundation Books, 2005)

politicians and officials, media and other commentators alike. The bombers were fantasists – wannabe terrorists – searching for an identity and a meaning to their lives. They hoped to find it in a global cause that was not their own, but that appeared to give expression to their nihilistic sense of grievance. Islam was their motif, not their motive.

This interpretation may offer little solace to the relatives of those affected. Their demands, as well as those of others, for a public inquiry into the matter appear more like a desperate attempt to find a more substantial explanation or to attribute blame where, for now at least, none can be found.[71]

That is hardly surprising, as the desire to understand the causes of, or to attach some kind of meaning to, adversity is a strong one. It can be deflating or confusing to discover that some event did not have the profundity originally attached to it, or that it was largely pointless. Nevertheless, we could all learn from the mother of Theo van Gogh, the Dutch filmmaker murdered by a similar, self-styled radical Islamist, who indicated in relation to her plight: "What is so regrettable ... is that Theo has been murdered by such a loser, such an incoherent person. Murder or manslaughter is always a terrible thing but to be killed by such a figure makes it especially hard."[72]

Recognising the random and unpredictable character of her loss ensures it is not endowed with portentous meaning. It does not lead to a demand to reorganise society around the presumption of similar events occurring again. To do so would be to normalise extremes and thereby to marginalise what is normal. This would effectively "do the terrorists' job for them",[73] by institutionalising instability.

The usual rejoinder to this is to argue that terrorists "only need to be lucky once",[74] while governments and their security agencies must counter them at all times if they are not to lose the public's support. But the evidence from 7 July 2005 rather suggests this perception not to be true. Most people sought to go to work the following day rather than blame the authorities.

An absence of meaning is not just disorienting, it can be debilitating. In his book *Man's*

71 This is not to belittle the genuine grief of all those concerned, or indeed their understandable desire for support.
72 Cited in *De Telegraaf*, 26 July 2005. Available at: http://www.telegraaf.nl/binnenland/23285701/Moeder_Van_Gogh:_enige_juiste_straf.html
73 A common warning from the Prime Minister, the head of the security service and many others
74 A phrase attributed to the IRA after failing to assassinate the then Prime Minister, Margaret Thatcher

Search for Meaning, the Holocaust survivor and philosopher Viktor Frankl wrote: "Man is not destroyed by suffering; he is destroyed by suffering without meaning."[75] It is our failure to place things into an agreed framework that can readily make random events assume catastrophic proportions, thereby inducing a sense of fear and terror. In a similar vein, French political scientist Zaki Laïdi has suggested that the dissolution of the old – Cold War – world order was what in particular helped to create what he has termed "a world without meaning"[76] Accordingly, there is now a growing search for meaning and identity in society.

Within an assumed framework of meaning, or in pursuit of agreed goals, adverse events are understood and can be withstood – as was the case during the IRA's terror campaign on mainland Britain. Today, in an age when nothing is, or appears, so obvious any more, such incidents accentuate our uncertainties.

The causes of radicalisation

To some, what is happening was supposedly predicted. The idea of a "clash of civilisations", taken from the title of Samuel Huntington's book,[77] assumed that future conflicts would increasingly pit East against West in a fundamental conflict over values. This thesis benefited from renewed interest in the aftermath of the attacks upon America in September 2001. But few have inquired critically into the true ideological origins of those perpetrating acts of terrorism in the name of Islam.

Others have been more circumspect in their pronouncements, but in essence the core assumption remains. In a speech on security to the Foreign Policy Centre in London early in 2006,[78] British Prime Minister Tony Blair argued in reference to the on-going war on terror:

This is not a clash between civilisations. It is a clash about civilisation. It is the age-old battle between progress and reaction, between those who embrace and see opportunity in the modern world and those who reject its existence; between optimism and hope on the one hand, and pessimism and fear on the other.

75 Frankl, VE *Man's Search for Meaning* (Boston: Beacon Press, 1959)
76 Laïdi, Z *A World Without Meaning* (London: Taylor & Francis, 1998)
77 Huntington, SP *The Clash of Civilizations & the Remaking of World Order* (New York: Simon & Schuster, 1996)
78 Speech at the Foreign Policy Centre, London, 21 March 2006. Available at: http://fpc.org.uk/events/past/231

But the ideas and protagonists Tony Blair apparently had in mind in his "clash about civilisation" are all foreign in their origins, or, at least, externally oriented and focused. He continued: "The roots of global terrorism and extremism are indeed deep. They reach right down through decades of alienation, victimhood and political oppression in the Arab and Muslim world."

In a similar vein, the recently released British government document *Countering International Terrorism: The United Kingdom's Strategy*[79] identifies the need for a "battle of ideas, challenging the ideological motivations that extremists believe justify the use of violence". This key strand of the strategy is described in terms indicating its having been solely conceptualised as affecting, or targeting, Muslims or Muslim communities.

So while most politicians and officials have slowly reconciled themselves to the fact that many of the perpetrators of contemporary acts of terror are Western-born or educated, the assumption remains that what drives them is a foreign ideology or agenda that only Muslims can understand or address – a point reasserted by the Prime Minister in subsequent comments to the House of Commons liaison committee,[80] and by the Home Secretary, Dr John Reid.[81]

But is the problem really a "clash about civilisation", or even, as the Home Secretary proposed, that we are having to manage the consequences of some kind of conflict within Islam? In some ways it seems we rather face a more profound cultural crisis domestically. To recognise the problem as such would be discomfiting for Western leaders and societies. It would require understanding the extent to which many of the ideas that inspire the nihilist terrorism we witness today are often home grown and inculcated.

Common explanation is poorly grounded

While conceding that many of the perpetrators and conspirators are increasingly turning out to have been Western in their origins, most, including Tony Blair, still presume their guiding influences to have been reactionary ideas and ideologies from the East. Hence, a lazy empirical approach has been employed to identify so-called "risk factors" that may

79 Cm 6888 (2006) (Norwich: HMSO)
80 Uncorrected transcript of oral evidence to the House of Commons liaison committee, 4 July 2006. Available at: http://www.publications.parliament.uk/pa/cm200506/cmselect/cmliaisn/uc709-iii/uc70902.htm
81 Speech to Muslim groups in east London, 20 September 2006. Available at: http://press.homeoffice.gov.uk/Speeches/sp-muslim-group-20-09-06

lead individuals to become "radicalised".[82] But this approach assumes a conclusion and then goes in search of the evidence to corroborate it. It is profoundly unscientific. Above all, it ignores the dominant social context within which most such individuals find themselves – that is, advanced Western societies.

Unsurprisingly, many researchers find their prejudices confirmed by using this method – that is what is wrong with it. Accordingly, an impoverished background, or having listened to the inflammatory rhetoric of an obscure cleric, are factors that appear to be confirmed in the minds of these researchers as "radicalising" influences. All agree that a deep sense of injustice as regards affairs in the Middle East is also key.[83]

But one could equally propose that being a billionaire, driving a white Mercedes or running the family business are significant risk factors. Certainly all three have featured in Osama bin Laden's life. Starting with an answer and then joining up the dots is child's play. It offers no insight beyond assumed conclusions.

The trial in London of the so-called "Crawley Group", accused of plotting further terrorist atrocities after acquiring a large quantity of ammonium nitrate fertiliser, is quite apposite in this regard. Their list of alleged intended targets included shoppers, drinkers, football supporters and "slags" in nightclubs.[84] The notion that these are major problems requiring to be regulated appears to reflect the ideas of certain policy makers and their exaggerated fears of social disorder in some sectors of society, rather more than verses from the Koran. So, could paying too much attention to contemporary commentators be a radicalising factor too?

As the academic Marc Sageman has pointed out in the most authoritative study of people associated with al-Qaeda,[85] there are no clear radicalising influences or predisposing risk factors that can be identified. If anything, these individuals are likely to a have a middle- or upper-class, secular background and to be reasonably well educated. That would put many of the critics and commentators at risk of becoming radicalised too.

82 There is a burgeoning literature on the causes of so-called radicalisation, emerging from a wide variety of organisations, very little of which is peer-reviewed.
83 *Towards a Community-based Approach to Counter-terrorism*, WPS06/5 (2006). Available at: http://www.wiltonpark.org.uk/documents/conferences/WPS06-5/pdfs/WPS06-5.pdf
84 "Gang 'Planned to Bomb London Nightclub'" in *The Guardian*, 25 May 2006
85 Sageman, M *Understanding Terror Networks* (University of Pennsylvania Press, 2004)

In particular, though, the individuals concerned were rarely recruited from above but rather seem actively to have sought out terrorist networks or sects that they might join. Some only converted to Islam after this. This would seem to confirm their desire to be part of something, but more importantly it raises the issue as to why they were unable to find that something closer to home.

What in the West is radicalising individuals?

The key is not what it is that attracts a minority from a variety of backgrounds, including some who are relatively privileged, to fringe Islamist organisations, but rather what it is about our own societies and culture that fails to provide aspirational, educated and energetic young individuals with a clear sense of purpose and collective direction through which to lead their lives and realise their ambitions, so that they are left looking for this elsewhere – including, for some, among various arcane and distorted belief systems.

In some ways the nihilist criminals that detonated their rudimentary devices in London in the summer of 2005 appear to reflect the sentiments of other disgruntled individuals and groups across the developed world today. Their acts seem more akin to the Columbine high-school massacre and other such incidents, where usually respectable young men, born and educated in the West, decide for various reasons – or none that we can work out – to kill themselves and scores of civilians.

Their ideas and influences appear to have far less to do with imams and mullahs, and far more in common with the dystopian views of numerous commentators who criticise Western society today. Indeed, a recently published compilation of Osama bin Laden's writings reveals how frequently he is inclined to cite Western writers, Western diplomats and Western thinkers.[86] At one point he even advises the White House to read Robert Fisk, rather than, as one might have supposed, the Koran.

It would be remiss to ignore the growing influence of a significant degree of what some have identified as a culture of self-loathing in the developed world. If one wants to discover anti-American views coherently expressed, or people who reject the benefits of science, progress and modernity, then one need not look far to find them. Such opinions are all around us.

86 Bin Laden, O, Lawrence, B (ed) and Howarth, J (transl) *Messages to the World: The Statements of Osama bin Laden* (London: Verso, 2005)

Indeed, less than two days had passed after 9/11 when Seumas Milne first used the term anti-American in a Guardian newspaper article, entitled "They Can't See Why They Are Hated".[87] On the same day, the Reverend Jerry Falwell, pastor of the 22,000-member Thomas Road Baptist Church of Lynchburg, Virginia, told US television viewers that God had given America "what we deserve".[88] Aside from such extremes, many others point to continued American intransigence over issues such as global warming and human rights as purported explanations for what happened.

Cultural self-loathing is widespread

It may be unpalatable or unpleasant to recall or recognise that a significant number of people, not all of whom were Muslim, were not that saddened to see the Twin Towers in New York going down. A sense that America had it coming was quite widespread in some supposedly respectable quarters, where a barely concealed Schadenfreude was in evidence. Many – including those in positions of authority or charged with defeating terrorism – are inclined to caricature contemporary culture as decadent and degenerate, or corrupt and selfish.

But this reflects a broader view of human action in the world. Increasingly, Western intellectuals have come to portray this as being largely negative.[89] Now mainstream milieus depict ambition as arrogant, development as dangerous and success as selfish. Within certain circles in America, too, power has become presented as egotism, freedom as illusory and the desire to defend oneself as the act of a bully.

Western society today is replete with individuals and institutions that appear determined to criticise and undermine human achievements. Even environmental agendas have been turned into sorry moral tales of human hubris, rather than an identification and celebration of the need for greater ingenuity.

Reflecting these trends, the President of the Royal Society called one of his latest books *Our Final Century: Will the Human Race Survive the Twenty-First Century?*,[90] while the Professor of European Thought at the London School of Economics & Political Science is comfortable describing human beings as being little more than a plague upon the planet

87 Milne, S "They Can't See Why They Are Hated" in *The Guardian*, 13 September 2001
88 Cited in "God Gave US 'What We Deserve', Falwell Says" in *Washington Post*, 14 September 2001
89 Bookchin, M *Re-enchanting Humanity: A Defense of the Human Spirit against Anti-Humanism, Misanthropy, Mysticism & Primitivism* (London: Cassell, 1995)
90 Rees, M (London: William Heinemann, 2003)

in his book *Straw Dogs: Thoughts on Humans & Other Animals*.[91] A recent edition of the prestigious UK science journal *New Scientist* speculated positively as to what the earth would be like without humans (and presumably without *New Scientist*) being there.[92]

Nor are such ideas limited to those of a few academics. Surely, when Michael Moore's *Stupid White Men* became the best-selling book on both sides of the Atlantic – selling over 300,000 copies in the UK in its first year of publication alone – a few bright minds in the security world and beyond should have noticed the growing depth of cynicism and disillusionment in society and their potentially adverse consequences?[93]

It is this cultural malaise and pessimistic outlook that forms the backdrop, and inevitably shapes, contemporary terrorism. Increasingly, it appears that this is sustained by two elements – the radical nihilists who are prepared to lose their lives and those of others around them in their misguided determination to leave their mark upon a world that they reject, and the nihilist intellectuals who help frame a public discourse and culture of apocalyptic failure and rejection.

Conclusion

Instead of imagining the root causes of terrorism in the UK as emanating from overseas, or reflecting some foreign ideology, it is time for us to recognise their domestic dimension. This is not, as some suppose, driven by social deprivation or exclusion, nor is it the consequence of a few influential individuals.

Rather it appears to reflect a broader sense of alienation and confusion that has gripped the modern world. Many today are in search of an identity and a meaning to their lives as the old networks and affiliations that used to provide these in the last century – national, religious and secular – have been eroded.

The uncertainty of our times has led many to view human action with concern, encouraging a destructive misanthropy that has been acted upon by some who view themselves as particular victims. It is this dominant dystopian culture, which is our own, that needs to be addressed if we are to defeat terrorism.

91 Gray, J (London: Granta, 2003)
92 "Earth Without People: What If We All Disappeared Tomorrow?" (14 October 2006)
93 Moore, M *Stupid White Men... & Other Sorry Excuses for the State of the Nation!* (London: Penguin, 2002)

Chapter 13

Waging war – parliament's role

Elizabeth Wilmshurst CMG, Associate Fellow at Chatham House

Waging war – parliament's role

The Prime Minister may commit British troops to a military engagement abroad without the approval of parliament. Acting under the royal prerogative, the government has the power to engage the UK in an armed conflict and to deploy armed forces overseas for any purpose. This freedom to act applies to the use of military force in any circumstance, whether in defence of the realm, in UN peacekeeping operations or in military intervention for humanitarian or any other purposes.

It may seem surprising, in a modern democratic state, that a matter as important as engaging British troops in conflict should be for decision by the government alone. This constitutional position is by no means rare in the rest of the world, but there are other approaches to be found, for example, in Sweden, Denmark, the Netherlands, Germany, Spain, and the USA.[94] Each of these states has its own system of requiring control by the legislature over the executive, although not all of them are regarded as very effective. But in the UK, while there has in recent times been an increase in parliamentary scrutiny and debate on specific instances of use of troops abroad,[95] there is no formal requirement for any parliamentary approval.

The intervention in Iraq in March 2003 provides a strong incentive to reconsider this lack of parliamentary involvement in decision making. In fact, in that case, a parliamentary vote was sought before the military action began. But there was no obligation on the government to follow that course; it chose to do so, and was also able to choose the wording of the motion, and the timing of the vote – at a period when substantial troop deployment had already taken place, and when there was very great pressure to support the action in view of the enormous diplomatic and other repercussions that would have resulted if approval was not secured.[96]

The House of Lords committee's findings

The House of Lords select committee on the constitution has recently enquired into the

94 For an illustrative list of the requirements in different states see the House of Lords constitution committee's 15th report of session 2005-06, *Waging War: Parliament's Role & Responsibility, Vol II: Evidence*, p56. For further detail see p242 (Sweden), pp31, 57 and 225 (Germany) and p89 (USA).

95 Examples may be found in White, N "The UK: Increasing Commitment Requires Greater Parliamentary Involvement" in Ku, C and Jacobson, H (eds) *Democratic Accountability & the Use of Force in International Law* (Cambridge: CUP, 2003), p300

96 See for example Clare Short's oral evidence to the House of Lords committee in *Waging War: Parliament's Role & Responsibility*, report of the House of Lords constitution committee, 15th report of session 2005-06 (Vol I: Report), p3

powers of the government to act without parliamentary approval. In its report of July 2006 under the title *Waging War: Parliament's Role & Responsibility*,[97] the committee concluded that the government should indeed seek parliamentary approval before deploying British forces outside the UK into actual or potential armed conflict, and for that purpose should inform parliament of the objectives of the deployment, its legal basis, likely duration and an estimate of its size. In times of emergency, approval should be sought from parliament retrospectively. The committee did not believe that this requirement on the government should be incorporated in legislation. There should instead be a "parliamentary convention" – a flexible rule that usually evolves over time, but which the committee envisaged as emerging fully grown.

The government rejected this recommendation, even in the relatively weak terms in which it was cast. In its response to the committee,[98] it reiterated the Prime Minister's statement of 7 February 2006: "The fact of the matter is that I cannot conceive of a situation in which a government ... is going to go to war – except in circumstances where militarily for the security of the country it needs to act immediately – without a full parliamentary debate," and added that the government was not persuaded of the need to go beyond that.[99] The present government's position therefore is that a policy decision should be taken on whether to involve parliament in each specific instance.

The arguments against

Proposals that there *should* be a legal requirement to seek parliamentary approval before the government commits the UK to engagement in an armed conflict are not new. Five bills have been introduced recently along these lines,[100] and there is a sixth one now before parliament.[101] None of them has made progress. The arguments against making any change look reasonable at first sight. In the first place, a requirement for parliament to approve the deployment of troops, in a political system where the party of the executive has a large parliamentary majority, may not significantly change the nature of existing democratic accountability. Further, opponents of proposals for change fear that the expected result of more parliamentary accountability would be a loss in the flexibility and speed of military response.

97 Ibid
98 Government response to the House of Lords constitution committee's report, 15th report of session 2005-06 (Cm 6923)
99 Ibid at para 4
100 See: p80, *Vol I: Report*
101 Waging War (Parliament's Role and Responsibility) Bill, a private member's bill introduced by Michael Meacher MP and others

They also point to the fact that general parliamentary tools of oversight and control are always available, such as the power to seek a vote of censure or no confidence in the Prime Minister, parliamentary control of finance, and general techniques of oversight by parliamentary questions and committees. In its response to the House of Lords constitution committee,[102] the government mentioned the general accountability of ministers to parliament as a reason why it considered no change was needed.

But the fact that ministers are responsible to parliament for *all* matters does not of course provide a reason why on a specific matter parliament should not have a more particular power to give its approval before the event, rather than blaming ministers after action is taken. Once conflict has started, it is the practice to exercise restraint in making any criticisms – to avoid damaging troop morale, among other reasons. The opportunities that exist at present to debate British involvement in conflict can in fact turn out to be chances for the government to persuade, rather than a real possibility for parliament to challenge and reject a decision before the start of military action.

Democratic legitimacy requires that there be a more formal role for parliament in the taking of decisions to engage the UK in armed conflict. There would be other advantages in making a change. The need to secure approval would impose a discipline on the government to clarify its objectives, and this in itself could help with the effectiveness of the operation. The morale of the forces would be benefited if they were to have a decision by parliament on the basis of such a statement by the government.[103] This is particularly the case with those conflicts where urgent requirements of self-defence are not present, as with the interventions in Kosovo in 1999 and in Iraq in 2003.

How to proceed

There is widespread support, including across the political parties,[104] for formalising a parliamentary role in this area. How should it be done?

102 At para 5

103 See, for instance, the memorandum of General Sir Michael Rose at p241, *Vol II: Evidence*; there were, however, voices on both sides of the question of the effects on troop morale – see paras 45-47 and 59 of *Vol I: Report.*

104 Gordon Brown has said that "a case now exists for a further restriction of executive power and a detailed consideration of the role of parliament in the declaration of peace and war"; David Cameron: "the time has come to look at those [prerogative] powers exercised by ministers ... Giving parliament a greater role in the exercise of these powers would be an important and tangible way of making government more accountable"; Menzies Campbell supported the 2003 motion for parliamentary approval on war-making decisions and the Armed Forces (Parliamentary Approval for Participation in Armed Conflict) Bill.

There should be a legal requirement for government to obtain approval from parliament before ordering a deployment of troops for combat. Retrospective approval could be sought in an emergency. The government should be required to present to parliament:

- The objective or objectives for the deployment plans following the close of hostilities and, where appropriate, for post-conflict reconstruction. Do the objectives include disarmament or regime change, for example, and how much commitment is there to reconstruction? The interventions in Iraq and Afghanistan provide obvious examples of the need for the latter.
- The justification under international law for taking action. The objectives given by the government must be wholly consistent with the legal basis for the action. In the case of the Iraq intervention, the Attorney General's controversial advice, on which the government relied, was that the use of force was lawful because Iraq had not complied with Security Council resolutions on weapons of mass destruction, and that those resolutions had authorised the use of force to secure compliance. But government spokesmen from time to time relied on other objectives for the military action, including purported self-defence and humanitarian intervention.

Such new legal requirements should be set out by legislation, not by a "parliamentary convention" as the House of Lords committee recommended. Conventions can be broken when governments wish. Further, the parliamentary process for debating and adopting legislation is desirable where a major constitutional step such as this is being taken. Legislation will allow the necessary qualifications and exceptions to the new requirement to be properly formulated. And legislation would seem the more appropriate vehicle to secure the necessary public debate.

Any new legislation would need to be carefully worded to define the trigger for parliamentary approval, to preserve speed and flexibility of military action, and to avoid any necessity for tactical or operational decisions to be taken by parliament. The issue of covert operations would need to be considered. It would have to be made clear that the consequences of failure by government to seek approval would not result in legal liability for the troops. The grant of approval by parliament would not detract from the requirement for the government and the troops to comply throughout the operation with international law and UK law regarding the conduct of the conflict. It would be open to parliament to strengthen its ability to take decisions in this matter by setting up a new committee or using an existing one, if it wished, to inquire more closely into the intelligence and other factual grounds for proposing military action, and for taking its

own legal advice.

The preparation of any such legislation would undoubtedly be very difficult, particularly in view of the need to avoid unwanted consequences. But the difficulties of the work should not detract from the desirability of taking seriously the democratic principle and improving the process of decision making in such a crucial matter as engaging in conflict.

It may well be that even as things stand, no Prime Minister would commit British troops to a major engagement without a debate in parliament. To formalise this as a legal requirement would ensure that reliance on the political will of government would not be necessary and that approval would indeed be sought for all deployments into combat. It may also encourage more openness about the basis in international law on which the government is proposing to enter into a military engagement, and about any surrounding circumstances that would allow parliament to take the decision with a better understanding of the facts.

The motivation for new legislation is not simply to subscribe to the principle of democratic legitimacy, but to seek an improvement that will make decision making on the use of military force a better process in practice. At a time when what have been described as the two major catastrophes of British military interventions in modern times – Suez in 1956 and Iraq in 2003 – are being discussed and compared, consideration should be given to how a fuller engagement by parliament might secure a better result "next time". In the aftermath of a military intervention that is considered by so many to be unjustified, unlawful and ill-prepared, with disastrous consequences for the region, now would be the time to act.